Journal de Théorie des Nombres
de Bordeaux **11** (1999), 91–109

Imbrications entre le théorème de Mason, la descente de Belyi et les différentes formes de la conjecture (abc)

par Michel LANGEVIN

Résumé. Soient $A, B, C = A + B$ trois éléments de l'ensemble $\mathbb{N}^*$ des entiers >0 (resp. $\mathbb{C}[X]$ des polynômes complexes) premiers entre eux ; on note $r(ABC)$ le produit des facteurs premiers (resp. le nombre des facteurs premiers dans $\mathbb{C}[X]$) du produit ABC. La conjecture (abc) énonce que, pour tout $\varepsilon > 0$, il existe $C_\varepsilon > 0$ pour lequel l'inégalité: $r(ABC) \geq C_\varepsilon S^{1-\varepsilon}$ (avec $S = \max(A, B, C)$) est toujours vérifiée. Le théorème de Mason établit l'inégalité, D (supposé > 0) désignant le plus grand des degrés des polynômes A, B, C : $r(ABC) \geq D + 1$. Les cas de triplets de polynômes où l'égalité $r(ABC) = D + 1$ est vérifiée sont reliés à de nombreux problèmes de théorie des nombres ; les triplets d'entiers qu'ils engendrent conduisent, modulo la conjecture (abc), à des minorations de $r(G(A, B))$ où $G \in \mathbb{Z}[X, T]$ est un polynôme homogène et A, B des entiers premiers entre eux ; dans ces constructions de polynômes et d'entiers, le théorème de Mason et son environnement jouent un rôle-clef.

Abstract. Let $A, B, C = A + B$ be relatively prime polynomials with complex coefficients and maximal degree D (>0). The Mason's theorem implies that $D + 1$ does not exceed the number $r(ABC)$ of distinct roots of the product ABC. Similarly, let $A, B, C = A + B$ be relatively prime positive integers and $S = \max(A, B, C)$. Let $r(ABC)$ be the product of all primes dividing the product ABC. The *abc*-conjecture implies that, for any $\varepsilon > 0$, there exists $C_\varepsilon > 0$ such that the inequality: $r(ABC) \geq C_\varepsilon S^{1-\varepsilon}$ holds for any triple $A, B, C = A + B$ of integers. The cases of equality $r(ABC) = D + 1$ for polynomials $A, B, C = A + B$ are linked to numerous results in number theory; triples of integers generated by these cases lead, by using the *abc*-conjecture, to optimal minoration of $r(G(A, B))$ (where $G \in \mathbb{Z}[X, T]$ is a form and A, B are coprime integers) ; in these polynomial constructions of integers, the role of the Mason's theorem is crucial.

1. Le théorème de Mason, la conjecture (abc)

Dans son Algebra (3° éd.), S. Lang (cf.[L]) présente, avec le commentaire : *Mason started a new trend of thought about polynomials by discovering an entirely new relation ...*, le théorème de Mason ; il s'énonce :

Théorème 1 (cf. [M], [Z]). *Soient $A, B, C = A + B$ trois polynômes d'une variable à coefficients complexes, premiers entre eux deux à deux, D (supposé > 0) le plus grand des degrés des polynômes A, B et*

$$r(ABC) = \#((ABC)^{-1}(0))$$

le nombre des racines complexes du produit ABC. Alors : $r(ABC) > D$.

Cet énoncé est d'abord celui d'une inégalité (pour des polynômes de $\mathbb{C}[X]$, cas de tout cet exposé, mais valable en fait dans tout corps algébriquement clos de caractéristique 0, cf. [He] pour des analogues en caractéristique p) ; mais l'appellation *théorème de Mason* employée dans le texte n'est pas limitée à cette inégalité ; elle inclut la démonstration (cf. §2), ses extensions et surtout la description de l'ensemble CE des cas d'égalités (i.e. ceux pour lesquels $r(ABC) = D + 1$).

Dans un cas d'égalité, on peut voir (cf. ci-dessous) qu'il est impossible que les degrés des trois polynômes intervenant soient les mêmes. Par suite, on écrira les éléments de CE sous la forme de représentants de couples (R, S) de polynômes premiers entre eux, de même degré (noté D dans la suite) et ayant même coefficient dominant. Il s'agira en fait d'une commodité de langage puisqu'on ne distinguera pas (R, S) de $(kR(h(z)), kS(h(z)))$ (k constante $\neq 0$, h homographie). Ensemblistement, CE apparaît donc comme un sous-ensemble des classes de $\mathbb{C}(z)$ modulo les homographies. Un sous-ensemble intéressant (cf. ci-dessous) de CE est CEL (cas d'égalité locaux) formé par les éléments (R, S) pour lesquels $(R - S)$ est séparable.

Voici quelques exemples d'éléments de CEL puis CE :

$$(\beta) \qquad X - (X - 1) = 1$$

$$(*) \qquad (X - 1)^2(X + 2) - (X + 1)^2(X - 2) = 4$$

$$(\wedge) \qquad (X + 1)^3(X - 3) - (X - 1)^3(X + 3) = -16X$$

$$(T + 5)(T - 4)^2(T + 1)^3 - (T - 5)(T + 4)^2(T - 1)^3 = 2^2 3^3 T$$

(combinaison de (*) et (^))

$$(X + 5)(X - 5)^5(X - 4)^2(X + 4)^{10}(X + 1)^3(X - 1)^{15}$$
$$- 2^{10} 3^6 X^3 (A(X) - 2^2 3^4 X)(5A(X) - 2^3 3^4 X)^2$$

$$= A^3(X)(A(X) - 2^3 3^2 5X)^2 (A(X) - 2^4 3^2 X)$$
$$\text{avec } A(X) = X^6 - 2 \cdot 3 \cdot 5X^4 + 3 \cdot 5 \cdot 11X^2 + 2^4 5.$$

On sait le rôle joué par le théorème de Mason dans la genèse de la conjecture (abc) aux conséquences gigantesques et aux vertus structurantes comme l'écrit E. Bombieri :

The abc-conjecture of Masser and Oesterlé is a typical example of a simple statement which can be used to unify and motivate a number of results in number theory, which otherwise would be scattered statements without a common link.

Pour énoncer la conjecture (abc), on introduit sur les entiers la fonction *radical* ou *plus grand diviseur sans facteur carré* qu'on note u ; ainsi, en réservant la lettre p aux nombres premiers, pour tout entier n, $u(n) = \prod_{p|n} p$. Par abus de langage, on conservera cette notation u pour les polynômes ; plus précisément, on écrira : $u(P(X)) = \prod_{P(x)=0}(X - x)$ et donc $r(P(X))$ est le degré de $u(P(X))$. La définition précédente fait de $u(P)$ un polynôme unitaire ; c'est une simple convention de normalisation dans un domaine de nature projective ; en fait, mais ce ne sera pas utile ici, il est des contextes où il convient d'unifier ces deux notations sur un anneau d'entiers, ce qui est rendu possible car les coefficients du polynôme $u(P)$ restent dans le corps engendré par les coefficients de P ; en effet, $u(P)$, dénominateur de l'écriture irréductible de la fraction rationnelle P'/P, est proportionnel au quotient $P/\mathrm{pgcd}(P, P')$.

Conjecture (abc) (Oesterlé-Masser). *Pour tout nombre réel $\varepsilon > 0$, il existe une constante $C_e > 0$ telle que l'inégalité :*

$$u(abc) \geq C_\varepsilon c^{1-\varepsilon}$$

soit vérifiée pour tout triplet $(a, b, c = a + b)$ d'entiers strictement positifs premiers entre eux.

Le but de ce travail est de décrire quelques applications puissantes du théorème de Mason au sens élargi donné plus haut. Les généralisations du théorème au cas de plus de 3 polynômes (travaux de Browkin, Brzezinski, Davies ...) ne seront pas examinées ici, pas plus que les considérations sur les corps de fonctions ayant donné naissance au théorème ou encore que d'autres applications de la conjecture (abc) en logique et qui sont reliées au théorème de Mason (cf. [L.3]).

On examinera ici :

1) - le rôle majeur joué par le théorème de Mason dans la démonstration de l'équivalence entre la conjecture (abc) et la conjecture apparemment plus forte (Form-abc), énoncée plus loin, qui exprime grosso modo la même inégalité que (abc) mais en remplaccant $c = a + b$ par $c = F(a, b)$, F étant un polynôme homogène à coefficients entiers (cf. [L.1],[L.2],[L.4],[L.5]).

2) - le rôle classificateur joué par le théorème de Mason dans les questions diophantiennes se résolvant par des procédés de *descente* (cf. [A-D,L],[L.5]).
3) - le rôle joué par le théorème de Mason pour la construction d'éléments de CE à coefficients entiers, de degré élevé mais dont les facteurs premiers restent de petit degré (le *niveau*) ; de tels exemples sont importants pour l'étude de l'ensemble dérivé de l'ensemble des valeurs prises (avec les notations de la conjecture (abc)) par $\log c/\log(u(abc))$ (cf. [B,F,G,S],[G-N],[L-N]).

Certains des résultats obtenus dans les parties 2 (resp. 3) l'ont été en collaboration avec S. Abgrall-Duchemin (resp. A. Nitaj).

2. Les conjectures (Form-abc) et (abGén)

Conjecture (Form-abc). *Pour tout polynôme homogène de degré f, $F = F(U,V)$ de deux variables à coefficients entiers pour lequel $UVF(U,V)$ est sans facteur multiple et pour tout $\varepsilon > 0$, il existe une constante $K_{F,\varepsilon} > 0$ telle que, quel que soit le couple (a,b) d'entiers premiers entre eux vérifiant $abF(a,b) \neq 0$, on ait*

$$u(abF(a,b)) > K_{F,\varepsilon} \sup(|a|,|b|)^{f-\varepsilon}.$$

Le cas où F est le polynôme (rendu homogène) minimal d'un nombre réel algébrique irrationnel (cas du théorème de Roth) montre la puissance de la conjecture. En fait, le point important est qu'il suffit qu'elle soit vraie pour une $F(U,V)$ convenable (telle que $U+V$) pour que (Form-abc) soit vraie pour toute F . Mais, l'écriture directe du résultat s'obtient en rompant la symétrie des rôles joués par a et b ; c'est la suivante :

Conjecture (abGén.). *Pour tout polynôme homogène de degré g, $G = G(U,V)$ de deux variables à coefficients entiers pour lequel $VG(U,V)$ est sans facteur multiple et pour tout $\varepsilon > 0$, il existe une constante $K'_{G,\varepsilon} > 0$ telle que, quel que soit le couple (a,b) (avec $a \geq b \geq 1$) d'entiers premiers entre eux vérifiant $G(a,b) \neq 0$, on ait :*

$$u(G(a,b)) > K'_{G,\varepsilon} a^{g-1-\varepsilon}/u(b).$$

Dans la preuve de l'implication (abc) $\Longrightarrow$ (abGén.), le théorème de Mason (et son environnement) intervient deux fois :
1°- Pour traiter le cas où $G(U,V)$ se décompose en produit de facteurs linéaires sur les entiers.
2°- Pour se ramener du cas général au cas précédent.

Le 1° utilise la *forme locale* du théorème 1 (celle de l'auteur depuis le début des années 90), laquelle est en fait à l'infini une conséquence du théorème de Mason :

Théorème 2. *Soient $R = R(X)$ et $S = S(X)$ deux polynômes premiers entre eux, x un nombre complexe vérifiant $R(x) = S(x)$ et $\omega_x = \omega_x(R - S)$ la multiplicité de x en tant que racine du polynôme $(R - S)$. Alors, les inégalités (optimales) ci-dessous sont vérifiées :*
$\omega_x \leq r(RS)$ et, si les degrés de R et S sont égaux, $\omega_x + 1 \leq r(RS)$.

Exemple. $R(X) = (1-X)^2(1+2X)$, $S(X) = -(1+X)^2(1-2X)$, $R(X) - S(X) = 4X^3$, $x = 0$, $\omega_x + 1 = 4 = r(RS)$.
Si x est à l'infini, ce qui suppose que R et S soient de même degré D, $\omega_\infty(R-S) = D - d(R-S)$; le théorème 2 reste valable et se déduit comme annoncé du théorème 1 ; par substitution de $X-1$ à la place de X, l'exemple précédent ramène à (*) :

$$R(X) = (1-X)^2(2+X), \quad S(X) = -(1+X)^2(2-X),$$
$$R(X) - S(X) = 4, \quad \omega_x + 1 = 4 = r(RS).$$

Le 2° utilise un résultat semblant éloigné du théorème de Mason mais faisant intervenir lui aussi la fonction *nombre de racines.* En clair, le résultat suivant de [L.1] cache sous des habits très simples la *descente de Belyi* :

Théorème 3. *Soient P et Q deux polynômes d'une variable. Alors,*

$$r(P(Q)) \geq (r(P) - 1)d(Q) + 1.$$

Et il y a égalité si et seulement si Q' divise $P(Q)$.

3. Preuve du théorème 1 et liens avec le §2

Pour voir que les théorèmes 2 et 3 sortent de la même source, il faut *bien* montrer le théorème 1 (cf. [L.5]) :

Théorème 4. (i) *Pour tout couple (R, S) de polynômes premiers entre eux tel que $RS(R - S) \neq 0$, le produit $RS(R - S)$ divise le produit*

$$u(RS(R - S))(R'S - RS').$$

(ii) *Pour tout couple (R, S) de polynômes premiers entre eux de degré maximal D, $r(RS(R - S)) \geq D + 1$ (cf. théorème 1).*
(iii) *On conserve ci-dessous les hypothèses de* (ii). *Il y a égalité dans* (ii) *si et seulement si le polynôme (sic, cf.* (i)*)*

$$u(RS)(R'/R - S'/S)((R - S)/u(R - S))^{-1}$$

est constant, ou encore si et seulement si

$$(R'S - S'R)^{-1}(0) \supset (RS(R - S))^{-1}(0).$$

Démonstration. (i) Il suffit de comparer la multiplicité d'une racine x de $RS(R - S)$ dans chacun des deux membres (observer que $R(x) - S(x) = 0$ implique $R(x) = S(x) \neq 0$); on voit qu'en fait ces multiplicités sont égales mais d'autres racines peuvent apparaître dans le wronskien $(R'S - RS')$.

(ii) On applique (i) et on compare les degrés des deux membres. On obtient immédiatement l'inégalité $d(R-S) \leq r(RS(R-S)) - 1$ et on conclut donc si $d(R-S) = D$. Lorsque $d(R) = d(S) = D > d(R-S)$, on conclut également puisqu'alors $d(R'S - S'R) = d((R'-S')S - S'(R-S)) = D + d(R-S) - 1$.
N.B. : Si R, S et $(R-S)$ sont de degré D, alors $d(R'S - S'R) \leq D + d(R-S) - 2$ et l'inégalité du théorème 1 est donc améliorée dans ce cas. Par suite, si $r(RS(R-S)) = D+1$, les polynômes $R, S, R-S$ ne peuvent pas être de même degré.
(iii) se déduit de ce qui précède. □

3.1. **Développement du théorème 4 en vue du** $1°$. On conserve les notations du théorème 4. Il y a égalité si $(R'S - S'R)^{-1}(0) \supset (RS(R-S))^{-1}(0)$ et seulement dans ce cas. Une condition suffisante pour qu'il en soit ainsi est que la dérivée logarithmique $(R'/R - S'/S)$ (s'écrivant toujours sous la forme $N/u(RS)$) soit de numérateur N constant et on vérifie aisément sur le (i) du théorème 4 qu'il y équivalence de ce cas avec le *cas local* vu plus haut (i.e. $(R-S)$ séparable).

Ce *cas local* est un cas de caractérisation facile, lisible sur le radical $r(RS)$; en effet :

Théorème 5 (cf. [L.1]). (i) *Soient (R,S) un cas d'égalité local et $P = u(RS)$; alors, pour tout couple (x, y) de racines de P, le rapport $P'(x)/P'(y)$ est rationnel.*
(ii) *Soit P un polynôme séparable tel que, pour tout couple (x, y) de racines de P, le rapport $P'(x)/P'(y)$ soit rationnel. Alors, il existe une constante N (unique à des conditions évidentes de normalisation près) telle que N/P apparaisse comme la dérivée logarithmique d'une fraction rationnelle R/S et le couple(R,S) est un cas d'égalité local vérifiant $P = u(RS)$.*

C'est essentiellement ce théorème 5 qui permet de résoudre le 1° dans la preuve de $(abc) \Longrightarrow (ab\text{Gén.})$. En effet, il montre que, pour tout polynôme P à coefficients et racines rationnels, il existe un élément (R, S) de CEL, à coefficients entiers, tel que P divise RS. On y reviendra plus loin en montrant qu'on peut, grâce au théorème 3, omettre l'hypothèse : *racines rationnelles.*

3.2. **Développement du théorème 4 en vue du** $2°$. La remarque importante est que le wronskien $W = RS' - R'S$ apparaissant naturellement dans la preuve du théorème 4 ne dépend que de la droite projective (faisceau) Φ des polynômes engendrée par R et S . Ce qu'exprime le (i) du théorème 4 est que, pour tout élément P de Φ, $P/u(P)$ divise W . En fait, on vérifie aisément la formule suivante (cf. [L.5]) où $c \neq 0$ est une constante :

Théorème 6.

$$W = c \prod_{P \in \Phi} \frac{P}{u(P)}$$

(i.e., à une constante multiplicative $\neq 0$ *près,* $W = \prod_{P\in\Phi} P/u(P)$*).*

Il s'agit clairement d'un produit fini. Pour écrire ce résultat - c'est le *bon* théorème de Mason (mais il est moins original ainsi) - de façon algorithmiquement utilisable, il est préférable de le reformuler (on abrège résultant et discriminant en Rés et Disc, l'indéterminée considérée est rappelée en indice) :

Corollaire. *Soient* $(R, S) = (R(X), S(X))$ *et le résultant :*

$$\rho(X) = \text{Rés}_Y(u_Y(\text{Disc}_X(R + YS)), R + YS) \ ;$$

alors, à un coefficient multiplicatif $\neq 0$ *près,* $\rho/u(\rho) = W(R, S) = (RS' - R'S)$*.*

Pour revenir du langage ci-dessus à celui du théorème de Mason, on introduit un polynôme homogène à 2 variables $G(U, V)$ à coefficients complexes sans facteur multiple de degré g . La valeur prise $G(R, S)/u(G(R, S)$ lorsque (R, S) est un couple de polynômes apparaît, puisqu'on travaille sur les complexes, comme un certain sous-produit de $\prod_P P/u(P)$ (P décrivant le faisceau des polynômes engendré par R et S) d'où le prolongement naturel suivant du théorème 3 (cf. [L.5]) :

Théorème 6-bis. $G(R, S)/u(G(R, S)$ *divise* $W(R, S)$ *et il y a égalité si et seulement si* $W(R, S)$ *divise* $G(R, S)$.

Le théorème 6-bis redonne le (i) de la preuve du théorème de Mason. En particulier, pour (ii), il vient :

Théorème 6-ter. $r(G(R, S)) \geq (g - 2)D + 1$.

Ce théorème 6-ter énoncé avec la forme projective de la fonction r est la généralisation naturelle du théorème de Mason et l'analogue polynomial du passage de (*abc*) à (*ab*Gén). Cet énoncé ne résout pas la question de J. Oesterlé sur le cas où $G(U, V)$ a ses coefficients dans $\mathbb{C}[X]$, a-t-on : $r(G(R, S)) \geq (g - 2)D - K(G)$?

On laisse de côté cette question conjecturale établie seulement dans des cas très spécifiques. On revient au théorème 6-ter pour voir le lien annoncé avec le 2°. Il est clair que les énoncés affines ou semi-affines utilisés jusqu'à présent ne sont que des *traductions* (importantes pour l'exploitation algorithmique) de résultats projectifs. En bref, les théorèmes 6, 6-bis, 6-ter sont des conséquences de la réécriture suivante du théorème 3 (cf. [L.5]) :

Théorème 7. (i) *Soient* $F(U, V)$*,* $R(U, V)$*,* $S(U, V)$ *trois polynômes homogènes de deux variables non nuls. On suppose* F *sans facteur multiple et* R*,* S *sans facteur commun. Alors,*

$F(R(U,V),S(U,V))$ *divise le produit*

$$u(F(R(U,V),S(U,V))) \times \mathrm{Jacobien}_{U,V}(R,S).$$

et il y a égalité si et seulement si

$$\mathrm{Jacobien}_{U,V}(R,S) \textit{ divise } F(R(U,V),S(U,V)).$$

(ii) *Soient $F(U,V)$, $R(U,V)$, $S(U,V)$ trois polynômes homogènes de deux variables non nuls. On suppose R, S sans facteur commun et de même degré D. Alors,*

$$r(F(R(U,V),S(U,V))) - 2 \geq (r(F) - 2)D.$$

Et il y a égalité si et seulement si $F(R(U,V),S(U,V))$ est un multiple de $\mathrm{Jacobien}_{U,V}(R,S)$.

Exemple. $F(U,V) = UV(U-V)$, $R(U,V) = (U+2V)(U-V)^2$, $S(U,V) = (U-2V)(U+V)^2$. Alors,

$$F(R(U,V),S(U,V)) = 4(U-2V)(U+V)^2(U+2V)(U-V)^2V^3$$

est un multiple du jacobien $18V^2(U^2 - V^2)$, et

$$r(F(R(U,V),S(U,V))) - 2 = 5 - 2 = (r(F) - 2)D = (3-2)3.$$

Une application du théorème 7 se trouve dans la possibilité d'aller d'un élément de CE à un autre par spécialisation (cf. théorème 9, §3). A vrai dire, tout se ramène toujours à une spécialisation dans l'identité basique

$$(\beta) \qquad X - (X-1) = 1$$

de CE ; ce qu'exprime le théorème 7 est que la spécialisation (en vocabulaire affine) de X en R/S permet de rester dans CE si et seulement si le wronskien (ou le jacobien en termes projectifs) divise le produit des facteurs obtenus. Cette première étape est l'étape triviale dans la structure arborescente prise par CE. C'est autour de cette structure et des étapes suivantes que s'articule la suite de l'exposé (cf. §5) puisqu'elle est un des aspects majeurs du théorème de Mason comme on le verra (on laissera de côté les applications du théorème 1 au cas des corps des fonctions et celles déduites de l'interprétation de l'application associant $R(z)/S(z)$ à z en termes de revêtement).

4. Esquisse de preuve de $(abc) \Longrightarrow (ab\text{Gén})$

Soit $G \in \mathbb{Z}[X,T]$ un polynôme homogène de degré g sans facteur multiple tel que $G(X,0) \neq 0$. On suppose d'abord que G se décompose en produit de facteurs linéaires à coefficients entiers. Soit $P_1(X) = G(X,1)$, lequel est séparable et aussi de degré g. On construit par le théorème 5 un couple (R,S) appartenant à CEL et vérifiant $u(RS) = P_1$ à partir duquel on reconstitue des polynômes homogènes HR et HS de même degré et de différence $HR(X,T) - HS(X,T) = T^{d(R-S)}\Delta(X,T)$. Soient maintenant des entiers $a, b \neq 0$ premiers entre eux tels que $G(a,b) \neq 0$; on peut supposer sans perte de généralité, puisque l'étude porte sur $G(a,b)$, que $0 < b \leq a$ (remplacer au besoin G par son symétrique ou modifier les signes de ses coefficients). Les diviseurs communs des entiers $HR(a,b)$, $HS(a,b)$ et $HR(a,b) - HS(a,b) = b^{d(R-S)}\Delta(a,b)$ sont majorés indépendamment de a et b et on peut donc appliquer la conjecture (abc) (un choix de ε étant fait et compte-tenu de ce pgcd) au triplet :

$$(HR(a,b), HS(a,b), b^{d(R-S)}\Delta(a,b)).$$

Il vient :

$$\begin{aligned} u(bG(a,b))|\Delta(a,b)| &\geq u(HR(a,b)HS(a,b)b^{d(R-S)}\Delta(a,b)) \\ &\gg_{\varepsilon,G} \sup(|HR(a,b)|, |HS(a,b)|)^{1-\varepsilon}. \end{aligned}$$

On conclut en traitant chacun des termes de l'inégalité précédente comme suit (cf. [L.2], [L.4]) :

- pour ceux à majorer (i.e. $|\Delta(a,b)|$) qui sont de la forme $|V(a,b)|$ où V est homogène de degré v on utilise l'inégalité $|V(a,b)| \leq a^v ||V||$ (avec $||V|| = \sup_{0\leq z\leq 1} |V(1,z)|$).
- pour celui à minorer :

$$\sup(|HR(a,b)|, |HS(a,b)|) \geq a^D \inf_{0\leq z\leq 1} (\sup(|HR(1,z)|, |HS(1,z)|)),$$

on applique le lemme classique de K. Mahler permettant de minorer

$$\inf_{z\in\mathbb{C}} (\sup(|A(z)|, |B(z)|))$$

par une constante ne dépendant que des coefficients des polynômes sans racine commune A et B.

Reste maintenant à se ramener au cas qu'on vient de résoudre : racines rationnelles pour $G(X,1)$.

L'idée générale est la suivante : Soit $G \in \mathbb{Z}[X,T]$ un polynôme homogène de degré g sans facteur multiple tel que $G(X,0) \neq 0$. On se ramène d'abord en affine en considérant $G_1(X) = G(X,1)$. On va construire deux polynômes auxiliaires, le premier $A(X)$ à racines rationnelles, le second Q à coefficients entiers, tels que le composé $A(Q)$ soit un multiple du produit $G_1 Q'$. A partir du polynôme $A(X)$ à racines rationnelles, on pourra remonter à un couple (R_1, S_1) de CEL et il suffira de former $(R_1(Q), S_1(Q))$, qui reste dans CEL, pour obtenir un multiple $u(R_1(Q)S_1(Q))$ de G_1 qui suffira pour conclure. Ce programme est résumé par le théorème suivant :

Théorème 8. *Soit P un polynôme à coefficients rationnels. Il existe un couple (R,S) de polynômes à coefficients rationnels de même degré D, vérifiant $r(RS) = D - d(R-S) + 1$ et tel que P divise le produit RS.*

Autrement dit, pour tout polynôme P à coefficients entiers, il existe un élément (R,S) de CEL tel que P divise RS.

Exemple. Soit $P(X) = X^3 - 6X^2 + 7X + 7$; le calcul déduit de la preuve du théorème précédent (cf. ci-dessous) conduit à :

$$A(X) = X(X+500)(X+675), \qquad Q(X) = -27((X-2)(X^2-4X-1))^2.$$

Il vient:

$$\begin{aligned} A(Q(X)) &= -27((X-2)(X^2-4X-1))^2 \\ &\quad \times(-27((X-2)(X^2-4X-1))^2+500) \\ &\quad \times(-27((X-2)(X^2-4X-1))^2+675) \\ &= (-27)^3((X-2)(X^2-4X-1))^2 \\ &\quad \times(3X^2-12X-8)(3X^2-12X+7)^2 \\ &\quad \times(X^3-6X^2+7X+7)(X^3-6X^2+7X-3). \end{aligned}$$

Enfin, $Q' = -54(3X^2-12X+7)(X^2-4X-1)(X-2)$ est un facteur du terme précédent et le quotient résiduel est bien un multiple de P.

Pour ce programme, on utilise les résultats intermédiaires suivants conséquences de l'ensemble *théorème de Mason* (cf. §1 et [L.5]) :

Théorème 9. *Pour tout polynôme Q , soit $Q^\sharp(X) = \mathrm{Disc}_Y(Q(Y) - X)$. Alors :*

$$Q'(X) = u(Q^\sharp)(Q(X))/u(Q^\sharp(Q(X))).$$

De plus, tout polynôme P tel que Q' divise $P(Q)$ est un multiple de $u(Q^\sharp)$.

Démonstration. Soit x une racine de Q', donc une racine multiple de $Q(Y)-Q(x)$; par suite, $(X - Q(x))$ est un facteur de $Q^\sharp(X)$ donc de $u(Q^\sharp(X))$; réciproquement, par construction, $Q^\sharp(X)$ ne comporte pas d'autre facteur ; le reste de l'énoncé est clair, l'écart d'ordres de multiplicité de la racine x des polynômes en Y, $Q(Y) - Q(x)$ et $Q'(Y)$, étant 1. □

Exemples (N.B. : la convention de normalisation du §1 n'est pas respectée ici).

1) - Soit $Q(X) = X^3 + pX + q$; alors, $Q^\sharp(X) = 4p^3 + 27(q - X)^2$,

$$u(Q^\sharp(X)) = \begin{cases} 4p^3 + 27(q-X)^2 \text{ si } p \neq 0, \\ 27(q-X) \text{ si } p = 0\ ; \end{cases}$$

$$u(Q^\sharp)(Q(X)) = \begin{cases} 4p^3 + 27X^2(X^2+p)^2 = (3X^2+p)^2(3X^2+4p) \\ \hfill \text{si } p \neq 0, \\ 27X^3 \text{ si } p = 0\ ; \end{cases}$$

$$u(Q^\sharp(Q(X))) = \begin{cases} (3X^2+p)(3X^2+4p) \text{ si } p \neq 0, \\ 27X \text{ si } p = 0. \end{cases}$$

2) - Soit $Q(X) = X^3 - 6X^2 + 7X + 7$; alors,

$$u(Q^\sharp(X)) = Q^\sharp(X) = -27X^2 + 270X - 175,$$

tandis que

$$\begin{aligned} u(Q^\sharp)(Q(X)) &= -(3X^2-12X-8)(3X^2-12X+7)^2, \\ u(Q^\sharp(Q(X))) &= -(3X^2-12X-8)(3X^2-12X+7). \end{aligned}$$

3) - Soit $Q(X) = X^3 - 6X^2 + 7X - 3$; alors,

$$u(Q^\sharp(X)) = Q^\sharp(X) = -27X^2 - 270X - 175,$$

tandis que

$$\begin{aligned} u(Q^\sharp)(Q(X)) &= -(3X^2-12X-8)(3X^2-12X+7)^2, \\ u(Q^\sharp(Q(X))) &= -(3X^2-12X-8)(3X^2-12X+7). \end{aligned}$$

(N.B.: les coïncidences qu'on peut observer entre 2) et 3) ne sont pas fortuites, en effet, la somme des racines du polynôme $Q^\sharp$ dans le cas 2) (resp. 3)) est -10 (resp. 10)).

Soient maintenant Q un polynôme et β l'application définie par $\beta(Q) = u(Q^\sharp)$. En fait, il conviendrait de chasser les éventuelles racines rationnelles de $\beta(Q)$ en ne conservant que ses facteurs premiers de degré au moins 2 ; on ne le fera pas ici pour simplifier l'exposé. Par construction, $d(\beta(Q)) < d(Q)$. En itérant cette opération, on voit qu'existe un rang g tel que $\beta^g(Q)$ soit de degré 1. D'autre part, les coefficients des polynômes $\beta^i(Q)$ appartiennent au corps engendré par les coefficients de Q. On note $\gamma(Q)$ (resp. $\zeta_Q(X)$) le composé des polynômes (resp. le polynôme suivant dont les racines sont éléments du corps des coefficients de Q) :

$$\gamma(Q)(X) = \beta^g(Q) \circ \beta^{g-1}(Q) \circ \cdots \circ \beta(Q) \circ Q(X).$$

$$\begin{aligned} \zeta_Q(X) = u(X(X - \beta^g(Q)(0))(X - \beta^g(Q) \circ \beta^{g-1}(Q)(0)) \cdots \\ \cdots (X - \beta^g(Q) \circ \beta^{g-1}(Q) \circ \cdots \circ \beta(Q)(0))). \end{aligned}$$

Alors, avec ces notations, on obtient le résultat suivant :

Théorème 10. *Le produit* $u(Q)\gamma(Q)'$ *divise* $\zeta_Q(\gamma(Q))$.

Démonstration. Par construction, $\zeta_Q(\gamma(Q))$ est un multiple des $(g+1)$ polynômes en X :

$$\gamma(Q) = \beta^g(Q) \circ \beta^{g-1}(Q) \circ \cdots \circ \beta(Q) \circ Q \ , \ \beta^{g-1}(Q) \circ \cdots \circ \beta(Q) \circ Q \ , \ \ldots \ , \ Q.$$

D'autre part, Q' divise $\beta(Q) \circ Q$ et donc $(\beta^i(Q))'$ divise $\beta^{i+1}(Q) \circ \beta^i(Q)$ pour tout entier i.

On en déduit que $(\beta^i(Q))' \circ \beta^{i-1}(Q) \circ \cdots \circ \beta(Q) \circ Q$ divise $\beta^{i+1}(Q) \circ \cdots \circ \beta(Q) \circ Q$.

Ces deux remarques montrent que toute racine de $\gamma(Q)'$ est une racine de $\zeta_Q(\gamma(Q))$ ce qui suffit pour établir la première partie du résultat d'après le théorème 4.

D'autre part, le même résultat montre que

$$\zeta_Q(\gamma(Q))/\gamma(Q)' = u(\zeta_Q(\gamma(Q))),$$

lequel est un multiple de $u(Q)$ d'après la première partie de la démonstration. $\square$

Exemples.
1) - Soit $Q(X) = X^3-6X^2+7X+7$; alors, $\beta(Q)(X) = -27X^2+270X-175$, $\beta(Q)(0) = -175$, de même, en négligeant le facteur 108, $\beta^2(Q)(X) = (X-500)$, $\beta^2(Q)\circ\beta(Q)(0) = -675$. Il vient donc :

$$\begin{aligned}
\gamma(Q) &= (-27Q^2+270Q-175)-500\\
&= -27((X-2)(X^2-4X-1))^2,\\
\zeta_Q(X) &= X(X+500)(X+675),\\
\gamma(Q) &= -27((X-2)(X^2-4X-1))^2,
\end{aligned}$$

$$\begin{aligned}
\zeta_Q(\gamma(Q)) &= -27((X-2)(X^2-4X-1))^2\\
&\qquad\times(-27((X-2)(X^2-4X-1))^2+500)\\
&\qquad\times(-27((X-2)(X^2-4X-1))^2+675)\\
&= (-27)^3((X-2)(X^2-4X-1))^2(3X^2-12X-8)\\
&\qquad\times(3X^2-12X+7)^2(X^3-6X^2+7X+7)\\
&\qquad\times(X^3-6X^2+7X-3)
\end{aligned}$$

Enfin,

$$\gamma(Q)' = -54(3X^2-12X+7)(X^2-4X-1)(X-2)$$

est un facteur du terme précédent et le quotient résiduel est bien un multiple de $Q = u(Q)$.

2) - De même, $Q(X) = X^3-6X^2+7X-3$; alors, $\beta(Q)(X) = -27X^2-270X-175$, $\beta(Q)(0) = -175$ et, en négligeant le facteur 108, $\beta^2(Q)(X) = (X-500)$, $\beta^2(Q)\circ\beta(Q)(0) = -675$. On retrouve :

$$\begin{aligned}
\zeta_Q(X) &= X(X+500)(X+675),\\
\gamma(Q) &= -27((X-2)(X^2-4X-1))^2,
\end{aligned}$$

et

$$\begin{aligned}
\zeta_Q(\gamma(Q)) &= -27((X-2)(X^2-4X-1))^2\\
&\qquad\times(-27((X-2)(X^2-4X-1))^2+500)\\
&\qquad\times(-27((X-2)(X^2-4X-1))^2+675)\\
&= (-27)^3((X-2)(X^2-4X-1))^2(3X^2-12X-8)\\
&\qquad\times(3X^2-12X+7)^2(X^3-6X^2+7X+7)\\
&\qquad\times(X^3-6X^2+7X-3).
\end{aligned}$$

Enfin, le produit $Q\gamma(Q)'$ est un facteur du terme précédent.

5. Autres applications du théorème de Mason

5.1. Le théorème de Mason est un *outil de classification.* L'idée est la suivante : De multiples résultats de théorie des nombres se déduisent d'identités algébriques ou de spécialisations convenables à l'intérieur d'identités algébriques. Regrouper ces résultats en fonction de l'identité algébrique leur ayant donné naissance est une *classification* et l'ensemble des cas d'égalité CE (ou cas d'égalité locaux CEL) fournit un tel outil de référence.

On va illustrer ce discours par quelques exemples.

1) - (avec S. Abgrall-Duchemin, cf. [A-D, L])

($) $\qquad ((X-3)^2-5)^3-(X^2+1)(X^2-9X+19)^2 = 3^3(2X-11)$

peut être exploité dans deux directions étrangères :

- D'une part, la spécialisation

$$\begin{aligned} X &= (11Z^{10}+4Z^5-11)/(2Z^{10}-22Z^5-2) \\ &= (11(Z^5-Z^{-5})/2+2)/(Z^5-Z^{-5}-11), \end{aligned}$$

(qu'on peut décomposer en $X = (11U+2)/(2U-11)$, où $U = (V-V^{-1})/2$ et $V = Z^5$) dans ($) conduit à la relation :

$$G^3 - H^2 = 1728F^5$$

où

$$\begin{aligned} F(V,W) &= VW(V^{10}-11V^5W^5-W^{10}), \\ G(V,W) &= (V^{20}+228V^{15}W^5+494V^{10}W^{10}-228W^{15}+W^{20}) \\ &= -11^{-2}\mathrm{Hessien}(F), \\ H(V,W) &= (V^{10}+W^{10})(V^{20}-522V^{15}W^5-10006V^{10}W^{10}+522W^{15} \\ &\qquad +W^{20}) \\ &= -(20)^{-1}\mathrm{Jacobien}(F), \end{aligned}$$

sont les invariants de Klein pour l'icosaèdre. Cette relation (*syzygie* dont ($) est une *résolvante*), écriture projective d'un élément de CE , a été utilisée par F. Beukers (cf. [B]) pour traiter l'équation diophantienne : $x^5+y^3=z^2$ (où les inconnues x,y,z vérifient $\mathrm{pgcd}(x,y,z)=1$).

- D'autre part, des spécialisations entières convenables dans ($) (qu'on construit à partir du cas d'égalité (*) $(X-1)^2(X+2)-(X+1)^2(X-2)=4$ du §1) conduisent au résultat de Danilov et Schinzel :

Il existe une infinité de couples (a,b) d'entiers vérifiant :

$$0 < |a^3-b^2| < 2\cdot 3^3\cdot 5^{-2}\sqrt{a/5},$$

montrant explicitement le caractère optimal de la conjecture de Hall :

Il existe une constante C positive vérifiant, pour tout couple (a,b) d'entiers naturels avec $a^3 \neq b^2$, $|a^3 - b^2| > C\sqrt{a}$.

Par exemple, la relation pour laquelle le quotient $|a^3 - b^2|/\sqrt{a}$ vaut $0,96598136437\ldots$ (inférieur à $0,9659813662799 < 2.3^3.5^{-5/2}$) :

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

se déduit du choix $X = X_0$ dans ($) avec :

$$X_n = (((2 \cdot 11 \cdot 31 + 61\sqrt{125})^{4n+3} + (2 \cdot 11 \cdot 31 - 61\sqrt{125})^{4n+3})/2 - 3)^2/5 - 1 ;$$

la suite (X_n) fournit le point d'accumulation $2 \cdot 3^3 \cdot 5^{-5/2}$ pour $|a^3 - b^2|/\sqrt{a}$ (le plus petit à ce jour) mais on connaît des points isolés meilleurs à ce titre comme $|2^3 - 3^2|/\sqrt{2}$ et 11 autres exemples jusqu'à $(23 \cdot 197 \cdot 6221)^3 - (3 \cdot 19 \cdot 491 \cdot 5347183)^2 = -2 \cdot 5 \cdot 109$, $(2 \cdot 5 \cdot 109/\sqrt{23 \cdot 197 \cdot 6221} = 0,20530...)$.

En fait, la conjecture (abc) implique (cf. [L.3]) :

$$u(a^3 - b^2) \gg_{\varepsilon,\mu} (\sqrt{a})^{1-\varepsilon}$$

où $\mathrm{pgcd}(a, b \geq \mu)$ et $|a^3 - b^2| \gg_\varepsilon (\sqrt{a})^{1-\varepsilon}$ (sans restriction).

2) - les travaux de Beukers évoqués ci-dessus ne concernent pas seulement l'équation $x^5 + y^3 = z^2$. En fait, toutes les équations $Ax^p + By^q = Cz^r$ dans le cas $p^{-1} + q^{-1} + r^{-1} > 1$ (A, B, C entiers $\neq 0$ donnés, x, y, z inconnues entières $\neq 0$ premières entre elles) qui admettent une solution en ont une infinité d'autres, lesquelles sont décrites par une famille finie de paramétrisations polynomiales liée aux invariants de Klein des polyèdres réguliers [N.B. : L'hypothèse $p^{-1} + q^{-1} + r^{-1} > 1$ exclut toute contradiction avec la conjecture (abc) de laquelle se déduit notamment la finitude de l'ensemble des solutions de l'équation $Ax^p + By^q = Cz^r$ lorsque $p^{-1} + q^{-1} + r^{-1} < 1$, finitude prouvée directement par Darmon et Granville]. La classification des solutions par spécialisation dans des éléments de CE convenables donne lieu à des résultats de descente déduits de calculs de D. Zagier comme le suivant :

Théorème 11 (cf. [L.5]). (i) *Toutes les solutions de l'équation diophantienne $a^4 + b^2 = c^3$ (avec a, b, c entiers non nuls premiers entre eux) s'obtiennent par des spécialisations rationnelles convenables dans l'identité :*

$$(*) \qquad (X-1)^2(X+2) - (X+1)^2(X-2) = 4.$$

(ii) *Toutes les solutions de l'équation diophantienne $a^4 + b^3 = c^2$ (avec a, b, c entiers non nuls premiers entre eux) s'obtiennent par des spécialisations rationnelles convenables dans les identités :*

$$(*) \qquad (X-1)^2(X+2) - (X+1)^2(X-2) = 4$$

$$1 + (3X + 1)(X - 1)^3 = X^2(3X^2 - 8X + 6).$$

(iii) *Toutes les solutions de l'équation diophantienne* $a^3 + b^3 = c^2$ *(avec* a, b, c *entiers non nuls premiers entre eux) s'obtiennent par des spécialisations rationnelles convenables dans les identités :*

$$3(X^2 - 3)^2 - 4(2X - 3)^3 = (3X - 5)(X - 3)^3$$

$$(X + 1)^3 - (X - 1)^3 = 2(3X^2 + 1)$$

$$(ou\ X^3 - (X - 1)(X^2 + X + 1) = 1).$$

5.2. (Avec A. Nitaj , cf. [L,N]). Les éléments de CE sont intéressants en eux-mêmes dans l'optique d'un problème sur l'ensemble dérivé L' de l'ensemble des valeurs prises par la quantité

$$\log c/\log(u(ab(a + b))$$

où, comme à l'habitude pour la conjecture (abc), (a, b) décrit l'ensemble des couples d'entiers positifs premiers entre eux .

La borne supérieure de L' est au moins 1 (choisir $a = 1, b = 2n$); dire qu'elle est au plus 1 revient donc à établir la conjecture (abc) ; si cette dernière est vraie, alors $L' \subset [1/3, 1]$ (cf. [B,F,G,S]) ; dans cette référence, on montre aussi que $[1/3, 15/16] \supset L'$ en incluant dans L' des intervalles dont les bornes sont reliées à l'écriture de cas d'égalité (R, S) pour le théorème de Mason. Dans le cas présent, on désire de plus que les polynômes $R, S, R - S$ soient à coefficients entiers et que le niveau (i.e. la borne supérieure des degrés des facteurs irréductibles intervenant dans $RS(R - S)$) soit au plus 4 (*This restriction on the degrees is regrettable but is typical of the current state of knowledge*, cf. [G,N], loc. citée). Si ces conditions sont vérifiées, alors on peut envisager (cf. [B,F,G,S], [G,N]) pour L' un minorant α de la borne supérieure avec (en niveau 4) $\alpha = 3D/(3(D + 1) + 1)$. Par suite, il est intéressant de découvrir des cas d'égalité de bas niveau et de degré grand. A. Nitaj a produit une identité (£) de degré 48 reliée aux polynômes homogènes $A(s, t)$, $B(s, t)$, $C(s, t)$ déjà évoqués dans les travaux de Beukers (et liés eux-mêmes aux invariants de Klein de l'octaèdre) : $A^4 + B^2 = C^3$ avec

$$\begin{aligned} A(s, t) &= (s^2 + 3t^2)(s^4 - 18s^2t^2 + 9t^4), \\ B(s, t) &= 4st(s^2 - 3t^2)(s^4 + 6s^2t^2 + 81t^4)(3s^4 + 2s^2t^2 + 3t^4), \\ C(s, t) &= (s^4 - 2s^2t^2 + 9t^4)(s^4 + 30s^2t^2 + 9t^4), \end{aligned}$$

ce qui permet d'améliorer en $36/37 = 3 \cdot 48/(3 \cdot (48 + 1) + 1)$ (cf. [G,N]) la borne 15/16 de [B,F,G,S].

Ce cas d'égalité (£) pour le théorème de Mason s'écrit :

$$(\pounds) \qquad I^8 - H^4 = J^3K$$

avec :

$$\begin{aligned} H &= 4Z(3Z^2-1)(81Z^4+6Z^2+1)(3Z^4+2Z^2+3),\\ I &= (9Z^4-18Z^2+1)(3Z^2+1),\\ J &= (9Z^4+30Z^2+1)(9Z^4-2Z^2+1),\\ K &= K'K'', \end{aligned}$$

où

$$\begin{aligned} K'(Z) = K''(-Z) = {}&(27Z^4-36Z^3+30Z^2-12Z-1)\\ &\times(3Z^4-12Z^3-10Z^2-4Z-1)(9Z^4+12Z^3+6Z^2-4Z+1). \end{aligned}$$

La factorisation naturelle fournit $H^2+I^4=J^3$ et permet, grâce au changement de variable $\mathrm{Z}=\mathrm{t}/\mathrm{s}$ de retrouver les polynômes A, B, C précédents ; plus précisément, on passe de (*) à ces derniers en composant les transformations : $X=-(6Y+4)(3Y+10)^{-1}$, $Y=T+T^{-1}$, $T=(U-1)^2/4U$, $U=3(T/S)^2$.

La démarche est ici inverse de celle précédente où l'on effectuait une *descente*. Ici, on cherche à écrire des identités de grand degré et de niveau ≥ 4. Celle ci-dessus s'obtient par spécialisation dans une identité de CEL :

$$(X-1)^4(X+2)^2-(X+1)^4(X-2)^2=8X(X^2-3),$$

se déduisant aussitôt (si (R,S) appartient à CE (resp. CEL), alors (R^n,S^n) appartient à CE (resp. CEL)) de (*) $(X-1)^2(X+2)-(X+1)^2(X-2)=4$.

Précisément, on peut vérifier le résultat de calcul suivant (cf. [L-N]) :

Théorème 12. *Soient F et G les polynômes :*

$$\begin{aligned} F(Z) &= (9Z^4+30Z^2+1)(9Z^4-2Z^2+1)\\ G(Z) &= 2(9Z^4+12Z^3+6Z^2-4Z+1)(9Z^4-12Z^3+6Z^2+4Z+1). \end{aligned}$$

La spécialisation $X=-G(Z)/F(Z)$ dans l'identité (se ramenant à (*)) :

$$(X-1)^4(X+2)^2-(X+1)^4(X-2)^2=8X(X^2-3)$$

fournit l'identité (£).

Remarque. Une variante de (£) s'écrivant $(K'K'')^2+4H^2I^4=J^6$ avec les notations précédentes se déduit aussi de la variante par translation : $(U+4)(U+1)^2-(U+3)^2U=4$ de (*) avec :

$$U=-(2^4Z(3Z^2-1)(3Z^2+1)^2/(9Z^4+30Z^2+1)(9Z^4-2Z^2+1))^2.$$

De fait, toutes ces spécialisations sont bien sûr gouvernées par le *théorème de Mason* (au sens élargi), plus précisément par la variante suivante des théorèmes précédents :

Théorème 13 (cf. [L.5]). *Soient $A(X) + B(X) = C(X)$ un cas d'égalité pour le théorème de Mason et $R(T)/S(T)$ une fraction rationnelle. La spécialisation $X = R(T)/S(T)$ dans l'identité précédente fournit un nouveau cas d'égalité pour le théorème de Mason si et seulement si le wronskien $(RS' - R'S)(T)$ divise le polynôme $(ABC)(R(T)/S(T))S(T)^{3D}$ (D désignant le plus grand des degrés des polynômes A, B, C).*

En fait, pour conserver un bas niveau, la difficulté consiste à effectuer des spécialisations fournissant de multiples factorisations et répondant aux conditions du théorème 12 ; c'est précisément le but de [L-N].

En utilisant le théorème 13, on voit que des relations comme (*) peuvent s'auto-engendrer. Ainsi, l'identité (*) - issue de $(T+4) - T = 4$ comme on vient de le voir - engendre elle-même une suite de cas d'égalité : en effet, (*) s'écrit par décalage $T(T-3)^2 - (T-1)^2(T-4) = 4$ (expression contenant les facteurs T et $(T-1)$) et la spécialisation $T = (X-1)^2(X+2)(X+1)^{-2}(X-2)^{-1}$ de wronskien associé $X^2 - 1$ (cf. ci-dessus) conduit donc à un nouveau cas d'égalité :

$$(X+2)(X-1)^2(X^3-3X-4)^2 - (X-2)^3(X+1)^6 = -12X^3 + 36X + 40.$$

Ce dernier s'écrit après décalage sous la forme suivante où réapparaissent les facteurs T et $(T-1)$:

$$(T+3)T^2(T^3+3T^2-6)^2 - (T-1)^3(T+2)^6 = -12T^3 - 36T^2 + 64,$$

d'où, à nouveau par la spécialisation $T = (X-1)^2(X+2)(X+1)^{-2}(X-2)^{-1}$:

$$\begin{aligned} A^2(X)(X-1)^4(X+2)^2(X^3-3X-1) - B(X)(X+1)^{12}(X-2)^6 \\ = 4(3X^3-9X-2)^6 \end{aligned}$$

avec :

$$\begin{aligned} A(X) &= X^9 - 9X^7 - 24X^6 + 27X^5 + 144X^4 + 9X^3 - 216X^2 \\ &\quad -108X - 16, \\ B(X) &= X^9 - 9X^7 - 33X^6 + 27X^5 + 198X^4 + 21X^3 - 297X^2 \\ &\quad -144X - 20, \end{aligned}$$

et on peut poursuivre ...

On peut faire plus à partir des deux corollaires suivants du théorème 13.

Corollaire 1. *Si un couple de polynômes (R, S) engendre un cas d'égalité, alors le wronskien du faisceau engendré par R et S est égal à $RS(R-S)/u(RS(R-S))$.*

Exemple. Le wronskien associé à l'identité

$$(T+5)(T-4)^2(T+1)^3 - (T-5)(T+4)^2(T-1)^3 = 432T$$

est $(T+4)(T-4)(T+1)^2(T-1)^2$.

Corollaire 2. *Si deux couples de polynômes $(R(X), S(X))$, $(U(X), V(X))$ appartiennent à CE et si de plus $X(X-1)$ divise $UV(U-V)$, alors la substitution de $R(X)/S(X)$ à X dans le cas d'égalité engendré par (U, V) fournit un autre élément de CE (par suite, si $X(X-1)$ divise aussi $RS(R-S)$, alors la substitution de $R(X)/S(X)$ à X dans le cas d'égalité engendré par (R, S) peut être itérée, d'où une branche infinie dans l'arbre CE).*

Exemple. $R(T) = U(T) = (T+5)(T-4)^2(T+1)^3$, $S(T) = V(T) = (T-5)(T+4)^2(T-1)^3$ donne naissance à

$$\begin{aligned}(X+5)(X-5)^5&(X-4)^2(X+4)^{10}(X+1)^3(X-1)^{15}\\ &-2^{10}3^6X^3(X^6-30X^4+165X^2-324X+80)\\ &\qquad\times(5X^6-150X^4+825X^2-648X+400)^2\end{aligned}$$

$$\begin{aligned}&=(X^6-30X^4+165X^2-144X+80)(X^6-30X^4+165X^2-360X+80)^2\\ &\qquad\times(X^6-30X^4+165X^2+80)^3,\end{aligned}$$

identité qui s'écrit plus commodément en posant $A(X) = X^6 - 30X^4 + 165X^2 + 80$:

$$\begin{aligned}(X+5)(X-5)^5(X-4)^2&(X+4)^{10}(X+1)^3(X-1)^{15}\\ &-2^{10}3^6X^3(A(X)-324X)(5A(X)-648X)^2\end{aligned}$$

$$= A^3(X)(A(X)-360X)^2(A(X)-144X).$$

Remerciements. L'auteur remercie vivement le rapporteur pour la précision de ses remarques et corrections.

N.B. : Relativement à la conjecture de Hall (cf. 5.1), N. Elkies a mis récemment (8/1998) en évidence deux exemples nouveaux pour lesquels le rapport $|a^3 - b^2|/\sqrt{a}$ améliore celui donné au §5 :

$$\begin{aligned}(3\cdot 7211\cdot 38791\cdot 6975841)^3-(2\cdot 3^2\cdot 15228748819\cdot 1633915978229)^2&\\ = 3^3\cdot 7^2\cdot 17\cdot 73&\end{aligned}$$

$$\begin{aligned}(3\cdot 89\cdot 97\cdot 319147\cdot 4611407)^3-(13\cdot 73\cdot 10939\cdot 395141\cdot 1814115338729)^2&\\ = 2\cdot 5\cdot 3003227,&\end{aligned}$$

ainsi, si C existe, $C < 0,021459$.

Bibliographie

[A-D,L] S. Abgrall-Duchemin, M. Langevin, *Links between the Danilov and Schinzel inequality, the Diophantine equation* $x^5+y^3=z^2$ *and the algebraic identities for which the Mason theorem is an equality*, soumis.

[B] F. Beukers, *The diophantine equation* $Ax^p+By^q=Cz^r$, Duke Math. J. **91** (1998), 61–88.

[B,F,G,S] J. Browkin, M. Filaseta, G. Greaves, A. Schinzel, *Squarefree values of polynomials and the abc-conjecture*, in Sieve Methods, Exponential Sums and their Applications in Number Theory (Greaves, Harman, Huxley Eds.), Camb. Univ. Press, 1996.

[G, N] G. Greaves, A. Nitaj, *Some Polynomial Identities related to the abc-Conjecture*, à paraître.

[H] M. Hall , *The diophantine equation* $x^3-y^2=k$, in Computers in Number Theory, Atkin and Birch Eds, Acad. Press, 1971, 173–198.

[He] Y. Hellegouarch, *Analogues en caractéristique* p *d'un théorème de Mason*, C. R. Acad. Sc. Paris **325** (1997), 141–144.

[L] S. Lang , Algebra, 3rd ed., Addison-Wesley, 1993, Ch. IV §7, 194–200.

[L.1] M. Langevin, *Cas d'égalité pour le théorème de Mason et applications de la conjecture* (abc), C. R. Acad. Sci. Paris **317** (1993), 441–444.

[L.2] M. Langevin, *Partie sans facteur carré de* $F(a,b)$ *modulo la conjecture* (abc), Sém. Th. des Nombres Caen 93/94, Publ. Univ. Caen, 1995.

[L.3] M. Langevin, *Sur quelques conséquences de la conjecture* (abc) *en arithmétique et en logique*, Rocky Mount. J. of Math. **26** (1996), 1031–1042.

[L.4] M. Langevin, *Liens entre le théorème de Mason et la conjecture* (abc), dans C.R.M., Proc. and Lect. Notes A.M.S., vol. 18, K. Williams and R. Gupta Eds, 1998 , 187–213.

[L.5] M. Langevin, *Extensions du théorème de Mason et de la conjecture* (abc), en préparation.

[L-N] M. Langevin, A. Nitaj, *Algebraic specializations in polynomial identities of low level*, soumis.

[M] R.C. Mason, *Diophantine equations over function fields*, LMS Lect. Notes **96**, Camb. Univ. Press, 1984.

[Z] U. Zannier ,*On Davenport's bound for the degree of* f^3-g^2 *and Riemann's Existence Theorem*, Acta Arithm. **LXXI** (1995), 107–137 et *Acknowledgement of priority*, Acta Arithm. **LXXIV** (1996), p. 387.

Michel Langevin
Laboratoire A2X
Institut Mathématiques Bordeaux
351 cours de la Libération
F-33450 Talence Cedex
E-mail : `lgv@math.u-bordeaux.fr`