Journal de Théorie des Nombres
de Bordeaux **13** (2001), 211–226

Équations diophantiennes polynomiales à hautes multiplicités

par Michel LANGEVIN

Résumé. On montre comment écrire de grandes familles, avec de hautes multiplicités, de cas d'égalité $A + B = C$ pour l'inégalité de Stothers-Mason (si $A(X)$, $B(X)$, $C(X)$ sont des polynômes premiers entre eux, le nombre exact de racines du produit ABC dépasse de 1 le plus grand des degrés des composantes A, B, C). On développera pour cela des techniques polynomiales itératives inspirées des décompositions de Dunford-Schwartz et de fonctions de Belyi. Des exemples d'application avec les conjectures (abc) ou de M. Hall sont développés.

Abstract. One shows how to write and to classify large sets of relations $A+B = C$ (where $A = A(X)$, $B = B(X)$, $C = C(X)$ are coprime polynomials such that the exact number of roots of the product ABC exceeds by 1 the greatest degree of components A, B, C) with high multiplicities. Iterative polynomial methods generating high multiplicities (decomposition of Dunford-Schwartz, Belyi's functions) are developed. Links with Stothers-Mason Theorem and classical conjectures (M. Hall, abc) are studied.

1. Introduction, Généralités et Résultats

1.1. La formulation du titre "Équations diophantiennes polynomiales" peut surprendre puisque l'expression "équations diophantiennes" s'applique aux "équations ou systèmes dont on recherche les solutions en entiers ou nombres rationnels" (M. David, l'Encyclopædia Universalis, loc. citée). La raison en est qu'on s'intéresse ici aux éventuelles équations polynomiales (à coefficients entiers ou rationnels) susceptibles d'être "au-dessus" de telle ou telle équation diophantienne. À ce titre, ce travail s'inscrit dans la continuité de celui exposé aux Journées Arithmétiques de Limoges (1997) et publié dans cette revue (cf. [L]) et, comme dans celui-ci, la caractéristique est toujours supposée nulle. On y montrait que l'inégalité de Mason (où $A(X)$, $B(X)$, $C(X) = A(X) + B(X)$ sont des polynômes complexes premiers entre eux et où D (supposé > 0) désigne le plus grand des degrés

Manuscrit reçu le 1er novembre 1999.

correspondants) : $r(ABC) = \operatorname{card}((ABC)^{-1}(0)) > D$ est beaucoup plus qu'une forme polynomiale démontrée possible [1] de la conjecture (abc) de J. Oesterlé et D. Masser : Pour tout réel $\varepsilon > 0$, la borne inférieure suivante est strictement positive :

$$\inf_{\substack{(a,b)\in\mathbb{N}^{*\,2},\ \mathrm{pgcd}(a,b)=1 \\ c=a+b}} \left(\prod_{p|abc} p\right) c^{\varepsilon-1} = C(\varepsilon) > 0$$

(en bref et avec les notations de [L] où le radical – *i.e.* le produit des facteurs premiers – est noté u : $u(abc) \geqslant C_\varepsilon c^{1-\varepsilon}$). Comme exposé dans la partie 1 de [L], l'appellation théorème de Mason , *i.e.* l'énoncé polynomial $r(ABC) > D$, masque un ensemble de calculs et de méthodes projectives d'où ressort l'importance de l'étude d'une part des cas d'égalités (*i.e.* ceux où $r(ABC) = D + 1$, ce qui correspond à un revêtement $x \mapsto A(x)/B(x)$ ramifié au plus en $0, 1, \infty$), et, d'autre part, des spécialisations de l'indéterminée X en un polynôme ou une fraction rationnelle convenables (avec les notations habituelles, ces spécialisations représentent des endomorphismes de l'algèbre $K[X]$ (ou $K(X)$), naturellement "au-dessus" de fonctions algébriques dans les anneaux ou corps de nombres). Ces spécialisations ont généralement pour but d'augmenter les multiplicités (plutôt que les degrés des composantes irréductibles) dans les relations (A, B, C) qui sont des cas d'égalité, et ce tout en restant dans ce dernier ensemble (cf. théorème 13 et le 5.2 de [L] pour des justifications et applications).

1.2. Avant de poursuivre vers ces "hautes multiplicités", on donne deux exemples relatifs aux notions qu'on vient d'évoquer.

Exemple 1.

Les identités[2] :

$$(X-1)^3(X+3) - (X+1)^3(X-3) = 16X,$$
$$(X+3)^3(X-1) - (X-3)^3(X+1) = 16X^3$$

[1] Les traductions de la conjecture (abc) –et la formulation de cette dernière elle-même– peuvent varier avec le contexte ; les exposés ou comptes-rendus de nombreux auteurs (E. Bombieri à Zurich en 1994, A. Baker à Eger en 1996, J. Top au Centre Emile Borel (I.H.P., Paris 1999) en témoignent) ; on pourra consulter le récent article [P] de P. Philippon et voir la forme polynomiale proposée par J. Oesterlé dans [L].

[2] Concernant des exemples de solutions multiples, une variante homographiquement équivalente m'a été communiquée "par retour" par J. Oesterlé :
$(2X-1)^3(2X+1) - 16X^3(X-1) = 4X-1, \quad (2X+1)^3(2X-1) - 16X(X-1)^3 = (4X-1)^3.$

sont des cas d'égalité homographiquement équivalents (par la spécialisation involutive $X \mapsto 3/X$) ; ils montrent que l'équation $A+B=C$ où les radicaux de A, B, C sont donnés peut avoir plusieurs solutions [3]. À l'opposé, il y a unicité si l'un des polynômes A, B, C est constant. Autrement dit,

Proposition. *P étant un polynôme de degré positif, les ensembles $P^{-1}(0)$ et $P^{-1}(1)$ caractérisent P.*

Démonstration. Si le polynôme Q vérifie $Q^{-1}(0) = P^{-1}(0)$ et $Q^{-1}(1) = P^{-1}(1)$, son degré est, d'après l'inégalité de Mason, au plus $(\mathrm{card}(P^{-1}(0)) + \mathrm{card}(P^{-1}(1)) - 1)$ et ses coefficients satisfont à un système de Cramer montrant que $P = Q$. □

N.B. : Deux parties finies disjointes A, B de $\mathbb{C}$ étant données, il se peut que n'existe aucun $P \in \mathbb{C}[X]$ vérifiant $A = P^{-1}(0)$, $B = P^{-1}(1)$.

Exemple 2. Un cas facile du théorème 13 de [L] montre qu'un cas d'égalité $A(X) + B(X) = C(X)$ demeure un cas d'égalité par la spécialisation $X \mapsto Q(X)$ quand la dérivée $Q'(X)$ divise le produit $A(Q(X))B(Q(X))C(Q(X))$. Les polynômes de Čebičev C_n (de première espèce) et D_n (de deuxième espèce), définis par $C_n(\cos\theta) = \cos(n\theta)$, $D_n(\cos\theta) = \sin(n\theta)/\sin\theta$ ($D_n = C_n'/n$), vérifient l'identité

$$(\Theta_n) \ : C_n^2 - (X^2-1)D_n^2 = 1,$$

laquelle est un cas d'égalité, et, comme on va le voir, ces polynômes fournissent deux exemples naturels d'application de ce théorème 13 qu'on utilisera dans la suite de ce travail. Explicitement, ces polynômes s'écrivent :

$$C_n(X) = (n/2)\left(\sum_{j\geqslant 0}(-1)^j(n-2j)^{-1}\binom{n-j-1}{j}(2X)^{n-2j}\right)$$

$$D_n(X) = \left(\sum_{j\geqslant 0}(-1)^j\binom{n-j-1}{j}(2X)^{n-2j-1}\right).$$

Dans (Θ_n), on voit que X^2 apparaît seul, donc (Θ_n) est une spécialisée en X^2 d'un cas d'égalité (Θ_n') de degré n, et le critère du théorème 13 de [L] est vérifié puisque X divise $C_n(X)D_n(X)$. De plus, si, dans (Θ_n), on spécialise X en $C_m(X)$, on obtient un nouveau cas d'égalité puisque $C_m'(X)/m = D_m(X)$ divise

$$\left[X^2-1\right]_{X=C_m(X)} = (X^2-1)D_m^2(X),$$

[3] D'autres solutions sont possibles en sortant des "cas d'égalité". Par exemple :

$(X-1)(X+3)-(X+1)(X-3)=4X$, $\quad (X+1)(X-3)-X(X-1)=-(X+3)$, $\quad (X-1)(X+3)-X(X+1)=X-3$,

$(2X-1)(2X+1)-4X(X-1)=4X-1$, $\quad (2X-1)(2X+1)-X(4X-1)=X-1$, $\quad 8X(X-1)+(2X+1)=(4X-1)(2X-1)$.

et ce nouveau cas d'égalité est (Θ_{nm}) puisque, comme le rappelle la définition $C_n(\cos\theta) = \cos(n\theta), C_n \circ C_m = C_m \circ C_n = C_{mn}$.

1.3. D'autres illustrations de ces spécialisations et multiplicités sont évoquées dans les parties 3 et 4 de [L] : ainsi, derrière un énoncé plus général, le but du théorème 5 est de montrer que, pour tout polynôme à racines rationnelles distinctes $A(X) = \prod_{i=1}^{r}(X - x_i)$, existent des multiplicités $e_i \in \mathbb{Z}^*$ $(1 \leqslant i \leqslant r)$ telles que le triplet de polynômes $(R, S, R - S)$ avec $R(X) = \prod_{e_i>0}(X - x_i)^{e_i}, S(X) = \prod_{e_i<0}(X - x_i)^{e_i}$ soit un cas d'égalité ; de même, le but du théorème 8 est de montrer que, pour tout polynôme séparable $P(X)$ à coefficients entiers, il existe deux polynômes auxiliaires $A(X)$ et $Q(X)$ à coefficients entiers, le premier à racines rationnelles distinctes, tels que le produit $P(X)Q'(X)$ (où Q' désigne la dérivée) divise le composé (ou spécialisé) $A(Q(X))$. Avec cette dernière condition et la construction précédente d'un cas d'égalité $(R, S, R - S)$ "au-dessus" du polynôme séparable A à racines rationnelles, on démontre (et c'est encore un lemme de multiplicités) que cette spécialisation de X en $Q(X)$ conserve au triplet $\big(R\big(Q(X)\big), S\big(Q(X)\big), \big(R - S\big)\big(Q(X)\big)\big)$ sa qualité de cas d'égalité ; et c'est ainsi (cf. partie 4 dans [L]) qu'on en déduit que la conjecture (abc) – où $c = a + b$ – implique l'inégalité $(abF(a, b))$, valable pour tout polynôme homogène F à coefficients entiers de degré $f > 0$ tel que $UVF(U, V)$ soit sans facteur multiple :

$$\inf_{\substack{(a,b)\in\mathbb{Z}^{*2},\ \mathrm{pgcd}(a,b)=1,\\ c=F(a,b),\ abc\neq 0}} \left(\prod_{p|abc} p\right) (|a| + |b|)^{\varepsilon - f} = C(\varepsilon, F) > 0.$$

Autrement dit, $u(abF(a, b)) > C_{\varepsilon,F}(|a| + |b|)^{f-\varepsilon}$.

En résumé, les énoncés évoqués plus haut sont des applications de techniques polynomiales dont la démonstration s'effectue directement et souvent simplement. À titre d'exemple, on peut vérifier que la forme donnée ci-dessus au théorème 8 s'obtient par récurrence sur le plus grand des degrés des facteurs irréductibles de $P(X)$ (soit par exemple $F(X)$) en formant le radical (où Res_Y désigne le résultant pour l'indéterminée Y) : $u\left(\mathrm{Res}_Y\big(P(Y)F'(Y), X - F(Y)\big)\right)$.

1.4. On ne poursuit pas ici sur la voie des développements totalement explicités de ces théorèmes (et de leurs applications) mais sur la voie initiale en traitant d'autres "lemmes polynomiaux" permettant de faire apparaître de hautes multiplicités (et, dans les cas favorables, de rester dans l'ensemble des "cas d'égalité"). Comme conséquence de ces lemmes polynomiaux, on retrouvera la classique décomposition (dite "de Dunford et Schwartz") pour les endomorphismes des espaces vectoriels de dimension finie sur un corps parfait (mais les corps considérés dans ce travail sont de caractéristique 0) en composante semi-simple et composante nilpotente. On traitera un exemple et une application de ces lemmes en développant un résultat dû à Danilov et Schinzel évoqué dans le 5.1 de [L] : “ Il existe une infinité de couples (a, b) d'entiers vérifiant : $0 < |a^3 - b^2| < 2 \cdot 3^3 \cdot 5^{-2}\sqrt{a/5}$”. On renvoie à [L] pour replacer ce résultat dans le contexte de la conjecture de Hall : $|a^3 - b^2| \gg \sqrt{a}$ et pour le nouveau cas obtenu en 1998 par N. Elkies :

$$(3 \cdot 7211 \cdot 38791 \cdot 6975841)^3 - (2 \cdot 3^2 \cdot 15228748819 \cdot 1633915978229)^2 = 3^3 \cdot 7^2 \cdot 17 \cdot 73.$$

Ce qu'on mettra en évidence, c'est une suite de cas $(A, B, C = A + B)$ polynomiaux vérifiant $r(ABC) = D + 1$ qui, tous spécialisés au point 11, conduiront à cette valeur d'adhérence (la meilleure connue présentement) $2 \cdot 3^3 \cdot 5^{-5/2}$ pour l'ensemble des quotients non nuls de la forme $|a^3 - b^2|/\sqrt{a}$. Les lemmes polynomiaux font l'objet de la partie 2 ; l'application qu'on vient d'évoquer fait celui de la partie 3.

2. L'endomorphisme DS

2.1.

Théorème 1. *Soit $P(X)$ un polynôme séparable de degré $d > 0$ à coefficients dans un corps K de caractéristique nulle ; il existe un unique endomorphisme DS de l'algèbre $K[X]$: $X \mapsto DS(X)$, où $DS(X)$ est un polynôme de degré $< 2d$, tel que, pour tout entier $m > 1$, $P(X)^m$ divise $P\big(DS^f(X)\big)$ lorsque $f = f(m)$ est assez grand (DS^f désigne l'itéré d'ordre f : $DS \circ DS \circ \cdots \circ DS$).*

Démonstration. On montre d'abord l'existence d'un polynôme $DS(X)$ tel que $P(X)^2$ divise $P(DS(X))$, et on en déduira par récurrence que $P(X)^{2^k}$ divise $P(DS^k(X))$ pour tout $k \geqslant 0$. En effet, on voit que, pour tout polynôme $U(X)$, $P(X)$ divise $P(X - U(X)P(X))$. Pour que $P(X)^2$ divise $P(X - U(X)P(X))$ qui, modulo $P(X)^2$, est égal à $P(X)(1 - U(X)P'(X))$, il suffit de choisir $U(X)$ pour que $(1 - U(X)P'(X))$ soit multiple de $P(X)$; l'hypothèse de séparabilité permettant d'écrire une relation de Bezout $U(X)P'(X) + U_1(X)P(X) = 1$, un tel choix est possible et la construction de cette relation et de $U(X)$ par l'algorithme d'Euclide permet d'obtenir un polynôme $DS(X) = X - U(X)P(X)$ de degré au plus $2d - 1$ (polynôme unique sous cette condition). Ce processus pourrait être poursuivi en considérant un polynôme comme $X - U(X)P(X) - V(X)P(X)^2$, mais, comme annoncé, il est préférable d'itérer le morphisme d'algèbre : $X \mapsto DS(X)$. La relation : “$P(X)^2$ divise $P(DS(X))$” montre, par application du morphisme DS, que $P(DS(X))^2$ divise $P(DS^2(X))$.

N.B. : $P(DS(X))^2$ est le carré du polynôme $P(DS(X))$ tandis que $P(DS^2(X))$ est le composé $P(DS(DS(X)))$. Par suite, $P(X)^4$ divise

$P(DS^2(X))$ et, par récurrence, pour tout $k \geqslant 0$, $P(X)^{2^k}$ divise $P(DS^k(X))$. Si maintenant k est un entier vérifiant $2^k \geqslant m$, on voit que l'entier $f = 2^k$ convient et le reste $Q_m(X)$ de la division de $DS^k(X)$ par $P(X)^m$ vérifie $P(Q_m(X)) = 0$ mod. $P(X)^m$ (pour $m > 0$ avec $Q_1(X) = X$) ; $Q_m(X)$ est le polynôme de plus bas degré possédant cette propriété. □

Exemples (les formules données pour tout indice n seront établies plus loin) :

Exemple 1. $P(X) = X(X+1)$, la relation de Bezout s'écrit : $(2X+1)^2 - 4X(X+1) = 1$. Alors, $DS(X) = Q^2(X) = X(1-(2X+1)(X+1)) = -X^2(2X+3)$; les itérés $DS^k(X)$ sont donc à coefficients entiers et, $P(X)$ étant unitaire, il en est de même des polynômes $Q_n(X)$ correspondants.

$$Q_n(X) = (-1)^{n-1}(2n-1)\binom{2n-2}{n-1}X^n\left(\sum_k \binom{n-1}{k}X^k/(n+k)\right) \qquad (\in \mathbb{Z}[X]).$$

Exemple 2. $P(X) = (X^2+1)$, la relation de Bezout est $-\frac{1}{2}X(2X)+(X^2+1) = 1$, $Q_2(X) = X(X^2+3)/2$, $Q_2(X)^2+1 = (1/4)(X^2+4)(X^2+1)2$,

$$Q_n(X) = (2n-1)2^{2-2n}\binom{2n-2}{n-1}\left(\sum_k \binom{n-1}{k}X^{2k+1}/(2k+1)\right)$$

à noter que $2^{2n-3}Q_n(X) \in \mathbb{Z}[X]$.

Exemple 3. $P(X) = X^n+1$, relation de Bezout : $-(X/n)(nX^{n-1}) + (X^n+1) = 1$, $DS(X) = X(X^n+(n+1))/n$.

Exemple 4. $P(X) = (X^2-1)$, relation de Bezout : $(1/2)X(2X) - (X^2-1) = 1$, $DS(X) = Q_2(X) = X(-X^2+3)/2$,

$$Q_n(X) = (2n-1)2^{2-2n}\binom{2n-2}{n-1}\left(\sum_k (-1)^k\binom{n-1}{k}X^{2k+1}/(2k+1)\right)$$

à noter que $2^{2n-3}Q_n(X) \in \mathbb{Z}[X]$.

2.2.

Théorème 2. *Pour tout polynôme $M(X)$ à coefficients dans un corps K de caractéristique 0 et de radical $rM(X)$, il existe un polynôme $D(X)$ à coefficients dans K tel que $M(X)$ divise $rM(D(X))$. Avec les conditions : $(X - D(X))$ est un multiple de $rM(X)$ et $\deg D < \deg M$, D est unique.*

Démonstration. Soit E le corps de décomposition de $M(X) = \prod_i (X - x_i)^{e(i)}$ appartient à $E[X]$. Le lemme chinois associé à l'isomorphisme

$$E[X]/M \cong \oplus_i E[X]/(X-x_i)^{e(i)}$$

montre qu'existe un polynôme unique $D(X)$ de degré inférieur à celui de M vérifiant, pour tout indice i, $D(X) \equiv x_i$ mod. $(X - x_i)^{e(i)}$. Par suite, le produit $\prod_i (D(X) - x_i) = rM(D(X))$ est un multiple de $M(X)$. De plus, le polynôme $D(X) - X$ ainsi construit vérifie $D(x_i) - x_i = 0$ pour tout i et est donc un multiple de $rM(X)$. Soit Δ un second polynôme possédant les mêmes propriétés que D. Comme $rM(X)$ divise $D(X) - X$ et $\Delta(X) - X$, $\Delta(x_i) = D(x_i) = x_i$ pour tout i. Par suite, seul le facteur $\Delta(X) - x_i$ de $\prod_i (\Delta(X) - x_i)$ est divisible par $(X - x_i)^{e(i)}$; donc, $(X - x_i)^{e(i)}$ divise $D(X) - \Delta(X) = (D(X) - x_i) - (\Delta(X) - x_i)$ pour toute valeur de i ; on en déduit que $M(X)$ divise $D(X) - \Delta(X)$, qui est donc nul vu l'hypothèse sur les degrés. Reste à montrer que les coefficients de D appartiennent à K (on peut oublier la condition “coefficients dans K” pour l'unicité). La construction explicite de D s'obtient par celle de polynômes $A_i = A_i(X)$ vérifiant la relation de Bezout : $\sum_i A_i(\prod_{j \neq i}(X - x_j)^{e(j)}) = 1$. À partir de ces A_i (obtenus par la décomposition en éléments simples de la fraction $1/M = \sum_i A_i(X)/(X - x_i)^{e(i)}$, forme polynomiale pratique du lemme chinois), on obtient $D(X) = \sum_i x_i A_i(X)(\prod_{j \neq i}(X - x_j)^{e(j)})$. L'unicité de cette décomposition en éléments simples (*i.e.* celle de la relation liée à la décomposition de $E[X]$ en somme d'idéaux principaux : $\oplus_i(\prod_{j \neq i}(X - x_j)^{e(j)}))$ montre que tout K-morphisme de E transformant un x_i en x_j transforme $A_i(X)$ en $A_j(X)$; comme l'existence d'un tel K-morphisme implique $e(i) = e(j)$, on voit que les coefficients du polynôme $M(\sum_i x_i A_i(X)/(X - x_i)^{e(i)})$ égal à D qu'on a construit sont dans le corps fixe du groupe de Galois $G(E/K)$, corps égal à K en caractéristique nulle. $\square$

Corollaire. (notations du théorème 2) : Soit $DS(X)$ le polynôme associé au radical $rM(X)$ par le théorème 1 ; les restes des divisions par $M(X)$ des itérés $DS^k(X)$ pour k assez grand sont tous égaux à $D(X)$.

2.3. Remarque 1. Le corollaire suit des résultats d'unicité contenus dans les théorèmes 1 et 2 mais, bien sûr, quand $M(X) = rM(X)$, il n'y a pas unicité des polynômes $D(X)$ pour lesquels $M(X)$ divise $rM(D(X))$ (par exemple, si $M(X) = X(X - 1)$, $M(X) = M(1 - X)$).

Remarque 2. Soit $P(X)$ un polynôme séparable ; les arguments d'unicité montrent que les polynômes $DS(X)$ (associé par le théorème 1 à $P(X)$) et $D(X)$ (associé par le théorème 2 au carré $P(X)^2$) coïncident ; les preuves de chacun de ces théorèmes fournissent des constructions explicites basées sur la relation $UP' + U_1P = 1$ pour le premier et la décomposition en éléments simples de $1/P^2$ pour le second, l'avantage de la première preuve étant d'être intrinsèque (on n'introduit aucun surcorps et on ne fait aucun appel à la théorie de Galois). En fait, décomposer $1/P^2$ permet d'écrire directement la relation de Bezout $UP' + U_1P = 1$ et est une alternative à l'algorithme d'Euclide. Ce fait est résumé par la proposition :

Proposition. *Soient* $P(X) = \prod_{1\leqslant i\leqslant r}(X - x_i)$ *un polynôme séparable,*

$$P(X)^{-2} = \sum_i A_i(X)(X - x_i)^{-2} \ (\textit{avec} \deg A_i \leqslant 1)$$

la décomposition de $P(X)^{-2}$*,*

$$U(X)P'(X) + U_1(X)P(X) = 1 \ (\textit{avec} \deg U < r,\ \deg U_1 < r - 1\ )$$

la relation de Bezout entre $P(X)$ *et sa dérivée, alors :*

$$\begin{aligned} U(X) &= \sum_i A_i(X)P(X)/(X - x_i), \\ U_1(X) &= \sum_{i\neq j} x_iA_i(X)P(X)/((X - x_i)(X - x_j)). \end{aligned}$$

Démonstration. $D(X) = \sum_i x_iA_i(X)(P(X)/(X - x_i))^2$,
$U(X) = (X - D(X))/P(X) = \sum_i A_i(X)P(X)/(X - x_i)$,
$1 - U_1(X)P(X) = U(X)P'(X)$
$= \Big(\sum_i A_i(X)P(X)/(X - x_i)\Big)\Big(\sum_i P(X)/(X - x_i)\Big)$
$= \sum_i A_i(X)(P(X)/(X - x_i))^2 + \sum_{i\neq j} x_iA_i(X)(P(X))^2/(X - x_i)(X - x_j)$
$= 1 + P(X)\Big(\sum_{i\neq j} x_iA_i(X)P(X)/(X - x_i)(X - x_j)\Big)$.

$\square$

Exemple. $P(X) = X(X - 1)(X + 1)$,
$(X(X - 1)(X + 1))^{-2} = 1/X^2 + ((-3/4)X + 1)/(X - 1)^2 + ((3/4)X + 1)/(X + 1)^2$,
$D(X) = (X^3/2)(-3X^2 + 5), U(X) = (3/2)X^2 - 1, U_1(X) = (-9/2)X$.

Remarque 3. Les théorèmes 1 et 2 représentent deux variantes du lemme polynomial "au-dessus" de la classique décomposition : semi-simple/nilpotent des endomorphismes des espaces de dimension finie. En effet, soient $M(X)$ le polynôme minimal d'une matrice carrée complexe U, $D(X)$, $N(X) = X - D(X)$ les polynômes associés à M par la construction de la preuve du théorème 2, $d = D(U)$, $n = N(U)$; le théorème 2 montre que $\prod_i(d - x_i\,\mathrm{Id}) = 0$ et que $\prod_i(U - x_i\,\mathrm{Id})$ divise n. Par suite, d, dont le polynôme minimal n'a que des racines simples, est diagonalisable, tandis que le théorème de Cayley-Hamilton montre que n est nilpotent. La décomposition $U = d + n$ est donc la décomposition diagonalisable/nilpotente de U. Quant à son unicité, elle se déduit de l'écriture de d sous la forme $D(U)$. Si $U = \delta + \nu$ où δ est diagonalisable, ν nilpotent et $\delta\nu = \nu\delta$, alors $d = \delta$, $n = \nu$; en effet, comme δ commute avec ν et avec lui-même, δ commute avec U et donc avec $D(U) = d$; les endomorphismes

d, δ et $d-\delta$ sont donc simultanément diagonalisables ; de même, ν commute avec n et la formule du binôme alors applicable montre que $n-\nu$ est nilpotent ; $d-\delta=\nu-n$, à la fois diagonalisable et nilpotent, est donc nul.

2.4. Calcul explicite des polynômes D et DS. Les théorèmes 1 et 2 fournissent des constructions explicites, de nature algorithmique pour le premier, et de la forme "interpolation avec multiplicités" pour le second ; on précise ce dernier point par le théorème 3 suivant :

Théorème 3. *Soit $M(X)=\prod_{1\leqslant i\leqslant r}(X-x_i)^{e(i)}$ un polynôme. Il existe un unique polynôme $D(X)$ de degré $d<\sum_i e(i)$ vérifiant $D(x_i)=x_i$ $(1\leqslant i\leqslant r)$ et dont la dérivée est un multiple de $\prod_{1\leqslant i\leqslant r}(X-x_i)^{e(i)-1}$. Ce polynôme $D(X)$ est le polynôme associé par le théorème 2 à M.*

Démonstration. Soit $D(X)$ le polynôme associé à $M(X)$ par le théorème 2. Il suffit d'établir que D vérifie les hypothèses satisfaites par D, dont on va voir qu'elles caractérisent ce dernier. Par construction, pour $i=1,\dots,r$, $(X-x_i)^{e(i)}$ divise $D(X)-x_i$. Le produit $\prod_{1\leqslant i\leqslant r}(X-x_i)^{e(i)-1}$ divise donc $D'(X)$ et, si $I(X)$ désigne une primitive de $\prod_{1\leqslant i\leqslant r}(X-x_i)^{e(i)-1}$, il existe donc une constante J et un polynôme $K(X)$ de degré au plus $(r-2)$ tels que $D(X)=K(X)(I(X)+J)$. Comme, pour tout i, $D(x_i)=x_i$, les $K(x_i)$ vérifient les $(r-1)$ équations linéaires : $K(x_1)/x_1-K(x_j)/x_j=I(x_1)-I(x_j)$ $(j\neq 1)$ à partir desquelles on détermine K (puis J) par la formule d'interpolation de Lagrange.

□

Quand le nombre des racines est $r=2$, K est une constante ; on explicite les résultats s'exprimant alors en termes de fonctions classiques. Ici, on utilise à la fois les notations du théorème 1 et celles du théorème 2 puisqu'on illustre ces deux théorèmes.

Corollaire 1. Si $P(X)=(X-a)(X-b)$,
$DS(X)=X-(a-b)^{-2}(2X-(a+b))(X-a)(X-b)$.

Démonstration. $P'(X)=2X-(a+b)$ d'où la relation de Bezout $(a-b)^{-2}((2X-(a+b))^2-4(X-a)(X-b))=1$ et le résultat. On peut vérifier les égalités : $DS'(X)=-6(b-a)^{-2}(X-a)(X-b)$ et $(DS(X)-DS(a))(DS(X)-DS(b))=(1/36)(DS'(X))^2(2X+a-3b)(2X+b-3a)=(b-a)^{-4}(X-a)^2(X-b)^2(2X+a-3b)(2X+b-3a)$. □

L'itération du morphisme d'algèbre DS, suivi d'une division euclidienne, permet de calculer (et fournit un procédé algorithmique) les polynômes $D_{\alpha,\beta}$ associés par le théorème 2 aux $(X-a)^\alpha(X-b)^\beta$ (avec cette notation, $DS(X)=D_{2,2}(X)$). Le calcul direct d'un polynôme égal à a (resp. b) au point a (resp. b) et de dérivée proportionnelle à $(X-a)^{\alpha-1}(X-b)^{\beta-1}$ conduit à l'énoncé suivant.

Corollaire 2.

$$D_{\alpha,\beta}(X) = \Big(a\int_X^b (t-a)^{\alpha-1}(t-b)^{\beta-1}\,dt + b\int_a^X (t-a)^{\alpha-1}(t-b)^{\beta-1}\,dt\Big) \times \Big(\int_a^b (t-a)^{\alpha-1}(t-b)^{\beta-1}\Big)^{-1}.$$

De plus, les polynômes définis par : $A_{\alpha,\beta}(X) = (b-a)^{-1}(D_{\alpha,\beta}(X)-a)(X-a)^{-\alpha}$, $B_{\alpha,\beta}(X) = (a-b)^{-1}(D_{\alpha,\beta}(X)-b)(X-b)^{-\beta}$ *vérifient :*

$D_{\alpha,\beta}(X) = bA_{\alpha,\beta}(X)(X-a)^{\alpha} + aB_{\alpha,\beta}(X)(X-b)^{\beta}$,
$1 = A_{\alpha,\beta}(X)(X-a)^{\alpha} + B_{\alpha,\beta}(X)(X-b)^{\beta}$.

Remarque 1. La relation de Bezout précédente $1 = A(X)(X-a)^{\alpha} + B(X)(X-b)^{\beta}$ est un cas d'égalité (exemple : $A_6(X)(1+X)^6 + A_6(-X)(1-X)^6 = 1$ avec $A_6(X) = 2-9(-63X^5+378X^4-938X^3+1218X^2-843X+256)$).

Remarque 2. Le changement de variable $x = a + t(b-a)$ montre que

$$\int_a^b (x-a)^{\alpha-1}(x-b)^{\beta-1}\,dx = (-1)^{\beta-1}(b-a)^{\alpha+\beta-2}\int_0^1 t^{\alpha-1}(1-t)^{\beta-1}\,dt = (-1)^{\beta-1}(b-a)^{\alpha+\beta-2}B(\alpha,\beta),$$

B désignant la fonction "bêta" associée à la fonction Γ par la relation d'Euler $B(x,y) = \Gamma(x)\Gamma(y)(\Gamma(x+y))^{-1}$. En utilisant de plus la fonction "bêta incomplète", on peut également écrire le numérateur de $D_{\alpha,\beta}(X)$; par suite, les résultats s'expriment effectivement, dans le cas de deux racines au plus pour P, par des fonctions classiques.

Remarque 3. Les exposants étant entiers, on peut aussi calculer le terme normalisateur $\int_a^b (x-a)^{\alpha-1}(x-b)^{\beta-1}\,dx$ en restant dans le monde des polynômes ; précisément, on a :

Proposition. $(\alpha+\beta-1)^{-1}(b-a)^{\alpha+\beta-1}$

$$= \binom{a+b-2}{k}\int_a^b (t-a)^k(b-t)^{\alpha+\beta-2-k}\,dt$$

pour tout k $(0 \leqslant k \leqslant \alpha+\beta-2)$.

Démonstration. On écrit
$(b-a)^{\alpha+\beta-1} = \int_a^b (b-a)^{\alpha+\beta-2}\,dt = \sum_k \binom{\alpha+\beta-2}{k}\int_a^b (t-a)^k(b-t)^{\alpha+\beta-2-k}\,dt$
et, par une intégration par parties, on voit que les contributions des $\alpha+\beta-1$ termes de la somme sont égales.

□

Corollaire. $$\int_a^b (x-a)^{\alpha-1}(x-b)^{\beta-1}\,dx = (-1)^{\beta}(1-\alpha-\beta)^{-1}(b-a)^{\alpha+\beta-1}\binom{\alpha+\beta-2}{\alpha-1}^{-1}.$$

(Bien qu'établi pour des valeurs entières, le corollaire s'étend aux réels ; par exemple, en choisissant $a=b=3/2$, on voit que l'intégrale ci-dessus est égale à l'aire d'un demi-cercle de diamètre $[a,b]$ et donc que $B(3/2,3/2)=\Gamma(3/2)^2/2=\pi/8$).

Exemples. (les exemples (notations) sont ceux (celles) annoncés (resp. utilisées) plus haut)

$a=-1, b=0, \alpha=\beta$.

$Q_2(X)=-2X^3-3X^2=-X^2(2X+3)$ $\qquad Q_2(X)+1=(X+1)^2(-2X+1)$

$Q_3(X)=X^3(6X^2+15X+10)$ $\qquad Q_3(X)+1=(X+1)^3(6X^2-3X+1)$

$Q_4(X)=-X^4(20X^3+70X^2+84X+35)$ $\qquad Q_4(X)+1=-(X+1)^4(20X^3-10X^2+4X-1)$

$Q_5(X)=X^5(70X^4+315X^3+540X^2+420X+126)$ $\qquad Q_5(X)+1=(X+1)^5(70X^4-35X^3+15X^2-5X+1)$

$a=-i, b=i, \alpha=\beta$

$Q_2=X(X^2+3)/2$

$Q_3=X(3X^5+10X^3+15)/8$

$Q_4=(5X^7+21X^5+35X^3+35X)/16$

$\vdots$

$Q_{10}=2^{-16}(12155X^{19}+122265X^{17}+554268X^{15}+1492260X^{13}+2645370X^{11}+3233230X^9+2771340X^7+1662804X^5+692835X^3+230945X)$

$\vdots$

$a=-1, b=1, \alpha=\beta$,

$Q_6=(-63X^{11}+385X^9-990X^7+1386X^5-1155X^3+693)/256$

$\vdots$

2.5. Un lien avec les polynômes de Čebičev. Dans la première partie, on a rappelé l'équation fonctionnelle (Θ_n) vérifiée par les polynômes de Čebičev C_n et l'action de la spécialisation $X\mapsto C_m(X)$ compte-tenu de la propriété $C_n\circ C_m=C_{mn}$. Cette propriété s'étend grâce au lemme :

Lemme. *Soit (C_n) une suite de fonctions vérifiant les identités fonctionnelles : $C_n\circ C_m=C_m\circ C_n=C_{mn}$. Soient A un paramètre et (A_n) les fonctions définies par $A_n(X)=AC_m(X/A)$; alors, la même identité fonctionnelle $F_n\circ F_m=F_m\circ F_n=F_{mn}$ est vérifiée par la suite (A_n).*

Démonstration.
$A_{mn}(X) = AC_m(C_n(X/A)) = AC_m(AC_n(X/A)/A) = A_m(AC_n(X/A)) = A_m \circ A_n(X)$. □

Théorème 4. *Soit*

$$\begin{aligned}\Gamma_{2m+1}(X) &= (-1)^m 2iC_{2m+1}(X/2i)\\ &= (2m+1)\Big(\sum_{j\geqslant 0}(2m+1-j)^{-1}\binom{2m+1-j}{j}X^{2m+1-2j}\Big).\end{aligned}$$

$\Gamma_{2m+1}(X)$ est un polynôme unitaire impair à coefficients entiers positifs vérifiant les propriétés :

(i) $\Gamma_{2m+1} \circ \Gamma_{2n+1} = \Gamma_{2n+1} \circ \Gamma_{2m+1} = \Gamma_{(2m+1)(2n+1)}$
(ii) $\Gamma_{2m+1}(X)^2 + 4 = (X^2+4)(\Gamma'_{2m+1}(X)/(2m+1))^2$
(iii) (X^2+4) *divise* $\Gamma_{2m+1}(X) - (-1)^m X$

Par conséquent, la suite d'identités donnée par (ii) est une suite de cas d'égalités pour l'inégalité de Mason, suite laissée stable par les morphismes $X \mapsto \Gamma_{2m+1}(X)$.

Démonstration. Pour montrer que $\Gamma_{2m+1}(X)$ est à coefficients entiers, on applique la remarque

Remarque. Soient k, n des entiers > 0, alors $(n+k)n^{-1}\binom{n}{k}$ et $(2n-k)n^{-1}\binom{n}{k}$ sont entiers. C'est en effet clair : si $(n+k)n^{-1}\binom{n}{k} = (n+k)k^{-1}\binom{n-1}{k-1}$ n'est pas entier, il existe une valuation v_p pour laquelle $v_p(n+k) - v_p(n)$ et $v_p(n+k) - v_p(k)$ sont strictement négatifs ; or, $v_p(n+k) \geqslant \inf(v_p(n), v_p(k))$.

Soit maintenant $\gamma_m(X) = 2iC_m(X/2i)$; le lemme et la partie 1 montrent que $\gamma_n \circ \gamma_m = \gamma_m \circ \gamma_n = \gamma_{mn}$. Comme C_{2m+1}, γ_{2m+1}, Γ_{2m+1} sont impairs, il vient :

$$\begin{aligned}\Gamma_{2m+1}(\Gamma_{2n+1}(X)) &= (-1)^m \gamma_{2m+1}((-1)^n \gamma_{2n+1}(X))\\ &= (-1)^{m+n}\gamma_{(2m+1)(2n+1)}(X) = \Gamma_{(2m+1)(2n+1)}(X)\end{aligned}$$

puisque les entiers $(2mn+m+n)$ et $(m+n)$ sont de même parité. Dans l'identité $C_n(X)^2 - 1 = (X^2-1)(C'_n(X)/n)2$, on spécialise X en $X/2i$ et on multiplie les deux membres par -4 ; en notant que $(\Gamma'_{2m+1}(X))2 = (C'_{2m+1}(X/2i))2$, on en déduit *(ii)*. Pour montrer *(iii)*, il suffit d'établir que $\Gamma_{2m+1}(2i) = (-1)^m 2i$; or, $\Gamma_{2m+1}(2i) = (-1)^m 2iC_{2m+1}(1)$ et $C_{2m+1}(1) = 1$. □

Application. L'exemple 2 qui suit le théorème 1 établit la formule $Q_2(X)^2 + 1 = (1/4)(X^2+4)(X^2+1)^2$ avec $Q_2(X) = X(X^2+3)/2$; autrement dit, Q_2(X) est le polynôme dont l'itération permet de former des facteurs $(1+X^2)$ avec de hautes multiplicités. Dans cette identité, écrite sous la forme $(2Q_2(X))^2+4=(X^2+4)(X^2+1)^2$, on reconnaît l'identité $\Gamma_3(X)^2+4=(X^2+4)(\Gamma_3'(X)/3)^2$ (et aussi la spécialisée par $X\mapsto X^2$ de l'identité $(*)$ de [L] après la translation $X\mapsto 1+X$ rendant applicable le théorème 13). Il y a par conséquent deux modes possibles pour obtenir par itération de hautes multiplicités à partir de l'identité précédente : $X\mapsto Q_2(X)$ et $X\mapsto\Gamma_3(X)$; ainsi : De $(X(X^2+3))^2+4=(X^2+4)(X^2+1)^2$, on déduit au premier rang : avec respectivement $X\mapsto\Gamma_3(X))$ et $X\mapsto Q_2(X))$

$$(X(X^2+3)((X(X^2+3))^2+3)^2+2^2=(X^2+4)(X^2+1)^2((X(X^2+3))^2+1)^2,$$

$$(X(X^2+3)((X(X^2+3))^2+12)^2+2^8=(X^2+4)^2(X^2+1)^4((X(X^2+3))^2+16).$$

3. Exemples d'applications

3.1. Une application directe des constructions de la partie 2 (et du théorème 13 de [L] tel que rappelé dans la partie 1) est de faire naître par itération des cas d'égalité avec des multiplicités élevées. Ainsi :

Théorème 5. *La substitution de $D_{\alpha,\beta}(X)$ à X dans tout cas d'égalité en X dont le radical est multiple de $(X-a)(X-b)$ fait apparaître un nouveau cas d'égalité contenant les facteurs $(X-a)^\alpha$ et $(X-b)^\beta$.*

Démonstration. Soit $(R,S,R-S)$ un cas d'égalité, il suffit de vérifier que la dérivée $D'_{\alpha,\beta}(X)$ (dont le théorème 3 montre qu'elle est proportionnelle à $(X-a)^{\alpha-1}(X-b)^{\beta-1}$) divise le spécialisé $(RS(R-S))(D(X))$; or, ce terme comporte un facteur $(D(X)-a)(D(X)-b)$ qui est un multiple de $(X-a)^\alpha(X-b)^\beta$.

□

Exemple. Dans $(X-a)-(X-b)=b-a$, la spécialisation de X en $D_{2,2}(X)$ conduit à : $(X-a)^2(2X+a-3b)-(X-b)^2(2X+b-3a)=(a-b)^3$.

Le théorème 5 s'applique à tous les cas d'égalité, y compris le trivial $(X+1)/2-(X-1)/2=1$ (ou $X-(X-1)=1$), générateur de tous les autres par spécialisation. En particulier, on peut l'appliquer à toutes les relations de Bezout explicitées dans la partie précédente comme $1=A_{\alpha,\beta}(X)(X-a)^\alpha+B_{\alpha,\beta}(X)(X-b)^\beta$ avec $\deg A_{\alpha,\beta}(X))<\beta$, $\deg B_{\alpha,\beta}(X))<\alpha$ et, par ce procédé itératif, on peut les écrire toutes algorithmiquement et explicitement.

Exemple. En spécialisant $(1/2)(X+1)-(1/2)(X-1)=1$ par le polynôme DS de $(X+1)(X-1)$: $X(-X^2+3)/2$, il vient :

$$-(1/4)(X-2)(X+1)^2+(1/4)(X+2)(X-1)^2=1$$

qui est la relation $(*)$ de [L] où elle joue un rôle important ; en itérant et après division euclidienne, on obtient les solutions $A_3(X)=(1/16)(3X^2-9X+8)$, $A_4(X)=2-5(-5X^3+20X^2-29X+16)$ de l'équation $A_n(X)(1+$

$X)^n + A_n(-X)(1-X)^n = 1$, puis $A_5(X)$, $A_6(X)$ (déjà vu dans la partie 2), $A_7(X)$, $A_8(X)$, et ainsi de suite ...

3.2. De même, à partir des polynômes de Čebičev, on peut construire des polynômes :

$$\mu_{n,[a,b]}(X) = (1/2)(b-a)C_n((b-a)^{-1}(2X-(a+b))) + (1/2)(a+b)$$

qui, substitués à X dans tout cas d'égalité en X dont le radical est multiple de $(X-a)(X-b)$, fait apparaître un nouveau cas d'égalité contenant le facteur $(X-a)(X-b)$ $(\mu'_{n,[a,b]}(X))^2$.

3.3. Dans le domaine des représentations par les formes binaires, les théorèmes 1 et 2 de la partie 2 permettent d'obtenir directement des solutions avec de hautes multiplicités. En utilisant l'exemple 2 qui suit le théorème 1 de (2.1) (et qui jouera un rôle important dans (3.3)), on voit que les identités :

$$(X^3+3XT^2)^2+(2T^3)^2=(X^2+T^2)^2(X^2+4T^2)$$
$$(3X^5+10X^3T^2+15XT^4)^2+(8T^5)^2=(X^2+T^2)^3(9X^4+33(XT)^2+64T^4)$$
$$\vdots$$

conduisent à itérer les transformations

$$(X,T) \mapsto (X^3+3XT^2, 2T^3) \text{ ou } \mapsto (3X^5+10X^3T^2+15XT^4, 8T^5)$$

pour faire apparaître des sommes de carrés (X^2+T^2) à des multiplicités élevées, tout en conservant pour T des facteurs premiers donnés.

3.4. Danilov a utilisé une résolvante de l'identité de Klein pour l'icosaèdre afin d'en déduire des valeurs d'adhérence pour les quantités de la forme $|a^3-b^2|/\sqrt{a}$ (a, b entiers naturels, $a^3 \neq b^2$) et Schinzel a donné le meilleur minorant positif connu pour ces valeurs d'adhérence : $2 \cdot 3^3 \cdot 5^{-5/2}$. Cette résolvante peut s'écrire comme le cas d'égalité suivant : $(X^2-12X+16)^3 - (X^2+4)(X^2-18X+76)^2 = 1728(X-11)$. En substituant $2X$ à X, on retrouve l'identité ($) utilisée dans [L] où l'on montre que ($) est une forme condensée, qu'on déduit en posant

$$X = (2+(11/2)(z^5-z^{-5}))(z^5-z^{-5}-11)^{-1},$$

de l'identité des invariants de Klein pour l'icosaèdre (et donc pour le dodécaèdre), laquelle peut être formulée ainsi (c'est un cas d'égalité puisque le morphisme respecte le critère du théorème 13 de [L] auquel on renvoie pour une écriture plus familière de l'identité de Klein) :

$$\Big(\prod_{1\leqslant i\leqslant 3} A_i\Big)^3 - \Big(\prod_{1\leqslant i\leqslant 5} B_i\Big)^2 = 1728\Big(\prod_{1\leqslant i\leqslant 4} C_i\Big)^5$$

avec :

$A_1(z)=z^8+z^7+7z^6-7z^5+7z^3+7z^2-z+1,\ A_2(z)=z^8-4z^7+7z^6-2z^5+15z^4+2z^3+7z^2+4z+1$
$A_3(z)=z^4+3z^3-z^2-3z+1,\ B_1(z)=z^2+1,\ B_2(z)=z^8-z^6+z^4-z^2+1,$
$B_3(z)=z^4-2z^3-6z^2+2z+1,$
$B_4(z)=z^8-4z^7+17z^6-22z^5+5z^4+22z^3+17z^2+4z+1,$
$B_5(z)=z^8+6z^7+17z^6+18z^5+25z^4-18z^3+17z^2-6z+1,$
$C_1(z)=z^4+3z^3+4z^2+2z+1,\ C_2(z)=z^4-2z^3+4z^2-3z+1,\ C_3(z)=z^2-z-1,\ C_4(z)=z.$

En spécialisant X dans ($) aux points de la suite d'entiers (cf. [L]) : $x_n = (((2\cdot 11\cdot 31+61\sqrt{125})^{4n+3}+(2\cdot 11\cdot 31-61\sqrt{125})^{4n+3})/2-3)^2/5-1$ on obtient pour (x_n^2+1) (resp. $((x_n-3)^2-5)^3$) un terme de la forme $125y_n^2$ (resp. un multiple de 125), d'où la simplification par 125 mise en évidence par Schinzel et la formation d'une différence de la forme $\alpha_n^3-\beta_n^2$. On va relever dans les polynômes cette suite de la façon suivante :

Théorème 6. *Soient* $\Gamma_3(X) = 2Q_2(X) = X(X^2+3)$ *(cf. fin de la partie 2),* $\gamma(X) = \Gamma_3(\Gamma_3(X)) = \Gamma_9(X)$, *et* (DS_n) *la suite des identités (cas d'égalité) déduites de la résolvante* (DS_0) *par itération successive de* $X \mapsto \gamma(X)$ *:*

$$(DS_0)\ (X^2-12X+16)^3-(X^2+4)(X^2-18X+76)^2 = 1728(X-11).$$

Alors, la spécialisation au point 11 dans cette suite (DS_n) *d'identités engendre une suite de différences* $a_n^3-b_n^2 = c_n$ *pour laquelle* $c_n/\sqrt{a_n}$ *tend vers* $2\cdot 3^3\cdot 5^{-5/2}$ *par valeurs inférieures.*

Démonstration. Comme l'indique le théorème 4, l'image par le morphisme $X \mapsto \gamma^n(X)$ de (X^2+4) engendre une suite de cas d'égalité (DS_n) (lesquels satisfont donc au théorème 13 de [L]) contenant le facteur (X^2+4). Cette dernière identité s'écrit : $A_n(X)^3-(X^2+4)B_n(X)^2 = 1728C_n(X)$ (A_n, B_n, C_n à coefficients entiers, le polynôme B_n se présentant lui-même sous la forme d'un produit : facteur, facteur carré, facteur biquadratique...). L'étude de la spécialisation au point 11 est basée sur le lemme (un résultat plus général a déjà été établi dans le *(iii)* du théorème 4 pour la première congruence du lemme) suivant :

Lemme. $\gamma^n(X) = X \bmod. (X^2+4) (n \geqslant 0)$; $\gamma^n(X) = 0 \bmod. \gamma(X)$.

Démonstration du lemme. Modulo (X^2+4), $\Gamma_3(X) = X(X^2+3) = -X$, donc $\gamma(X) = \Gamma_3(\Gamma_3(X)) = \Gamma_3(-X) = -\Gamma_3(X) = X$. □

Au point $X = 11$, les termes (X^2+4) et $C_n(X) = \gamma^n(X)-11$ sont tous deux divisibles par 125 et il en est donc de même de $A_n(X)^3$. D'autre part,tous les termes $\gamma^n(X)$ $(n>0)$ sont multiples de $X(X^2+3)$ et prennent donc au point 11 des valeurs multiples de 4 ; il en est donc de même de $A_n(11) = \left[(X^2-18X+76)\right]_{X=\gamma^n(11)}$. Comme $1728 = 2^6\cdot 3^3$, on voit que l'égalité en entiers :

$$A_n(11)^3 - (11^2+4)B_n(11)^2 = 1728C_n(11)$$

peut être simplifiée par $2^6 \cdot 5^3$. Pour n grand, $1728C_n(11)$ est voisin de $3^3\gamma^n(11)/5^3$ tandis que $(A_n(11)/2^2 \cdot 5)^{1/2}$ est voisin de $\gamma^n(11)/2 \cdot 5^{1/2}$ d'où le quotient annoncé : $2 \cdot 3^3 \cdot 5^{-5/2}$. Pour voir que la limite est atteinte par valeurs inférieures, il suffit de considérer la forme de DS_0 et d'observer que $\gamma^n(11)$ est un entier grand. $\square$

Pour $n = 1$, on retrouve le calcul (cf. [L]) :

$$(2^2{\cdot}2399{\cdot}60659{\cdot}553187221)^3 - (17{\cdot}19{\cdot}61{\cdot}839{\cdot}109441{\cdot}555301{\cdot}181879441)^2 = 3^4{\cdot}5{\cdot}11{\cdot}41{\cdot}3001.$$

Remarque. On rappelle qu'il est impossible de trouver un couple (P,Q) de polynômes tel que le degré de $(P^3 - Q^2)$ soit moitié de celui de P (s'il en était ainsi, en notant d le degré de $(P^3 - Q^2)$, le degré de P serait $2d$ et celui de Q serait $3d$, le nombre de racines du produit $PQ(P^3 - Q^2)$ serait alors $6d$, soit au plus le degré de P^3 (ou celui de Q^2, qui lui est égal), d'où une contradiction avec l'inégalité de Mason). Cette remarque, faite par Davenport dès les années 60, est de fait équivalente avec certaines formes du théorème de Mason (aussi énoncé par Stothers antérieurement et indépendamment). On renvoie à la bibliographie de [L] pour plus de détails.

Bibliographie

[L] M. LANGEVIN, *Imbrications entre le théorème de Mason la descente de Belyi et les différentes formes de la conjecture* (*abc*). J. Th. Nombres de Bordeaux **11** (1999), 91–109.

[P] P. PHILIPPON, *Quelques remarques sur des questions d'approximation diophantienne.* Bull. Aust. Math. Soc., **59**, (1999), 323–334 ; *Addendum* Ibid. **61**, (2000), 167–169.

Michel LANGEVIN
Th des Nombres, I.M. Jussieu & A2X, I.M. Bordeaux
Universite de Bordeaux I
33405 Talence cedex
France
E-mail : lgv@math.u-bordeaux.fr