La conjecture des anneaux de Hermite en dimension 1

Ihsen Yengui

Département de Mathématiques,
Faculté des Sciences de Sfax, Tunisie
Email: ihsen.yengui@fss.rnu.tn

JNCF 08, Luminy, Octobre 2008

The Hermite ring conjecture 1972: *If* $\mathbf{R}$ *is an Hermite ring, then* $\mathbf{R}[X]$ *is also Hermite.*

$\Updownarrow$

If $\mathbf{R}$ *is a ring and* $v = (v_0(X), \ldots, v_n(X))$ *is a unimodular row over* $\mathbf{R}[X]$ *such that* $v(0) = (1, 0, \ldots, 0)$*, then* v *can be completed to a matrix in* $\mathsf{GL}_{n+1}(\mathbf{R}[X])$*.*

Recall that a ring $\mathbf{A}$ is said to be Hermite if any finitely generated stably free $\mathbf{A}$-module is free. Examples of Hermite rings are local rings, rings of Krull dimension ≤ 1, polynomial rings over Bezout domains.

I will prove constructively that for any finite-dimensional ring $\mathbf{R}$ and $n \geq \dim \mathbf{R}+2$, the group $\mathsf{E}_n(\mathbf{R}[X])$ acts transitively on $\mathsf{Um}_n(\mathbf{R}[X])$.

In particular, I obtain, without any Noetherian hypothesis, that for any finite-dimensional ring $\mathbf{R}$, all finitely generated stably free modules over $\mathbf{R}[X]$ of rank $> \dim \mathbf{R}$ are free.

More particularly, $\mathbf{I}$ obtain that for any ring $\mathbf{R}$ with Krull dimension ≤ 1, all finitely generated stably free modules over $\mathbf{R}[X]$ are free. This settles the Hermite ring conjecture for rings of Krull dimension ≤ 1.

The proof relies heavily on the very nice paper of **M. Roitman** "*On stably extended projective modules over polynomial rings*, Proc. Amer. Math. Soc. 97 (1986) 585-589" .

Lemma 0: *Let* $\mathbf{R}$ *be a ring, and* $f, g \in \mathbf{R}[X]$ *with* f *a monic polynomial. Then*

$$\langle f, g \rangle = \mathbf{R}[X] \quad \Longleftrightarrow \quad \mathrm{Res}(f, g) \in \mathbf{R}^{\times}.$$

Proof: "$\Leftarrow$" This is an immediate consequence of the fact that $\mathrm{Res}(f, g) \in \langle f, g \rangle \cap \mathbf{R}$.

"$\Rightarrow$" Let $u, v \in \mathbf{R}[X]$ such that $uf + vg = 1$. Since f is a monic polynomial, we have

$$\mathrm{Res}(f, vg) = \mathrm{Res}(f, v)\,\mathrm{Res}(f, g)$$

$$= \mathrm{Res}(f, vg + uf) = \mathrm{Res}(f, 1) = 1.$$

Lemma 1: *Let* $\mathbf{R}$ *be a ring, and* I *an ideal in* $\mathbf{R}[X]$ *that contains a monic polynomial. Let* J *be an ideal in* $\mathbf{R}$ *such that* $I + J[X] = \mathbf{R}[X]$*. Then* $(I \cap \mathbf{R}) + J = \mathbf{R}$*.*

Classical Proof: Use the "going-up" property of integral extensions.

Constructive Proof: Let us denote by f a monic polynomial in I. Since $I + J[X] = \mathbf{R}[X]$, there exist $g \in I$ and $h \in J[X]$ such that $g + h = 1$. It follows that $\langle \overline{f}, \overline{g} \rangle = (\mathbf{R}/J)[X]$ where the classes are taken modulo $J[X]$. By virtue of Lemma 0, we obtain that $\mathrm{Res}(\overline{f}, \overline{g}) \in (\mathbf{R}/J)^{\times}$. As f is a monic polynomial, $\mathrm{Res}(\overline{f}, \overline{g}) = \overline{\mathrm{Res}(f, g)}$, and thus $\langle \mathrm{Res}(f, g) \rangle + J = \mathbf{R}$. The desired conclusion follows from the fact that $\mathrm{Res}(f, g) \in I \cap \mathbf{R}$.

Lemma 2 (Roitman): *Let* $\mathbf{R}$ *be a ring, and* $f(X) \in \mathbf{R}[X]$ *of degree* $n > 0$*, such that* $f(0) \in \mathbf{R}^{\times}$*. Then for any* $g(X) \in \mathbf{R}[X]$ *and* $k \geq \deg g(X) - \deg f(X) + 1$*,* $\exists$ $h_k(X) \in \mathbf{R}[X]$ *of degree* $< n$ *such that* $g(X) \equiv X^k h_k(X) \mod \langle f(X) \rangle$*.*

Proof: Let $f(X) = a_0 + \cdots + a_n X^n$, $g(X) = c_0 + \cdots + c_m X^m$. Let $g(X) - c_0 a_0^{-1} f(X) = X h_1(X)$. Then $g(X) \equiv X h_1(X) \mod \langle f(X) \rangle$ and $\deg h_1(X) < \max(m, n)$. Similarly we obtain $h_2(X)$ such that $h_1(X) \equiv X h_2(X) \mod \langle f(X) \rangle$, $g(X) \equiv X^2 h_2(X) \mod \langle f(X) \rangle$, $\deg h_2(X) < \max(m-1, n)$, and so on.

Lemma 3 (Vaserstein): *Let* $\mathbf{R}$ *be a ring, and* $(x_0, \ldots, x_r) \in \mathsf{Um}_{r+1}(\mathbf{R})$, $r \geq 2$, *and let* t *be an element of* $\mathbf{R}$ *which is invertible* mod $\langle x_0, \ldots, x_{r-2} \rangle$. *Then there exists* $E \in \mathsf{E}_{r+1}(\mathbf{R})$ *such that* $E\,(x_0, \ldots, x_r) = (x_0, \ldots, x_{r-1}, t^2 x_r)$.

Proof: This is also Proposition III.6.1.(b) of **T. Y. Lam**'s book "*Serre's Problem on Projective Modules.* Springer Monographs in Mathematics, 2006". The proofs given by Lam and Roitman are constructive and free of any Noetherian hypothesis.

Lemma 4 (Bass): *Let $k \in \mathbb{N}$, $\mathbf{R}$ a ring, $f_1, \ldots, f_r \in \mathbf{R}[X]$ with degrees $\leq k-1$, and $f_{r+1} \in \mathbf{R}[X]$ monic with degree k. If the coefficients of $f_1, \ldots, f_r$ generate the ideal $\mathbf{R}$ of $\mathbf{R}$, then $\langle f_1, \ldots, f_r, f_{r+1} \rangle$ contains a monic with degree $k-1$.*

Proof: Let us denote by $\mathfrak{a} = \langle f_1, \ldots, f_r, f_{r+1} \rangle$ and $\mathfrak{b}$ the ideal formed by the coefficients of X^{k-1} of the elements of $\mathfrak{a}$ having degree $\leq k-1$. It suffices to prove that $\mathfrak{b} = \mathbf{R}$. In fact we will prove that $\mathfrak{b}$ contains all the coefficients of $f_1, \ldots, f_r$. For $1 \leq i \leq r$, denoting by $f_i = b_0 + b_1 X + \cdots + b_{k-1} X^{k-1}$ and $f_{r+1} = a_0 + \cdots + a_{k-1} X^{k-1} + X^k$, we have $b_{k-1} \in \mathfrak{b}$ and $f_i' = X f_i - b_{k-1} f = b_0' + b_1' X + \cdots + b_{k-1}' X^{k-1} \in \mathfrak{a}$ with $b_j' \equiv b_{j-1} \mod \langle b_{k-1} \rangle$. Thus, $b_{k-1}' = b_{k-2} - a_{k-1} b_{k-1} \in \mathfrak{b}$, $b_{k-2} \in \mathfrak{b}$, and so on until getting that all the b_i's are in $\mathfrak{b}$.

Lemma 5 (Suslin): *Let* $\mathbf{A}$ *be a commutative ring. If* $\langle v_1(X), \ldots, v_n(X)\rangle = \mathbf{A}[X]$ *where* v_1 *is monic and* $n \geq 2$*, then there exist* $\gamma_1, \ldots, \gamma_\ell \in \mathsf{E}_{n-1}(\mathbf{A}[X])$ *such that, denoting by* w_i *the first coordinate of* ${\gamma_i}^{\mathsf{t}}(v_2, \ldots, v_n)$*, we have*

$$\langle \mathsf{Res}(v_1, w_1), \ldots, \mathsf{Res}(v_1, w_\ell)\rangle = \mathbf{A}.$$

Proof: A constructive proof is given in I. Y " *Making the use of maximal ideals constructive*. Theoretical Computer Science **392** (2008) 174-178" .

Stable range Theorem: *Let* $\mathbf{R}$ *be a ring of dimension* $\leq d$, $n \geq d+1$, *and let* $v = (v_0, \ldots, v_n) \in \mathsf{Um}_{n+1}(\mathbf{R})$. *Then there exists* $E \in \mathsf{E}_{n+1}(R)$ *such that* $Ev = (1, 0, \ldots, 0)$.

Stable range Theorem, bis: *For any ring* $\mathbf{R}$ *with Krull dimension* $\leq d$, *all finitely generated stably free* $\mathbf{R}$*-modules of rank* $> d$ *are free.*

Proof: A constructive proof is given by **T. Coquand, H Lombardi and C. Quitté** in "*Generating non-noetherian modules constructively.* Manuscripta mathematica **115** (2004) 513–520".

Recall that the boundary ideal of an element a of a ring $\mathbf{R}$ is the ideal $\mathcal{I}(a)$ of $\mathbf{R}$ generated by a and all the $y \in \mathbf{R}$ such that ay is nilpotent. Moreover, $\dim R \leq d \Leftrightarrow \dim(\mathbf{R}/\mathcal{I}(a)) \leq d-1 \ \forall\ a \in \mathbf{R}$.

This defines the Krull dimension recursively initializing with "$\dim \mathbf{R} \leq -1 \Leftrightarrow \mathbf{R}$ being trivial".

See the paper by **T. Coquand T, H. Lombardi, and M.-F. Roy** "*An elementary characterization of Krull dimension*, From sets and types to analysis and topology: towards practicable foundations for constructive mathematics (L. Corsilla, P. Schuster, eds), Oxford University Press, 2005".

Main Theorem: *Let* $\mathbf{R}$ *be a ring of dimension* $\leq d$, $n \geq d+1$, *and let* $v(X) = (v_0(X), \ldots, v_n(X)) \in \mathsf{Um}_{n+1}(\mathbf{R}[X])$. *Then there exists* $E \in \mathsf{E}_{n+1}(R[X])$ *such that* $E\,v(X) = (1, 0, \ldots, 0)$.

Proof: By virtue of the Stable range Theorem, it suffices to prove that there exists $E \in \mathsf{E}_{n+1}(R[X])$ such that $E\,v(X) = v(0)$. For this, by the local-global principle for elementary matrices, we can suppose that $\mathbf{R}$ is local. Moreover, it is clear that we can suppose that $\mathbf{R}$ is reduced.

We prove the claim by double induction on the number N of nonzero coefficients of $v_0(X), \ldots, v_n(X)$ and d, starting with $N = 1$ (in that case the result is immediate) and $d = 0$ (in that case the result is well-known).

We will first prove a first claim: $v(X)$ can be transformed by elementary operations into a vector with one constant entry.

Let $N > 1$ and $d > 0$. We may assume that $v_0(0) \in \mathbf{R}^\times$. Let us denote by a the leading coefficient of v_0 and $m_0 := \deg v_0$. If $a \in \mathbf{R}^\times$ then the result follows from Suslin's lemma. So we may assume $a \in \mathrm{Rad}(\mathbf{R})$. By the induction hypothesis applied to the ring $\mathbf{R}/\langle a \rangle$, we can assume that $v(X) \equiv (1, 0, \ldots, 0) \bmod (a\mathbf{R}[X])^{n+1}$.

By Roitman's Lemma, we assume now $v_i = X^{2k} w_i$, where $\deg w_i < m_0$ for $1 \leq i \leq n$. By Vaserstein's Lemma, we assume $\deg v_i < m_0$.

If $m_0 \leq 1$, our first claim is established. Assume now that $m_0 \geq 2$.

Let $(c_1, \ldots, c_{m_0(n-1)})$ be the coefficients of $1, X, \ldots, X^{m_0-1}$ in the polynomials $v_2(X), \ldots, v_n(X)$. By Lemma 1, the ideal generated in $\mathbf{R}_a$ by $\mathbf{R}_a \cap (v_0\mathbf{R}_a[X] + v_1\mathbf{R}_a[X])$ and the c_i's is $\mathbf{R}_a$. As $m_0(n-1) \geq 2d > \dim \mathbf{R}_a$, by the Stable range Theorem,

$$\exists\ (c'_1, \ldots, c'_{m_0(n-1)}) \equiv (c_1, \ldots, c_{m_0(n-1)})$$

$$\text{mod } (v_0\mathbf{R}[X] + v_1\mathbf{R}[X]) \cap \mathbf{R}$$

such that $c'_1\mathbf{R}_a + \cdots + c'_{m_0(n-1)}\mathbf{R}_a = \mathbf{R}_a$.

Assume that we have already $c_1\mathbf{R}_a + \cdots + c_{m_0(n-1)}\mathbf{R}_a = \mathbf{R}_a$. By Bass' Lemma, the ideal $\langle v_0, v_2, \ldots, v_n\rangle$ of $\mathbf{R}[X]$ contains a polynomial $w(X)$ of degree $m_0 - 1$ which is unitary in $\mathbf{R}_a$. Let us denote the leading coefficient of w by ua^k where $u \in \mathbf{R}^\times$ and that of v_1 by b. Using Vaserstein's Lemma, we can by elementary operations make the following transformations

$$(v_0, v_1, \ldots, v_n) \quad \rightarrow \quad (v_0, a^{2k}v_1, \ldots, v_n) \quad \rightarrow \quad (v_0, a^{2k}v_1 + (1 - a^k u^{-1}b)w, v_2, \ldots, v_n).$$

Now, $a^{2k}v_1 + (1 - a^k u^{-1}b)w$ is unitary in $\mathbf{R}_a$. So wa can assume that v_1 unitary in $\mathbf{R}_a$, and $\deg(v_1) := m_1 < m_0$.

By Vaserstein's Lemma, as a is invertible modulo $\langle v_0, v_1 \rangle$, by elementary operations, $(v_0, v_1, v_2, \ldots, v_n)$ can be transformed into $(v_0, v_1, a^\ell v_2, \ldots, a^\ell v_n)$ for a suitable $\ell \in \mathbb{N}$ so that we can divide (like in Euclidean division) all $a^\ell v_2, \ldots, a^\ell v_n$ by v_1, and thus we can assume that $\deg v_i < m_1$ for $2 \leq i \leq n$.

Repeating the argument above we lower the degree of v_1 until reaching the desired form of our first claim.

Assume now that $v_0 = a \in \mathbf{R}$. Let us consider the ring $\mathbf{T} := \mathbf{R}/\mathcal{I}(a)$. Since $\dim \mathbf{T} \leq d-1$ and $(\overline{v}_1, \ldots, \overline{v}_n) \in \mathsf{Um}_n(\mathbf{T}[X])$, there exists $E_1 \in \mathsf{E}_n(\mathbf{R}[X])$ such that

$$\begin{gathered} E_1(v_1, \ldots, v_n) \\ = (1 + ah_1 + y_1\tilde{h}_1, ah_2 + y_2\tilde{h}_2, \ldots, ah_n + y_n\tilde{h}_n), \end{gathered}$$

where $h_i, \tilde{h}_i \in \mathbf{R}[X]$, $y_i \in \mathbf{R}$ with $ay_i = 0$.

Denoting by $E_2 = \begin{pmatrix} 1 & 0 \\ 0 & E_1 \end{pmatrix} \in \mathsf{E}_{n+1}(\mathbf{R}[X])$, we have

$$E_2\, v = (a, 1+ah_1+y_1\tilde{h}_1, ah_2+y_2\tilde{h}_2, \ldots, ah_n+y_n\tilde{h}_n).$$

Thus,

$$\begin{gathered} E_{1,2}(-a)E_{2,1}(-h_1)\cdots E_{n+1,1}(-h_n)\, E_2\, v \\ = (0, 1 + y_1\tilde{h}_1, y_2\tilde{h}_2, \ldots, y_n\tilde{h}_n) =: \tilde{v}, \end{gathered}$$

and we can easily find $E_3 \in \mathsf{E}_{n+1}(\mathbf{R}[X])$ such that $E_3\, \tilde{v} = (1, 0, \ldots, 0)$.

Corollary 1: *For any ring* $\mathbf{R}$ *with Krull dimension* $\leq d$*, all finitely generated stably free modules over* $\mathbf{R}[X]$ *of rank* $> d$ *are free.*

Corollary 2: *The Hermite ring conjecture is true for rings with Krull dimension* ≤ 1*.*

Conjecture 1: *For any ring* $\mathbf{R}$ *with Krull dimension* $\leq d$*, all finitely generated stably free modules over* $\mathbf{R}[X_1, \ldots, X_k]$ *of rank* $> d$ *are free.*

Question 1: *Is it true that for any ring* $\mathbf{R}$ *of Krull dimension* $\leq d$*, all finitely generated stably free modules over* $\mathbf{R}[X, X^{-1}]$ *of rank* $> d$ *are free ?*

Conjecture 2: *For any ring* $\mathbf{R}$ *of Krull dimension* ≤ 1*, and* $k \in \mathbb{N}$*, all finitely generated stably free modules over* $\mathbf{R}[X_1, \ldots, X_k]$ *are free.*

Conjecture 3: *Let* $\mathbf{R}$ *be a ring of Krull dimension* ≤ 1 *and* $n \geq 3$*. Then every matrix* $M \in \mathsf{SL}_n(\mathbf{R}[X])$ *is congruent to* $M(0)$ *modulo* $\mathsf{E}_n(\mathbf{R}[X])$*.*

$\Updownarrow$

Conjecture 3': *Suppose* $\mathbf{R}$ *is a local ring of Krull dimension* ≤ 1*, and*

$$M = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathsf{SL}_3(\mathbf{R}[X]).$$

Then $M \in \mathsf{E}_3(\mathbf{R}[X])$*.*

Question ouverte

$\exists$ *?* $u_0, u_1, u_2 \in (\mathbb{Z}/2\mathbb{Z})[x_0, x_1, x_2, y_1, y_2, y_3]$ |

$$1 \in \langle x_0u_1 - x_1u_0, x_0u_2 - x_2u_0, x_1u_2 - x_2u_1, x_0^2 + x_1y_1 + x_2y_2 - 1\rangle$$

Si $x_0^2 + x_1y_1 + x_2y_2 - 1 \leftrightarrow x_0^2 + x_1^2 + x_2y_2 - 1$, la réponse est oui (facile, calcul direct sur le vecteur (x_0, x_1, x_2))

Si $x_0^2 + x_1y_1 + x_2y_2 - 1 \leftrightarrow x_0y_0 + x_1y_1 + x_2y_2 - 1$, la réponse est non (difficile, arguments topologiques compliqués)