Le 2 juillet 1998

Mémoire de D.E.A.

Quelques applications de la conjecture *abc*

Stéphane Fischler

Sous la direction de
Alain Kraus
et Michel Waldschmidt

Introduction

L'objectif de ce travail est d'étudier quelques aspects de la conjecture *abc*, dont l'énoncé est le suivant :

Conjecture 1 (abc) *Pour tout $\varepsilon > 0$ il existe une constante c_ε telle que, pour tout triplet (a, b, c) d'entiers relatifs non nuls premiers entre eux tels que $a + b = c$, on ait :*

$$|c| < c_\varepsilon |\mathrm{rad}(abc)|^{1+\varepsilon}$$

Dans le membre de gauche, on peut bien sûr remplacer $|c|$ par la plus grande des valeurs absolues de a, b, c.

Dans cet énoncé, on note $\mathrm{rad}(n)$ le radical d'un entier n, qui est (si $n > 0$) le produit des nombres premiers qui divisent n, comptés sans multiplicités. De plus, on pose $\mathrm{rad}(-n) = -\mathrm{rad}(n)$.

Le radical d'un entier n non nul (ou plus précisément la valeur absolue de ce radical) mesure la "multiplicité" de n : on dira qu'un entier n a "beaucoup de multiplicité" si les exposants qui apparaissent dans sa décomposition en facteurs premiers sont élevés. Ainsi, un entier positif n a beaucoup de multiplicité quand $\mathrm{rad}(n)$ est beaucoup plus petit que n.

La conjecture 1 date du début des années 80. Elle est due à J.Oesterlé, qui conjecturait seulement l'existence d'un $\varepsilon > 0$, en s'inspirant de la conjecture de Szpiro sur les courbes elliptiques (dont une forme est donnée à la section 6). Puis D.W. Masser a précisé cette conjecture pour lui donner sa forme actuelle.

On peut interpréter la conjecture *abc* de la manière suivante : si a, b, c sont trois entiers premiers entre eux tels que $a + b = c$, alors il est impossible que a, b et c aient tous les trois "beaucoup de multiplicité". Par exemple, on peut considérer, pour $p \geq 2$ et $n \in \mathbb{N}^*$, la relation

$$1 + [(1+p)^{p^n} - 1] = (1+p)^{p^n}$$

On constate facilement que p^{n+1} divise $(1+p)^{p^n} - 1$. Cette relation met en jeu des entiers qui ont suffisamment de multiplicité pour qu'on puisse en déduire (en prenant n assez grand) que dans l'énoncé de la conjecture *abc*, on ne peut pas prendre $\varepsilon = 0$. La recherche de telles relations *abc*, c'est-à-dire de triplets (a, b, c) d'entiers premiers entre eux, tels que $a + b = c$, et tels que a, b et c aient le maximum de multiplicité, fait l'objet de [19].

Par exemple, en appliquant la conjecture *abc* à une relation de la forme $x^n + y^n = z^n$, on montre que cette équation n'a qu'un nombre fini de solutions en nombres entiers premiers entre eux pour $n \geq 4$, et qu'elle n'a aucune solution non triviale pour n assez grand : c'est le théorème de Fermat asymptotique.

Outre ce théorème, la conjecture *abc* a de multiples conséquences en théorie des nombres : elle implique aussi bien la finitude du nombre de solutions de certaines équations diophantiennes (voir [19]) que la conjecture de Mordell (devenue le théorème de Faltings, voir au paragraphe 5.3).

Toutefois, malgré les progrès récents et la démonstration du théorème de Fermat, la conjecture *abc* reste actuellement hors de portée. Les seuls résultats obtenus à ce jour sont très partiels, et proviennent de méthodes complètement différentes de celles utilisées pour démontrer le théorème de Fermat. En effet, c'est grâce à la théorie des formes linéaires de logarithmes que C.L. Stewart et K. Yu ont démontré dans [29] le résultat suivant :

Théorème 1 *Pour tout $\varepsilon > 0$ il existe une constante c_ε telle que, pour tout triplet (a, b, c) d'entiers relatifs non nuls premiers entre eux tels que $a + b = c$, on ait :*

$$|c| < \exp(c_\varepsilon |\mathrm{rad}(abc)|^{\frac{2}{3}+\varepsilon})$$

Dans ce travail, on s'intéressera dans une première partie à un équivalent polynômial de la conjecture *abc*, le théorème de Mason. On cherchera à caractériser les cas d'égalité dans ce théorème (ou dans un corollaire de ce théorème). Puis on appliquera cette étude à la minoration (modulo la conjecture *abc*) du radical d'expressions polynômiales, quand la variable tend vers l'infini.

Dans une deuxième partie, on étudiera une conséquence de la conjecture *abc* en termes de courbes elliptiques, en rapport avec une question de Mazur concernant l'existence de couples (E, E') de courbes elliptiques sur $\mathbb{Q}$ non isogènes dont les représentations de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de p-torsion soient isomorphes, pour un nombre premier p donné.

Première partie
Liens avec les polynômes

1 Théorème de Mason

1.1 Enoncé et démonstration

NOTATIONS : soit P un polynôme à coefficients complexes. On note $d(P)$ son degré, et $\varrho(P)$ son nombre de racines dans $\mathbb{C}$ (comptées sans multiplicités). On note $u(P)$ le polynôme séparable (i.e. à racines simples), unitaire, ayant les mêmes racines que P. Ainsi, si $P = \lambda(X-x_1)^{n_1}\cdot\ldots\cdot(X-x_k)^{n_k}$, où les x_i sont deux à deux distincts, avec $\lambda \in \mathbb{C}^\star$, on a $u(P) = (X-x_1)\cdot\ldots\cdot(X-x_k)$.

Le théorème suivant, malgré sa formulation très simple, date de 1984 :

Théorème 2 (Mason) *Soient R et S deux polynômes à coefficients complexes, premiers entre eux, non tous les deux constants. Alors :*

$$\varrho(RS(R-S)) \geq \max(d(R), d(S)) + 1$$

N.B. Comme R et S sont premiers entre eux, cela s'écrit :

$$\varrho(R) + \varrho(S) \geq \max(d(R), d(S)) - \varrho(R-S) + 1$$

N.B. On peut établir entre $\mathbb{Z}$ et $\mathbb{C}[X]$ une analogie par laquelle la valeur absolue correspond au degré, le radical (noté rad) au radical (noté u), et la valeur absolue du radical (qui mesure le "manque de multiplicité") au nombre de racines (noté ϱ). Par cette analogie, l'énoncé du théorème de Mason (formulé avec des polynômes $A = R-S$, $B = S$ et $C = R$) correspondrait à l'existence d'une constante indépendante de ε dans la conjecture *abc*, ce qui est faux. Mais on peut retenir que ce théorème est, comme la conjecture *abc*, la minoration (en degré, ou en valeur absolue) d'un radical. Précisément, le théorème de Mason affirme qu'un produit de la forme $RS(R-S)$ (ou ABC, avec $A+B=C$) ne peut pas avoir trop de multiplicité (c'est-à-dire avoir trop peu de racines). Les cas d'égalité dans ce théorème sont donc des couples (R, S) tels que le polynôme $RS(R-S)$ ait autant de multiplicité que possible, c'est-à-dire ait le maximum de racines de multiplicité élevée (compte tenu des degrés de R et S).

DÉMONSTRATION : voir [12], page 194.

1.2 Passage des couples de polynômes aux fractions rationnelles

Dans le but de donner une autre démonstration du théorème de Mason, notons r la fraction rationnelle $\frac{R}{S}$. Ainsi associe-t-on une fraction rationnelle r à chaque couple (ordonné) (R, S) de polynômes à coefficients complexes premiers entre eux. Réciproquement, à une fraction rationnelle $r \in \mathbb{C}(X)$ on associe le couple formé par son numérateur et son dénominateur (en écrivant r comme quotient de deux polynômes premiers entre eux).

CONVENTION : Désormais, on supposera toujours que les polynômes R et S sont premiers entre eux et que l'un au moins est non constant. Cela signifie que r est une fraction rationnelle non constante. Ces conventions seront sous-entendues dans l'écriture $r = \frac{R}{S}$.

L'idée d'introduire cette fonction r (idée qui se trouve, par exemple, dans [6]) permet de reformuler le théorème de Mason. En effet, si $r = \frac{R}{S}$, le nombre de racines de R est le nombre de zéros de r dans $\mathbb{C}$, le nombre de racines de S est le nombre de pôles de r dans $\mathbb{C}$, et le nombre de racines de $R - S$ est le nombre de points de $\mathbb{C}$ auxquels r prend la valeur 1. Ainsi l'entier $\varrho(RS(R-S))$ est-il le nombre de points de $\mathbb{C}$ où r prend l'une des trois valeurs 0, 1 ou ∞. Cela explique pourquoi le théorème 3 cité plus bas est équivalent au théorème de Mason.

1.3 Notion de ramification d'une fraction rationnelle

Le but de ce paragraphe est de définir la notion de ramification. Soit $r = \frac{R}{S}$ une fraction rationnelle (avec R et S premiers entre eux); on la voit comme une application de $\mathbb{P}^1(\mathbb{C})$ dans $\mathbb{P}^1(\mathbb{C})$, l'image de l'infini étant zéro, l'infini, ou le quotient des coefficients dominants de R et S selon que le degré de R est inférieur, supérieur ou égal à celui de S.

DÉFINITION : Soit r une fraction rationnelle non constante. On appelle *degré* de r, et on note $\deg(r)$, le nombre d'images réciproques par r que possède chaque point de $\mathbb{P}^1(\mathbb{C})$ (sauf un nombre fini d'exceptions). Si on écrit $r = \frac{R}{S}$, alors $\deg(r)$ est le plus grand des degrés de R et S. Quand r est un polynôme, cette notion de degré coïncide avec le degré usuel, noté ici d. Mais le degré d'une fraction rationnelle défini ici n'a rien à voir avec le degré défini comme différence des degrés du numérateur et du dénominateur. Pour éviter la confusion, on n'utilisera pas cette deuxième notion.

Dans toute la suite, la fraction rationnelle r est supposée non constante.

DÉFINITION : Soit $x_0 \in \mathbb{C}$ qui ne soit pas un pôle de r ; posons $y_0 = r(x)$. L'indice de ramification de r en x_0, noté e_{x_0}, est la multiplicité avec laquelle il convient de compter x_0 comme solution de l'équation $r(x) = y_0$: c'est le plus petit entier k tel que la dérivée $k$ième de la fraction rationnelle r ne s'annule pas en x_0. Si on écrit $r = \frac{R}{S}$, c'est l'ordre de x_0 comme zéro du polynôme $R - y_0 S$. Puisque R et S sont supposés premiers entre eux et non tous les deux constants (puisque r est supposée non constante), l'entier e_{x_0} est bien défini. De plus, il est supérieur ou égal à 1.

Pour $x_0 \in \mathbb{C}$ pôle de r, on définit l'indice de ramification de r en x_0 comme étant celui de $\frac{1}{r}$ au même point x_0.

Pour $x_0 = \infty$, on définit l'indice de ramification de r en l'infini comme celui de $r(\frac{1}{X})$ en zéro. Si on a $r = \frac{R}{S}$ et $r(\infty) = \alpha \in \mathbb{C}^\star$, alors cet indice vaut $d(R) - d(R - \alpha S)$; si $r(\infty) \in \{0, \infty\}$ (c'est-à-dire si R et S sont de degrés différents), alors cet indice vaut $\mid d(R) - d(S) \mid$.

On peut noter la relation suivante, qui découle du fait que $\mathbb{C}$ est algébriquement clos :

$$\sum_{x \in \mathbb{P}^1(\mathbb{C}),\ r(x)=y_0} e_x = \deg(r) \text{ pour tout } y_0 \in \mathbb{P}^1(\mathbb{C}) \tag{1}$$

Il est à noter que lorsqu'on utilise les indices de ramification, on considère la fonction r comme allant de $\mathbb{P}^1(\mathbb{C})$ dans $\mathbb{P}^1(\mathbb{C})$. Il convient donc de toujours considérer les images réciproques dans $\mathbb{P}^1(\mathbb{C})$, c'est-à-dire en incluant le point à l'infini le cas échéant.

DÉFINITION : Une fraction rationnelle $r : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ est dite non ramifiée en $x \in \mathbb{P}^1(\mathbb{C})$ si $e_x = 1$. Elle est dite non ramifiée au-dessus de $y \in \mathbb{P}^1(\mathbb{C})$ si elle est non ramifiée en chaque antécédent de y par r. Elle est dite ramifiée en x (respectivement au-dessus de y) si elle n'est pas non ramifiée en x (respectivement au-dessus de y).

Les deux lemmes suivants se déduisent aisément des définitions :

Lemme 1 *Une fraction rationnelle r est non ramifiée au-dessus de $y \in \mathbb{P}^1(\mathbb{C})$ si, et seulement si, y admet $\deg(r)$ antécédents (deux à deux distincts) par r.*

Lemme 2 *Soient r une fraction rationnelle et $z \in \mathbb{P}^1(\mathbb{C})$ tels que $z \neq \infty$ et $r(z) \neq \infty$. Alors r est ramifiée en z si, et seulement si, $r'(z) = 0$.*

En particulier, on déduit de ce deuxième lemme qu'une fraction rationnelle n'est ramifiée qu'en un nombre fini de points.

Ces notions de ramification peuvent être définies dans un cadre beaucoup plus général, mais cela sera inutile ici (sauf aux paragraphes 4.3 et 5.3). La formule de Riemann-Hurwitz est primordiale; son énoncé général et sa démonstration se trouvent, par exemple, dans [28], page 41. Dans le cadre traité ici, cette formule se démontre de façon élémentaire et s'énonce de la façon suivante :

$$\sum_{x \in \mathbb{P}^1(\mathbb{C})} (e_x - 1) = 2 \deg(r) - 2$$

Cette formule a un sens car r n'est ramifiée qu'en un nombre fini de points. On peut interpréter cette formule de la façon suivante : la ramification totale de r (qui est représentée par le membre de gauche) ne dépend que du degré de r. En particulier, dès que r est de degré au moins 2, elle est ramifiée en au moins un point (en fait, si elle était ramifiée en un point seulement, ce point aurait pour indice de ramification $2\deg(r) - 1$, ce qui contredirait la relation (1)).

Donnons dès à présent une définition qui sera utile par la suite :

DÉFINITION : On appelle fonction de Belyi toute fraction rationnelle non constante $r : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ qui est non ramifiée au-dessus de chaque point de $\mathbb{P}^1(\mathbb{C})$, sauf peut-être au-dessus de $\{0, 1, \infty\}$.

1.4 Deuxième démonstration du théorème de Mason

La notion de ramification, et en particulier la formule de Riemann-Hurwitz, permettent de donner une autre démonstration du théorème de Mason, à condition de le formuler en termes de fractions rationnelles :

Théorème 3 (Mason, formulation équivalente) *Pour toute fraction rationnelle non constante $r \in \mathbb{C}(X)$ on a :*

$$\mathrm{Card}(\{x \in \mathbb{C} \mid r(x) \in \{0, 1, \infty\}\}) \geq \deg(r) + 1$$

DÉMONSTRATION du théorème 3 : Appliquons à la fraction rationnelle non constante r la formule de Riemann-Hurwitz mentionnée ci-dessus. On obtient :

$$\sum_{x \in \mathbb{P}^1(\mathbb{C})} (e_x - 1) = 2 \deg(r) - 2$$

Or l'indice de ramification de r en un point $x \in \mathbb{P}^1(\mathbb{C})$ est un entier supérieur ou égal à 1. D'où :

$$\sum_{x \in \mathbb{P}^1(\mathbb{C}),\ r(x) \in \{0,1,\infty\}} (e_x - 1) \ \leq \ 2 \deg(r) - 2$$

En écrivant la somme des $e_x - 1$ comme somme des e_x (qui, puisqu'on somme sur tous les antécédents des trois points $0, 1$ et ∞, donne trois fois le degré de r d'après la formule (1)) à laquelle on retranche la somme des 1 (qui est le nombre d'antécédents dans $\mathbb{P}^1(\mathbb{C})$ des trois points $0, 1, \infty$), on obtient :

$$3 \deg(r) - \mathrm{Card}(\{x \in \mathbb{P}^1(\mathbb{C}) \mid r(x) \in \{0, 1, \infty\}\}) \leq 2 \deg(r) - 2$$

Cela s'écrit aussi :

$$\mathrm{Card}(\{x \in \mathbb{P}^1(\mathbb{C}) \mid r(x) \in \{0, 1, \infty\}\}) \geq \deg(r) + 2$$

Quand on enlève au membre de gauche le point $x = \infty$, qui peut figurer parmi les antécédents de $\{0, 1, \infty\}$, on obtient :

$$\mathrm{Card}(\{x \in \mathbb{C} \mid r(x) \in \{0, 1, \infty\}\}) \geq \deg(r) + 1$$

Cela conclut la démonstration du théorème 3.

1.5 Corollaire du théorème de Mason

On déduit immédiatement du théorème de Mason le corollaire suivant :

Corollaire 1 *: Soient R et S deux polynômes à coefficients complexes, premiers entre eux, non tous les deux constants. Alors :*

$$\varrho(RS) \geq \max(d(R), d(S)) - d(R-S) + 1$$

Ce corollaire peut être vu comme une minoration du nombre de racines de RS, quand les degrés de R, S et $R-S$ sont fixés. On peut aussi le voir comme une minoration de $d(R-S)$ en fonction des degrés de R et S, et du nombre de racines de RS. Ce corollaire donne donc une réponse au problème suivant (qui apparaît dans [14]) :

Etant donnés un entier $d \geq 2$ et des complexes $x_1, \ldots, x_k$ (avec $k \geq 2$), on cherche des polynômes R et S premiers entre eux, de même degré d, tels que les racines de RS soient des x_i et tels que $R-S$ soit de degré minimal. On peut écrire :

$$\begin{aligned} R(X) = \textstyle\prod_i (X-x_i)^{e_i} = &\quad X^d + r_1 X^{d-1} + \ldots + r_d \\ et \quad S(X) = \textstyle\prod_i (X-x_i)^{f_i} = &\quad X^d + s_1 X^{d-1} + \ldots + s_d \end{aligned}$$

Dans ces formules, les e_i et les f_i sont des entiers naturels tels que pour tout indice i, l'un exactement parmi e_i et f_i est nul. Le problème est de choisir ces exposants tels que $d(R-S)$ soit minimal, c'est-à-dire que les suites $(r_1, \ldots, r_d)$ et $(s_1, \ldots, s_d)$ coïncident aussi loin que possible. Le corollaire 1 montre qu'au maximum, les $k-2$ premiers termes de ces suites coïncident. Les cas d'égalité dans le corollaire 1 correspondent aux choix des e_i et des f_i qui permettent d'avoir $r_1 = s_1, \ldots, r_{k-2} = s_{k-2}$.

Cette façon de voir les cas d'égalité dans le corollaire 1 sera sous-jacente à la démonstration de la proposition 7, au paragraphe 3.3.

Une autre question reliée au théorème de Mason est le problème de Tarry-Escott (voir [21]) : trouver des couples (R, S) de polynômes distincts, à zéros entiers, tels que $R-S$ soit constant. Le corollaire 1 montre que pour un tel couple, on a nécessairement $r(RS) \geq d+1$, où d désigne le degré commun de R et S. Un exemple de tel couple (R, S) sera donné au paragraphe 3.5.

2 Etude préliminaire des cas d'égalité

On s'intéresse maintenant aux cas d'égalité dans le théorème 2 (de Mason) et dans le corollaire 1.

2.1 Cas d'égalité dans le théorème 2

Soit (R, S) un couple de polynômes qui est un cas d'égalité dans le théorème 2. Posons $r = \frac{R}{S}$. Reprenons la preuve du théorème 3 (équivalent au théorème 2) à partir de la formule de Riemann-Hurwitz pour voir ce qu'on peut déduire du fait que la suite d'inégalités utilisée est en fait une suite d'égalités.

Tout d'abord, dans cette preuve, on minore $\sum_{x \in \mathbb{P}^1(\mathbb{C})} e_x - 1$ par $\sum_{x \in \mathbb{P}^1(\mathbb{C}), r(x) \in \{0,1,\infty\}} e_x - 1$. Comme maintenant on suppose que (R, S) est un cas d'égalité, cette minoration est elle aussi une égalité. On a donc $e_x = 1$ pour tout $x \in \mathbb{P}^1(\mathbb{C})$ tel que $r(x) \notin \{0, 1, \infty\}$. Cela signifie que r est une fonction de Belyi.

Ensuite, on a minore $\mathrm{Card}(\{x \in \mathbb{C} \mid r(x) \in \{0,1,\infty\}\})$ par
$$\mathrm{Card}(\{x \in \mathbb{P}^1(\mathbb{C}) \mid r(x) \in \{0,1,\infty\}\}) - 1.$$
Il y a égalité dans cette minoration si, et seulement si, $r(\infty) \in \{0, 1, \infty\}$.

Ces deux étapes sont les seules, dans la preuve du théorème 3 à partir de la formule de Riemann-Hurwitz (qui est une égalité), où il y ait des inégalités et non des égalités. On a donc démontré le résultat suivant :

Proposition 1 *: Les cas d'égalité dans l'inégalité du théorème 2 sont les couples (R,S) de polynômes tels que la fonction $r = \frac{R}{S}$ soit une fonction de Belyi qui envoie l'infini sur $0, 1$ ou ∞.*

CONVENTION : Désormais, on désignera par "cas d'égalité" aussi bien le couple de polynômes (R,S) que la fonction r associée.

Cette proposition permet en fait de traduire en termes de polynômes la notion de fonction de Belyi. En effet, elle affirme le résultat suivant : soit r une fraction rationnelle qui envoie l'infini sur $0, 1$ ou ∞ (ce qui, en écrivant $r = \frac{R}{S}$, signifie que R et S sont de degrés distincts, ou bien de même degré avec même coefficient dominant). Alors r est une fonction de Belyi si, et seulement si, $\varrho(RS(R-S)) = \max(d(R), d(S)) + 1$.

2.2 Cas d'égalité dans le Corollaire 1

Passons maintenant aux cas d'égalité dans le corollaire 1.

Tout d'abord, en termes de polynômes, soit (R,S) un couple de polynômes tels que

$$\varrho(RS) = \max(d(R), d(S)) - d(R-S) + 1.$$

En lui appliquant le théorème 2, on obtient $d(R-S) \leq \varrho(R-S)$, ce qui montre que $R-S$ est nécessairement à racines simples. De plus, (R,S) est un cas d'égalité dans le théorème 2. Ces conditions sont visiblement suffisantes, d'où la proposition suivante :

Proposition 2 *: Les cas d'égalité dans le corollaire 1 sont exactement les cas d'égalité (R,S) du théorème 2 tels que $R-S$ soit à racines simples.*

Toutefois, il existe des cas d'égalité triviaux dans le corollaire 1. En effet, quand on a $d(R-S) = \max(d(R), d(S))$, les cas d'égalité vérifient $\varrho(RS) = 1$: parmi R et S, l'un des deux est constant non nul et l'autre de la forme $(X-\alpha)^n$ avec $n \geq 1$ (puisque R et S sont supposés premiers entre eux et non tous les deux constants). Réciproquement, un tel couple (R,S) est toujours un cas d'égalité dans le corollaire 1.

Ces cas d'égalité triviaux correspondent à des fonctions r de la forme $\lambda(X-\alpha)^n$ avec $\lambda \in \mathbb{C}^\star$, $\alpha \in \mathbb{C}$ et $n \in \mathbb{Z} - \{0\}$ (l'exposant n est positif si c'est le polynôme S qui est constant, négatif si c'est R).

Cherchons à caractériser les cas d'égalité non triviaux dans le corollaire 1. Soit (R,S) un cas d'égalité quelconque; posons $r = \frac{R}{S}$. Comme les cas d'égalité dans le corollaire 1 sont des cas d'égalité dans le théorème 2, la proposition 1 montre que r est une fonction de Belyi et que $r(\infty) \in \{0, 1, \infty\}$. On peut distinguer deux cas :

1. Premier cas : $r(\infty) \in \{0, \infty\}$. Cela signifie que les polynômes R et S sont de degrés distincts. D'où $d(R-S) = \max(d(R), d(S))$: on est dans le cas d'égalité trivial annoncé plus haut ; parmi R et S, l'un des deux est constant non nul et l'autre de la forme $(X-\alpha)^n$ avec $n \geq 1$. Réciproquement, des polynômes de cette forme fournissent bien un cas d'égalité dans le corollaire 1.

2. Deuxième cas : $r(\infty) = 1$. Cela signifie que R et S ont même degré et même coefficient dominant; on peut les supposer tous les deux unitaires. De plus, comme (R,S) est un cas d'égalité dans le corollaire 1, le polynôme $R-S$ est à racines simples, donc r n'est ramifiée en aucun antécédent de 1, sauf peut-être en l'infini. Réciproquement, si $r = \frac{R}{S}$ avec r ramifiée seulement au-dessus de $\{0, \infty\}$ et en l'infini, avec $r(\infty) = 1$, alors (R,S) est un cas d'égalité dans le théorème 2 (par la proposition 1), avec $R-S$ à racines simples (car r n'est ramifiée en aucun antécédent de 1 autre que l'infini), donc (par la proposition 2) (R,S) est un cas d'égalité dans le corollaire 1.

On peut résumer les conclusions de ce raisonnement dans la proposition suivante :

Proposition 3 *: Les cas d'égalité dans le corollaire 1 sont de deux familles :*

- *Des cas dits "triviaux" : l'un des deux polynômes est constant non nul, l'autre est de la forme* $(X-\alpha)^n$ *avec* $n \geq 1$ *et* $\alpha \in \mathbb{C}$.
- *Les autres cas, où les deux polynômes ont même degré et même coefficient dominant (qu'on peut supposer égal à* 1*). Ces cas d'égalité correspondent exactement aux fonctions* r *ramifiées seulement au-dessus de* $\{0, \infty\}$ *et en l'infini, avec* $r(\infty) = 1$.

En fait, on peut regrouper ces deux familles, pour que les cas "triviaux" apparaissent comme des cas particuliers de l'autre famille :

Proposition 4 *: Les cas d'égalité dans le corollaire 1 correspondent aux fonctions* r *ramifiées seulement au-dessus de* $\{0, \infty\}$ *et en l'infini qui sont telles que* $r(\infty) \in \{0, 1, \infty\}$.

Cette proposition provient du fait que toute fonction non constante r qui envoie l'infini sur 0 ou sur l'infini et qui est ramifiée seulement au-dessus de $\{0, \infty\}$ est de la forme $\lambda(X-\alpha)^n$ avec $n \in \mathbb{Z}$, $\alpha \in \mathbb{C}$ et $\lambda \in \mathbb{C}^\star$. Mais regrouper ces deux familles de cas d'égalité pose des problèmes plus loin; c'est pourquoi on adopte la définition suivante :

Définition : on appelle *cas d'égalité non trivial* un cas d'égalité (R, S) dans le corollaire 1 pour lequel aucun des deux polynômes n'est constant. La proposition 3 signifie alors que les cas d'égalité non triviaux correspondent exactement aux fonctions r ramifiées seulement au-dessus de $\{0, \infty\}$ et en l'infini, avec $r(\infty) = 1$. Les mots *cas d'égalité non trivial* pourront désigner aussi bien un couple (R, S) de polynômes que la fraction rationnelle r associée.

Le but de la section suivante est de classifier les cas d'égalité non triviaux.

3 Classification des cas d'égalité non triviaux

3.1 Notations

Définition (Rappel) : on appelle cas d'égalité non trivial une fonction $r : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ non constante ramifiée seulement au-dessus de $\{0, \infty\}$ et en l'infini, avec $r(\infty) = 1$. En notant $r = \frac{R}{S}$ (avec toujours la convention R et S premiers entre eux), cela signifie que R et S sont de même degré, de même coefficient dominant, non constants (si l'un des deux était constant, r serait un polynôme ou l'inverse d'un polynôme, donc l'image de l'infini ne pourrait pas être 1), et constituent un cas d'égalité dans le corollaire 1 (d'après la proposition 3), c'est-à-dire qu'on a : $\varrho(RS) = d(R) - d(R-S) + 1$.

Notation : On note M l'ensemble des cas d'égalité non triviaux.

On considérera les éléments de M soit comme des fractions rationnelles, soit comme des couples de polynômes. La correspondance entre ces deux langages est donnée par $r = \frac{R}{S}$. On supposera toujours que R et S sont premiers entre eux. Quand $(R, S) \in M$, R et S ont même coefficient dominant. On supposera parfois que R et S sont unitaires, mais on pourra aussi s'affranchir de cette hypothèse.

Si $r \in M$, l'inverse r^{-1} de r envoie aussi l'infini sur 1, et est également ramifié seulement au-dessus de $\{0, \infty\}$ et en l'infini. Donc $r^{-1} \in M$. De plus, si $k \in \mathbb{N}^\star$, la dérivée de r^k est $kr'r^{k-1}$: les points de $\mathbb{C}$ où cette dérivée s'annule sont les points de $\mathbb{C}$ où r s'annule (ces points sont donc au-dessus de 0 pour r^k), auxquels on adjoint les points où r' s'annule (qui sont les points de $\mathbb{C}$ en lesquels r est ramifiée; ils sont au-dessus de 0 ou de ∞ pour r, donc aussi pour r^k). Or les points

de $\mathbb{C}$ où la dérivée de r^k s'annule sont exactement les points de $\mathbb{C}$ en lesquels r^k est ramifiée. On a donc démontré que r^k est non ramifiée sauf au-dessus de $\{0, \infty\}$, et sauf peut-être en l'infini. Donc r^k est aussi un cas d'égalité non trivial. Réciproquement, si r est une fraction rationnelle et k est un entier naturel non nul tel que r^k soit un cas d'égalité non trivial, alors les points de $\mathbb{C}$ en lesquels r est ramifiée annulent r' donc $(r^k)'$, donc sont au-dessus de $\{0, \infty\}$ pour r^k donc pour r. Donc $r \in M$.

La stabilité de M par passage à l'inverse et à la puissance $k$ième, démontrée ici directement sur les fonctions de Belyi, peut aussi être démontrée à l'aide de l'autre définition des cas d'égalité non triviaux : un cas d'égalité non trivial est (en identifiant r au couple (R, S) tel que $r = \frac{R}{S}$) un cas d'égalité dans le corollaire 1 pour lequel aucun des deux polynômes n'est constant. C'est donc un couple de polynômes non constants vérifiant la relation : $\varrho(RS) + d(R-S) - 1 = \max(d(R), d(S))$. Cette relation reste inchangée quand on inverse les rôles de R et S, ce qui démontre la stabilité de M par passage à l'inverse.

Démontrons de même la stabilité de M par passage à la puissance $k$ième. Soient (R, S) un cas d'égalité non trivial et $k \in \mathbb{N}^\star$. On a :

$$d(R^k - S^k) = d(R - S) + d(R^{k-1} + R^{k-2}S + \ldots + RS^{k-2} + S^{k-1})$$

Comme R et S ont même degré et même coefficient dominant, on en déduit :

$$d(R^k) - d(R^k - S^k) = d(R) - d(R - S) = \varrho(RS) + 1 = \varrho(R^k S^k) - 1$$

Donc $(R^k, S^k) \in M$: on a ainsi démontré la stabilité de M par passage à la puissance $k$ième.

On montre de la même manière que si r est une fraction rationnelle dont une puissance r^k (avec $k \in \mathbb{Z} - \{0\}$) appartient à M, alors $r \in M$.

On peut donc définir une relation d'équivalence $\mathcal{R}$ sur M par : "deux éléments r et s de M sont équivalents si, et seulement si, il existe une fraction rationnelle t et deux entiers relatifs non nuls a et b tels que $r = t^a$ et $s = t^b$". Il est clair que deux éléments r et s sont équivalents si, et seulement si, il existe deux entiers relatifs non nuls c et d tels que $r^c = s^d$.

NOTATION : On note $M/\mathcal{R}$ l'ensemble quotient de M par cette relation d'équivalence.

Cet ensemble est en bijection avec l'ensemble des éléments r de M qui ne sont pas des puissances (non triviales) de fractions rationnelles, quotienté par la relation identifiant chaque fraction rationnelle à son inverse. Donc $M/\mathcal{R}$ est en bijection avec l'ensemble des paires (non ordonnées) $\{R, S\}$ telles que (R, S) soit un cas d'égalité dans le corollaire 1, que R et S soient non constants, et que les multiplicités des racines du polynôme RS soient premières entre elles dans leur ensemble.

CONVENTION : On appellera éléments de $M/\mathcal{R}$ aussi bien l'un que l'autre des objets suivants :

- les fractions rationnelles ramifiées seulement au-dessus de $\{0, \infty\}$ et en l'infini, qui envoient l'infini sur 1, modulo l'identification d'une telle fraction rationnelle avec ses puissances (positives ou négatives).
- l'ensemble des paires (non ordonnées) $\{R, S\}$ de polynômes non constants, premiers entre eux, unitaires, telles que $\varrho(RS) = \max(d(R), d(S)) - d(R - S) + 1$ et que les multiplicités des racines du polynôme RS soient premières entre elles dans leur ensemble. Ces conditions impliquent que R et S sont de même degré.

N.B. L'ensemble $M/\mathcal{R}$ ici considéré est donc l'ensemble noté M dans [14].

3.2 Une propriété des cas d'égalité non triviaux

Dans [14] se trouve l'énoncé suivant :

Proposition 5 *: Pour tout élément (R, S) de M il existe une constante c telle que :*

$$\frac{R'}{R} - \frac{S'}{S} = \frac{c}{u(R)u(S)}$$

NOTATION (rappel) : si P est un polynôme, $u(P)$ est l'unique polynôme unitaire à racines simples dont les racines sont les mêmes que celles de P.

On peut transcrire cette proposition dans le langage des fractions rationnelles :

Proposition 6 *: Pour tout élément r de M il existe une constante c telle que :*

$$\frac{r'(z)}{r(z)} = \frac{c}{\prod_{w \in r^{-1}(\{0,\infty\})}(z-w)}$$

N.B. On note parfois z l'indéterminée dans une fraction rationnelle (qui est souvent vue comme une fonction de $\mathbb{P}^1(\mathbb{C})$ dans $\mathbb{P}^1(\mathbb{C})$), alors qu'on note en général X l'indéterminée dans un polynôme.

N.B. Dans la proposition 6 , l'écriture $\prod_{w \in r^{-1}(\{0,\infty\})}(z-w)$ a bien un sens puisque $\infty \notin r^{-1}(\{0,\infty\})$.

N.B. Dans les propositions 5 et 6, la constante c dépend du représentant r (ou $\frac{R}{S}$) choisi, même au sein d'une classe d'équivalence modulo $\mathcal{R}$. Cette dépendance est simple : quand le représentant est élevé à la puissance k, la constante c est multipliée par k. De plus, cette constante s'exprime facilement en fonction de zéros ou pôles w_i de r, de leurs ordres (algébriques) n_i, et du cardinal t de $r^{-1}(\{0,\infty\})$ (qui est le nombre d'indices i) :

$$c = (-1)^{t-1} \sum_i n_i \prod_{j \neq i} w_j$$

Le fait que la proposition 6 soit la transcription de la proposition 5 est clair, puisque la correspondance est donnée par $r = \frac{R}{S}$. De plus, la conclusion de la proposition 6 s'exprime en disant que, à un scalaire multiplicatif près, la fraction rationnelle $\frac{r}{r'}$ est le polynôme dont les racines, simples, sont les images réciproques par r de $\{0,\infty\}$. Une réciproque sera vue au paragraphe 3.3.

On donne ici deux démonstrations des propositions 5 et 6. La première, tirée de [14], utilise les éléments de M vus comme des paires de polynômes. La seconde utilise l'aspect fraction rationnelle.

DÉMONSTRATION de la proposition 5 (par les polynômes) : Ecrivons de deux manières la dérivée logarithmique de $\frac{R}{S}$. D'une part, c'est $\frac{R'}{R} - \frac{S'}{S}$ qu'on peut réduire au même dénominateur sous la forme $\frac{c}{u(R)u(S)}$ avec $c \in \mathbb{C}[X]$, puisque $\frac{R'}{R}$ admet pour pôles, simples, les racines de R (et de même pour S).

D'autre part, $\frac{R'}{R} - \frac{S'}{S}$ s'annule à l'infini et son développement (au voisinage de l'infini) s'obtient en dérivant celui de $\log(\frac{R}{S})$. On a, puisque $d(R-S) < d(S)$:

$$\log(\frac{R}{S}) = \log(1 + \frac{R-S}{S}) = \frac{R-S}{S} - \frac{1}{2}(\frac{R-S}{S})^2 + \cdots$$

Par dérivation, cela donne :

$$\frac{R'}{R} - \frac{S'}{S} = (\frac{R-S}{S})' + \cdots$$

où l'infini est zéro de $(\frac{R-S}{S})'$ avec pour ordre $d(S) - d(R-S) + 1$, et est zéro des termes suivants avec des ordres strictement plus grands. Donc l'infini est un zéro d'ordre $d(S) + 1 - d(R-S)$ de $\frac{R'}{R} - \frac{S'}{S}$, qui est égal à $\frac{c}{u(R)u(S)}$ avec $c \in \mathbb{C}[X]$. On a donc : $d(S) + 1 - d(R-S) = \varrho(R) + \varrho(S) - d(c)$. Comme (R,S) est un cas d'égalité dans le corollaire 1, cela donne $d(c) = 0$: c est une constante, ce qui achève la démonstration de la proposition 5.

DÉMONSTRATION de la proposition 6 (par les fractions rationnelles) : Soit $r \in M$. Il suffit de prouver que $\frac{r'}{r}$ est une fraction rationnelle ayant pour pôles, simples, les images réciproques par r de $\{0,\infty\}$ et n'ayant aucun zéro dans $\mathbb{C}$. Pour cela, soit $w \in \mathbb{C}$. On distingue plusieurs cas :

- Si $r(w) \notin \{0,\infty\}$, alors r n'est pas ramifiée en w, et $r'(w)$ est un complexe non nul. De plus, $r(w)$ n'est ni 0 ni ∞. Donc w n'est ni un zéro ni un pôle de $\frac{r'}{r}$.

– Si $r(w) = 0$, notons e_w l'ordre de w comme zéro de r; alors w est zéro de r' d'ordre $e_w - 1$, donc w est un pôle simple de $\frac{r'}{r}$.

– Si $r(w) = \infty$, on applique le raisonnement précédent à $\frac{1}{r}$ (dont la dérivée logarithmique est l'opposée de celle de r). Cela montre que w est un pôle simple de $\frac{r'}{r}$.

De l'examen de ces trois cas résulte la proposition 6.

Les propositions 5 et 6 admettent des réciproques, qui font l'objet du paragraphe suivant.

3.3 Une caractérisation des cas d'égalité non triviaux

Commençons par le lemme suivant :

Lemme 3 *: Soit $P \in \mathbb{C}[X]$ un polynôme à racines simples. Alors pour tout $0 \leq i \leq d(P) - 2$ on a*

$$\sum_{w \text{ racine de } P} \frac{w^i}{P'(w)} = 0$$

DÉMONSTRATION : Fixons un entier i compris entre 0 et $d(P) - 2$. Notons $Q(X)$ le monôme X^i. Supposons (dans un premier temps) que 0 n'est pas racine de P. Alors, si w est un zéro (simple) de P, $\frac{w^i}{P'(w)}$ est le résidu en w de $\frac{Q}{P}$. Donc la somme considérée dans l'énoncé du lemme est la somme des résidus de la fraction rationnelle $\frac{Q}{P}$ en tous ses pôles complexes. Cette somme est égale à l'opposé du résidu à l'infini de $\frac{Q}{P}$. Or ce résidu à l'infini est nul car $d(Q) \leq d(P) - 2$. Le lemme est donc démontré, dans le cas où 0 n'est pas racine de P. Dans le cas contraire, pour $w = 0$, $\frac{w^i}{P'(w)}$ vaut 0 si $i \geq 1$ et $\frac{1}{P'(0)}$ si $i = 0$; c'est aussi la valeur du résidu en 0 de $\frac{Q}{P}$ (puisque P est à racines simples, $\frac{Q}{P}$ n'admet pas de pôle en 0 si $i \geq 1$). Donc le raisonnement précédent s'applique sans autre modification, ce qui termine la démonstration du lemme.

N.B. Cette démonstration utilise la notion de résidu, donc n'est valable a priori que dans $\mathbb{C}$. En fait, on peut démontrer ce résultat en remplaçant $\mathbb{C}$ par n'importe quel corps algébriquement clos de caractéristique nulle.

Les propositions suivantes constituent, en quelque sorte, des réciproques aux propositions 5 et 6 :

Proposition 7 *Soit (R, S) un couple de polynômes premiers entre eux, unitaires, dont l'un au moins est non constant, tels que $\frac{R'}{R} - \frac{S'}{S}$ soit l'inverse d'un polynôme de degré au moins 2. Alors R et S sont de même degré non nul, et $(R, S) \in M$, c'est-à-dire $\varrho(RS) = d(R) - d(R - S) + 1$.*

Proposition 8 *Soit r une fraction rationnelle telle que $\frac{r}{r'}$ soit un polynôme P de degré au moins 2. Alors il existe une constante non nulle λ telle que $\lambda r \in M$.*

Ces deux propositions sont visiblement équivalentes, chacune étant la traduction de l'autre (noter cependant l'hypothèse selon laquelle R et S sont unitaires dans la proposition 7). Il est donc inutile, du point de vue logique, de donner une démonstration de chacune. C'est toutefois ce qu'on fait, car les deux démonstrations sont intéressantes.

DÉMONSTRATION de la proposition 8 : Tout d'abord, la condition $\frac{r}{r'} = P$ se traduit, en écrivant $r = \prod_i (X - x_i)^{n_i}$, et en écrivant de deux manières la décomposition en éléments simples de $\frac{1}{P}$, par $n_i = \frac{1}{P'(x_i)}$. Le lemme 3, appliqué avec $k = 0 \leq d(P) - 2$, montre que la somme des n_i est nulle. Donc r envoie l'infini sur un complexe non nul, d'où l'existence de λ tel que $\lambda r(\infty) = 1$. Quitte à remplacer r par λr, on peut supposer $r(\infty) = 1$. Montrons maintenant que tout point de $\mathbb{P}^1(\mathbb{C})$ en lequel r est ramifiée est au-dessus de $\{0, 1, \infty\}$. Pour cela, soit $z \in \mathbb{P}^1(\mathbb{C})$ en lequel r est

ramifiée. Si $z = \infty$, ou si $r(z) = \infty$, il n'y a rien à démontrer. Dans les autres cas, le fait que r soit ramifiée en z montre que $r'(z) = 0$ (d'après le lemme 2). Comme z ne peut pas être un pôle du polynôme $\frac{r}{r'}$, on a $r(z) = 0$, ce qu'on voulait démontrer.

DÉMONSTRATION de la proposition 7 : Notons (x_i) la famille des racines du polynôme RS. Pour chaque indice i, on note p_i l'ordre de x_i comme zéro de S, et q_i son ordre comme zéro de S. Puis on pose $n_i = p_i - q_i$: c'est l'ordre en x_i de $\frac{R}{S}$. Comme R et S sont premiers entre eux, pour chaque indice i exactement l'un des deux entiers p_i et q_i est nul. Par hypothèse, il existe un polynôme P tel que $\frac{1}{P} = \frac{R'}{R} - \frac{S'}{S} = \sum_i \frac{n_i}{X - x_i}$. Par unicité de la décomposition en éléments simples de $\frac{1}{P}$, on a $n_i = \frac{1}{P'(x_i)}$. Tout d'abord, le lemme 3 appliqué avec $k = 0$ donne $\sum_i p_i = \sum_i q_i$ donc R et S sont de même degré. Ensuite, le même lemme 3 montre que, pour tout k compris entre 0 et $u - 2$ (où u désigne le degré de P, qui est le nombre de racines du polynôme RS), on a $\sum_i n_i x_i^k = 0$, c'est-à-dire $\sum_i p_i x_i^k = \sum_i q_i x_i^k$: les sommes de Newton d'indices $0 \leq k \leq u - 2$ sont les mêmes pour les familles des zéros de R et de S. Donc les fonctions symétriques de ces racines, de degré au plus $u - 2$, sont les mêmes pour R et pour S : R et S (qui sont unitaires) ont les mêmes coefficients de degrés $d(R)$, $d(R) - 1$, ... , $d(R) - u + 2$. Donc $R - S$ est de degré au plus $d - u + 1$: on a $d(R - S) \leq d(R) - \varrho(RS) + 1$. Le corollaire 1 montre alors qu'il y a égalité, d'où le résultat.

3.4 Enoncés et démonstrations du théorème de classification

NOTATION : notons U l'ensemble des polynômes séparables (i.e. à racines simples) unitaires $P = (X - x_1) \cdot \ldots \cdot (X - x_k)$, de degré k supérieur ou égal à 2, tels que les nombres complexes $q_{i,j} = \frac{P'(x_i)}{P'(x_j)}$ soient rationnels pour tous $1 \leq i, j \leq k$.

NOTATION : notons L l'ensemble des familles finies de complexes $(x_1, \ldots, x_k)$ deux à deux distincts (avec $k \geq 2$) telles que le polynôme $P = (X - x_1) \cdot \ldots \cdot (X - x_k)$ appartienne à U. C'est l'ensemble des familles finies de complexes $(x_1, \ldots, x_k)$ deux à deux distincts telles que les nombres complexes $\prod_{h \neq i,j} \frac{x_h - x_i}{x_h - x_j}$ soient rationnels, pour tous $1 \leq i, j \leq k$.

En particulier, les polynômes unitaires à coefficients rationnels scindés sur $\mathbb{Q}$ et à racines simples appartiennent à U ; les familles de k rationnels deux à deux distincts (avec $k \geq 2$) appartiennent à L.

Ces notations L et U apparaissent dans [14], ainsi que le théorème suivant :

Théorème 4 *: L'application qui à r associe $r^{-1}(\{0, \infty\})$ établit une bijection entre $M/\mathcal{R}$ et L.*

Ce théorème peut se reformuler de deux façons équivalentes :

Théorème 5 *: L'application qui à (R, S) associe $u(RS)$ établit une bijection entre $M/\mathcal{R}$ et U.*

Théorème 6 *: L'application qui à r associe $\lambda \frac{r}{r'}$, où λ est l'unique constante complexe permettant de rendre le polynôme $\frac{r}{r'}$ unitaire, établit une bijection entre $M/\mathcal{R}$ et U.*

N.B. Dans le théorème 6, la constante λ dépend du représentant $r \in M$ choisi, mais le polynôme $\lambda \frac{r}{r'}$ ne dépend pas de ce représentant (au sein d'une classe d'équivalence).

Le théorème 6 peut se formuler de façon plus précise, compte tenu de la proposition 8 :

Théorème 7 *Soient r une fraction rationnelle non constante et P un polynôme de degré au moins 2 tels que $P = \frac{r}{r'}$. Notons μ la constante telle que μP soit unitaire. Alors :*

1. *On a $\mu P \in U$.*
2. *Il existe une constante $\nu \in \mathbb{C}^\star$ telle que $\nu r \in M$.*
3. *Pour toute fraction rationnelle s telle que $\frac{s}{s'}$ soit égal à P (à une constante multiplicative près), il existe un nombre complexe non nul ξ et deux entiers relatifs non nuls a et b tels que $(\nu r)^a = (\xi s)^b$.*

Il est clair que les théorèmes 4, 5 et 6 sont équivalents, puisque si $r = \frac{R}{S} \in M$, la proposition 5 montre que $\frac{r}{r'} = \frac{1}{c}u(RS)$, où c est une constante non nulle.

Toutefois, on donne deux démonstrations de ces théorèmes; la première utilise les fractions rationnelles, et la seconde (tirée de [14]) utilise les couples de polynômes.

DÉMONSTRATION du théorème 6 :

- Tout d'abord, il est clair que l'application définie sur M, qui à r associe $\lambda\frac{r}{r'}$, où λ est l'unique constante complexe permettant de rendre le polynôme $\frac{r}{r'}$ unitaire, passe au quotient par la relation d'équivalence $\mathcal{R}$. Elle définit donc une application ϕ sur $M/\mathcal{R}$.
- Cette application ϕ est à valeurs dans $\mathbb{C}[X]$ d'après la proposition 6 : l'image de r est le polynôme $P = \prod_{w \in r^{-1}(\{0,\infty\})}(X - w)$. Notons λ l'unique constante telle que $P = \lambda\frac{r}{r'}$. L'unicité de la décomposition en éléments simples de $\frac{1}{P}$ montre que l'ordre de tout zéro w de P comme zéro ou pôle de r est $\frac{\lambda}{P'(w)}$. Donc le quotient des valeurs prises par P' en deux zéros de P est l'inverse du quotient des ordres de ces points, vus comme zéros ou pôles de r : c'est toujours un rationnel, et le polynôme P (qui est unitaire et séparable) appartient à U. C'est pourquoi ϕ est bien à valeurs dans U.
- Montrons que ϕ est injective. Soient r et s deux éléments de M tels qu'il existe une constante μ non nulle avec $\frac{r}{r'} = \mu\frac{s}{s'}$. Notons $r = \prod_i (X - x_i)^{n_i}$ et $s = \prod_j (X - y_j)^{m_j}$. On a : $\sum_j \frac{m_j}{X - y_j} = \frac{s'}{s} = \mu\frac{r'}{r} = \mu\sum_i \frac{n_i}{X - x_i}$ Par unicité du développement en éléments simples d'une fraction rationnelle, on en déduit que $\mu \in \mathbb{Q}$; en écrivant $\mu = \frac{a}{b}$, on a $r^a = s^b$. D'où l'injectivité de ϕ.
- Montrons que ϕ est surjective. Soit $P \in U$. Notons λ un complexe non nul tel que $\frac{\lambda}{P'}$ prenne des valeurs entières aux zéros de P. Un tel λ existe car $P \in U$. Notons r la fraction rationnelle (définie à constante multiplicative non nulle près) ayant pour zéros et pôles les racines de P, avec pour multiplicités respectives les entiers $\frac{\lambda}{P'(w)}$ (cette multiplicité étant négative pour les w pôles de r, et positive pour les zéros). On a alors $\frac{\lambda}{P} = \frac{r'}{r}$ (par égalité de leur décomposition en éléments simples) soit $P = \lambda\frac{r}{r'}$. De plus, r admet $\sum_{w \text{ racine de } P \text{ telle que } \frac{\lambda}{P'(w)} > 0} \frac{\lambda}{P'(w)}$ zéros, comptés avec multiplicités, et $-\sum_{w \text{ racine de } P \text{ telle que } \frac{\lambda}{P'(w)} < 0} \frac{\lambda}{P'(w)}$ pôles. D'après le lemme 3, appliqué avec $i = 0$, elle a autant de zéros que de pôles, donc son numérateur et son dénominateur sont de même degré : elle envoie l'infini sur un nombre complexe non nul. Comme r est définie à constante multiplicative non nulle près, on peut supposer que $r(\infty) = 1$. Montrons que $r \in M$. D'après la proposition 8, il suffit de montrer que $\frac{r}{r'}$ est un polynôme, c'est-à-dire que $\frac{r'}{r}$ admet l'infini pour seul zéro. Donc il suffit de démontrer que $\frac{r'}{r}$ s'annule à l'infini, avec un ordre (au moins) égal à son degré, qui est celui de $\frac{\lambda}{P}$, donc

celui de P. Pour cela, on écrit le développement limité en zéro de $\frac{r'}{r}(\frac{1}{z})$:

$$\begin{aligned}\frac{r'}{r}(\frac{1}{z}) &= \sum_{P(w)=0} \frac{\lambda}{P'(w)} \frac{1}{\frac{1}{z}-w} \\ &= \sum_{P(w)=0} \frac{\lambda}{P'(w)} \frac{z}{1-zw} \\ &= \sum_{P(w)=0} \frac{\lambda}{P'(w)} z(1+wz+w^2z^2+w^3z^3+\cdots)\end{aligned}$$

D'après le lemme 3, le coefficient de z^i dans ce développement est nul pour $i \leq d(P)-1$. Donc l'infini est zéro de $\frac{r'}{r}$ d'ordre au moins égal à $d(P)$, ce qui achève la démonstration.

DÉMONSTRATION du théorème 5 (d'après [14]) :

- L'application qui à (R,S) associe $u(RS)$ est définie sur M, et passe au quotient pour définir une application ψ de $M/\mathcal{R}$ dans $\mathbb{C}[X]$.
- Pour montrer qu'elle est à valeurs dans U, notons $P=u(RS)$ et écrivons [1] $\frac{R}{S}=\prod_i (X-x_i)^{n_i}$. La dérivée logarithmique de cette égalité donne, d'après la proposition 5, $\sum_i \frac{n_i}{X-x_i} = \frac{c}{u(RS)}$ pour une certaine constante c non nulle. Par unicité du développement en éléments simples de $\frac{1}{u(RS)} = \frac{1}{\prod_i (X-x_i)} = \sum_i \frac{1}{P'(x_i)} \frac{1}{X-x_i}$, il vient $n_i = \frac{c}{P'(x_i)}$. Donc les quotients $\frac{P'(x_i)}{P'(x_j)} = \frac{n_j}{n_i}$ sont rationnels. Comme P est unitaire et séparable, P appartient donc à U : ψ est à valeurs dans U.
- L'argument précédent montre aussi que ψ est injective : si (R_1,S_1) et (R_2,S_2) ont la même image par ψ alors il existe des nombres complexes x_i et des entiers relatifs p_i et q_i tels que $\frac{R_1}{S_1}=\prod_i (X-x_i)^{p_i}$, $\frac{R_2}{S_2}=\prod_i (X-x_i)^{q_i}$ et, pour tous entiers i et j, $\frac{p_j}{p_i}=\frac{q_j}{q_i}$. Donc il existe des entiers relatifs n_i, et des facteurs de proportionnalité (entiers relatifs non nuls) p et q tels que pour tout i on ait $p_i=pn_i$ et $q_i=qn_i$. En notant $\frac{R}{S}=\prod_i (X-x_i)^{n_i}$ (avec R et S premiers entre eux, unitaires), on voit que $\frac{R_1}{S_1}=(\frac{R}{S})^p$ et $\frac{R_2}{S_2}=(\frac{R}{S})^q$. Donc les éléments (R_1,S_1) et (R_2,S_2) de M définissent le même élément de $M/\mathcal{R}$: l'application ψ est injective.
- Montrons que ψ est surjective. Soit $P \in U$. Pour construire (R,S), on utilise la condition nécessaire vue ci-dessus. Le fait que P appartienne à U montre qu'il existe un nombre complexe c non nul tel que les quotients $\frac{c}{P'(x_i)}$ (où les x_i sont les zéros de P) soient des entiers relatifs n_i, premiers entre eux dans leur ensemble. En notant $\frac{R}{S}=\prod_i (X-x_i)^{n_i}$ (avec R et S premiers entre eux, unitaires), on définit un couple (R,S) tel que $\frac{R'}{R}-\frac{S'}{S}=\frac{c}{P}$. On a alors $(R,S) \in M$. La vérification de ce dernier point [2] résulte de la proposition 7.

N.B. Cette démonstration est simplement la traduction en termes de polynômes de la démonstration du théorème 6 donnée précédemment. En particulier, le N.B. qui suit cette démonstration reste valable.

3.5 Synthèse, exemples

Le théorème ci-dessous se déduit aisément des résultats précédents. Il donne un critère pour savoir si une fraction rationnelle donnée appartient ou non à M, et permet d'exhiber des éléments de M.

1. Noter ici l'erreur probable dans [14].
2. Cette vérification est sous-entendue dans [14].

Théorème 8 (Synthèse) *Soit $r = \prod_{i=1}^{t}(X - x_i)^{n_i}$ une fraction rationnelle non constante (avec $n_i \in \mathbb{Z} - \{0\}$, et les x_i deux à deux distincts).*

Posons $P = \prod_{i=1}^{t}(X - x_i)$.

Alors r appartient à M si, et seulement si, il existe un nombre complexe λ tel que pour tout $1 \leq i \leq t$ on ait $n_i = \frac{\lambda}{P'(x_i)}$.

De plus, si r appartient à M, on a : $\frac{r'}{r} = \frac{\lambda}{P}$.

N.B. Avec les notations du théorème, on a la formule (déjà évoquée dans un N.B. qui suit l'énoncé de la proposition 6) :

$$\lambda = (-1)^{t-1} \sum_{i=1}^{t} n_i \prod_{j \neq i} x_j$$

N.B. Ce théorème affirme que pour toute famille $(x_i)_{1 \leq i \leq k}$ qui appartient à L, en particulier pour toute famille de $k \geq 2$ rationnels deux à deux distincts, il existe un cas d'égalité non trivial r dont les racines et les pôles sont exactement les x_i.

Grâce à ce théorème, à chaque polynôme de U on peut associer des éléments de M (on trouve en fait une classe d'équivalence modulo $\mathcal{R}$, selon le choix de λ). Ainsi, soient a et b deux entiers naturels non nuls distincts. Posons $P = (X + a)(X - a)(X + b)(X - b)$. Alors $P \in U$, et on a $P'(\pm a) = \pm 2a(a + b)(a - b)$ et $P'(\pm b) = \pm 2b(b + a)(b - a)$. Comme constante λ on peut prendre $2ab(a + b)(a - b)$, ce qui montre que la fraction rationnelle $\frac{(X-a)^b(X+b)^a}{(X+a)^b(X-b)^a}$ appartient à M.

Soient encore a et b deux entiers naturels non nuls distincts. Posons $P = X(X^2 - a)(X^2 - b)$. Les valeurs prises par P' aux zéros (complexes) de P sont $P'(0) = ab$, $P'(\pm\sqrt{a}) = 2a(a - b)$ et $P'(\pm\sqrt{b}) = 2b(b - a)$. On a donc $P \in U$ (ce qui donne, quand a ou b n'est pas un carré parfait, des exemples de polynômes à racines non toutes rationnelles mais qui appartiennent à U). En prenant $\lambda = 2ab(a - b)$, cela montre que la fraction rationnelle $\frac{X^{2(a-b)}(X^2-a)^b}{(X^2-b)^a}$ appartient à M.

Les deux exemples précédents se trouvent dans [14]; le deuxième n'y apparaît que dans le cas où a et b sont des carrés parfaits (ce qui signifie que le polynôme P est scindé sur $\mathbb{Q}$)[3].

Revenons au problème de Tarry-Escott formulé au paragraphe 1.5. Parmi les exemples de cas d'égalité non triviaux cités ci-dessus, la paire suivante est solution du problème de Tarry-Escott :

$$(X - 2)(X + 1)^2 \text{ et } (X + 2)(X - 1)^2$$

Ce couple (R, S) de polynômes est à la fois une solution du problème de Tarry-Escott et un cas d'égalité non trivial.

On peut chercher d'autres cas d'égalité non triviaux (R, S) tels que $R - S$ soit constant, mais sans imposer que R et S soient à racines entières. Cela revient à chercher les couples (R, S) de polynômes de même degré $d > 0$ qui vérifient $\varrho(RS) = d + 1$ et tels que $R - S$ est constant non nul. Ces couples correspondent exactement aux fonctions $r = \frac{R}{S}$ qui appartiennent à M, et telles que l'infini soit le seul antécédent de 1. Si on pose $s = \frac{1}{1-r}$, ce qui établit une correspondance bijective entre les fonctions r et les fonctions s, cela signifie que s est ramifiée seulement au-dessus de $\{0, 1, \infty\}$, et que l'unique antécédent de l'infini est l'infini. Autrement dit, s est un polynôme ramifié seulement au-dessus de 0 et de 1 (et, bien sûr, de l'infini). Un tel polynôme s'appelle un polynôme de Tchebychev généralisé (par analogie avec les polynômes de Tchebychev habituels, qui sont ramifiés seulement au-dessus de -1 et de 1). L'étude de ces polynômes intervient dans la théorie des dessins d'enfants.

3. Noter aussi la présence d'une faute de frappe.

4 Application de l'étude des cas d'égalité

4.1 Notations; énoncé du théorème 9

Dans cette section, on considère des polynômes à coefficients entiers. On adopte la définition suivante :

DÉFINITION : On appelle *contenu* d'un polynôme $P \in \mathbb{Z}[X]$ le pgcd de ses coefficients.

N.B. Le lemme de Gauss affirme que le contenu du produit de deux polynômes est le produit de leurs contenus.

Grâce à cette définition, on a une nouvelle notion de radical d'un polynôme $P \in \mathbb{Z}[X]$. En effet, la notation $u(P)$ utilisée jusqu'ici ne convient pas : même si P est à coefficients entiers, $u(P)$ (qui est le polynôme unitaire dont les racines, simples, sont celles de P) ne l'est pas en général. On adopte donc la notation suivante :

NOTATION : Soit $P = \alpha \prod_i P_i^{n_i}$ un polynôme non nul écrit comme produit de $\alpha \in \mathbb{Z} - \{0\}$ et de puissances de polynômes $P_i \in \mathbb{Z}[X]$ irréductibles, de contenu 1. On pose alors :

$$\tilde{u}(P) = \mathrm{rad}(\alpha) \prod_i P_i$$

N.B. Dans l'écriture $P = \alpha \prod_i P_i^{n_i}$, α est nécessairement (au signe près) le contenu de P. D'autre part, comme les $P_i \in \mathbb{Z}[X]$ sont de contenu 1, ils sont irréductibles dans $\mathbb{Z}[X]$ si, et seulement si, ils le sont dans $\mathbb{Q}[X]$.

A contrario, pour les cas où veut travailler à constante multiplicative près, on adopte la notation suivante :

NOTATION : Pour $P, Q \in \mathbb{C}[X]$, on note $P \doteq Q$ s'il existe une constante $\lambda \neq 0$ telle que $Q = \lambda P$.

N.B. Le fait de remplacer l'égalité par le symbole $\doteq$ permet de s'affranchir des problèmes de normalisation du coefficient dominant. C'est utile principalement quand on se sert du radical de P, ou de l'ensemble U (dont les éléments sont, par définition, unitaires).

Avant d'énoncer le théorème qui est au centre de cette section, on rappelle la définition suivante :

DÉFINITION (rappel) : un polynôme P est dit séparable si ses racines (dans $\mathbb{C}$) sont simples; si $P \in \mathbb{Z}[X]$, cela signifie qu'aucun facteur multiple n'apparaît dans sa décomposition en facteurs premiers dans $\mathbb{Z}[X]$.

On peut maintenant formuler le théorème suivant, qui figure dans [15] et dont la démonstration fait l'objet du reste de cette section :

Théorème 9 *Pour tout $P \in \mathbb{Z}[X]$ séparable, dont le contenu est sans facteur carré, il existe $(R, S) \in M$, avec R et S à coefficients entiers, tels que P divise $\tilde{u}(RS)$ dans $\mathbb{Z}[X]$. Si on note $r = \frac{R}{S}$, cela signifie que r est définie sur $\mathbb{Q}$, appartient à M, et envoie les racines de P dans $\{0, \infty\}$.*

Pour démontrer ce théorème, on aura besoin d'exhiber la fonction r (ou le couple (R, S)). Le théorème 8 permet de construire toutes les fractions rationnelles $r \in M$ dont les zéros et les pôles sont rationnels. Mais il n'est pas facile d'obtenir d'autres fractions rationnelles $r \in M$. On en a donné quelques-unes dans l'exemple du paragraphe 3.5; le but du paragraphe suivant est de décrire comment en construire d'autres.

4.2 Une façon d'obtenir de nouveaux cas d'égalité non triviaux

Tout d'abord, citons un lemme qui sera utile pour formuler la proposition 9 :

Lemme 4 *Soient $P \in \mathbb{C}[X]$ séparable et $T \in \mathbb{C}[X]$ non constant tels que T' divise $P(T)$. Alors $\frac{P\circ T}{T'} \doteq u(P \circ T)$.*

DÉMONSTRATION du lemme : Soit w une racine de $P(T)$, d'ordre n. Son ordre comme racine de $T(X) - T(w)$ est n (et pas moins, car P est séparable). Donc w est racine de T', d'ordre $n-1$. C'est pourquoi w est racine simple de $\frac{P\circ T}{T'}$. De plus, toute racine de $\frac{P\circ T}{T'}$ est une racine de $P(T)$. D'où le lemme.

L'objectif de ce paragraphe est de démontrer les deux propositions ci-dessous, dont l'équivalence sera justifiée plus bas :

Proposition 9 *Soient $P \in U$ et $T \in \mathbb{C}[X]$ non constant tels que $T' \mid P(T)$. Alors :*

$$\frac{P(T)}{T'} \doteq u(P(T)) \in U$$

Proposition 10 *Soient $r \in M$ et $T \in \mathbb{C}[X]$ non constant tels que T' divise le polynôme $\frac{r}{r'}(T)$. Alors $r \circ T \in M$.*

N.B. Le fait que $\frac{r}{r'}$ soit un polynôme résulte de la proposition 6.

Ces propositions permettent donc, à partir d'un élément $r \in M$ (ou du polynôme P associé), d'en construire d'autres. Toutefois, on a besoin d'un polynôme T tel que T' divise $P(T)$. Plutôt que de chercher un tel polynôme T à P fixé, on raisonne dans l'autre sens : on fixe T, et on cherche un polynôme P tel que T' divise $P(T)$. C'est le rôle du lemme suivant :

Lemme 5 *Soit T un polynôme non constant. On note $Aux_T(X) = \prod_{\xi \text{ racine de } T'}(X - T(\xi))$ le résultant des polynômes $X - T(Z)$ et $T'(Z)$ en l'indéterminée Z. Alors T' divise $Aux_T(T)$.*

DÉMONSTRATION du lemme 5 : On a $Aux_T \circ T = \prod_{\xi \text{ racine de } T'}(T(X) - T(\xi))$. Or, si w est zéro de T' d'ordre n, il est zéro d'ordre $n+1$ de $T(X) - T(w)$ donc il est zéro d'ordre au moins $n+1$ de $Aux_T \circ T$. Cela démontre le lemme.

Signalons un cas dans lequel la proposition 10 s'applique :

Lemme 6 *Soient $r \in M$ et T un polynôme non constant tels que chaque zéro de T' soit un zéro ou un pôle de $r \circ T$. Alors T' divise le polynôme $\frac{r}{r'}(T)$.*

DÉMONSTRATION du lemme 6 : Soit w un zéro de T'. Alors $T(w)$ est un zéro ou un pôle de r, donc c'est un pôle de $\frac{r'}{r}$, c'est-à-dire un zéro de $\frac{r}{r'}$. Donc w est un zéro de $\frac{r}{r'}(T)$. De plus, la dérivée de $\frac{r}{r'}(T)$ admet (puisque $\frac{r}{r'}$ est un polynôme, car $r \in M$) w comme zéro, avec une multiplicité au moins égal à son ordre comme racine de T'. Donc l'ordre de w comme zéro de $\frac{r}{r'}(T)$ est (strictement) plus grand que son ordre comme zéro de T'. Cela conclut la démonstration du lemme 6.

Revenons maintenant aux propositions 9 et 10. Leur équivalence résulte du calcul suivant, où r et P se correspondent comme au théorème 6 (i.e. $P = \lambda \frac{r}{r'}$ avec $\lambda \in \mathbb{C}^\star$) :

$$\frac{r \circ T}{(r \circ T)'} = \frac{1}{T'}\left(\left(\frac{r}{r'}\right) \circ T\right) = \frac{P \circ T}{\lambda T'} \tag{2}$$

En effet, pour démontrer que la proposition 9 implique la proposition 10, il suffit (compte tenu de (2)) d'appliquer la proposition 8 à $r \circ T$, étant donné que la constante λ fournie par cette

proposition vaut 1, puisque $r \circ T(\infty) = r(\infty) = 1$. Pour démontrer la réciproque, on applique (2) et le théorème 6 qui assurent que, à multiplication près par un complexe non nul, $\frac{P \circ T}{T'}$ appartient à U. La séparabilité suffit alors pour affirmer qu'on a $u(P \circ T) \doteq \frac{P \circ T}{T'}$, grâce au lemme 4.

On va donner trois démonstrations des propositions équivalentes 9 et 10. La première utilise les éléments de M vus comme des fractions rationnelles. La deuxième raisonne directement sur les polynômes $P \in U$. Enfin, la troisième utilise les éléments de M vus comme couples de polynômes.

DÉMONSTRATION de la proposition 10 (par les fractions rationnelles) : Soient $r \in M$ et $T \in \mathbb{C}[X]$ tels que T' divise le polynôme $\frac{r}{r'}(T)$. Tout d'abord, T étant un polynôme non constant, on a $T(\infty) = \infty$ donc $r \circ T(\infty) = r(\infty) = 1$. Il suffit donc de démontrer que $r \circ T$ est ramifiée seulement en l'infini et au-dessus de $\{0, \infty\}$. Soit $z \in \mathbb{P}^1(\mathbb{C})$ en lequel $r \circ T$ est ramifiée. Si $z = \infty$ ou si $r \circ T(z) = \infty$, il n'y a rien à démontrer. Sinon, le lemme 2 affirme que $(r \circ T)'(z) = 0$, c'est-à-dire $T'(z) = 0$ ou $r'(T(z)) = 0$. Dans le premier cas, comme $T' \mid \frac{r \circ T}{r' \circ T}$, z est au-dessus de 0 pour $r \circ T$. Dans le second cas, $T(z)$ est un point de $\mathbb{C}$ où r' s'annule, donc où r est ramifiée (par le lemme 2). D'où $r(T(z)) \in \{0, \infty\}$, ce qu'il fallait démontrer.

DÉMONSTRATION de la proposition 9, tirée de [15] : Soient $P \in U$ et $T \in \mathbb{C}[X]$ non constant tels que $T' \mid P(T)$. D'après le lemme 4, il suffit de démontrer qu'une fois rendu unitaire, $\frac{P \circ T}{T'}$ appartient à U. Pour cela, posons $Q = \alpha \frac{P \circ T}{T'}$, où α est la constante non nulle telle que Q soit unitaire. On a

$$Q'(X) = \alpha \frac{(P' \circ T)(X)T'(X) - (P \circ T)(X)T''(X)}{T'(X)^2} \tag{3}$$

Soit w un zéro de $P(T)$, d'ordre $n_w \geq 1$. Alors n_w est aussi l'ordre de w comme zéro de $T(X) - T(w)$ (car P est séparable). On peut donc écrire $T(X) - T(w) = (X - w)^{n_w} T_1(X)$ avec $T_1(w) \neq 0$. Ce développement limité permet de lever l'indétermination qui apparaît quand on évalue la formule (3) avec $X = w$. Le calcul donne :

$$Q'(w) = \frac{\alpha}{n_w}(P' \circ T)(w) \tag{4}$$

Soient maintenant w_1 et w_2 deux racines de $P(T)$, d'ordres respectifs n_1 et n_2. La formule (4) permet d'écrire :

$$\frac{Q'(w_1)}{Q'(w_2)} = \frac{n_2}{n_1} \frac{P'(T(w_1))}{P'(T(w_2))}$$

Comme $T(w_1)$ et $T(w_2)$ sont des racines de $P \in U$, cette formule démontre que $\frac{Q'(w_1)}{Q'(w_2)}$ est rationnel. Donc $Q = \alpha \frac{P \circ T}{T'} \in U$, ce qu'il fallait démontrer.

N.B. Dans la deuxième démonstration, un calcul donne la formule (4). En fait, cette formule s'interprète aisément dans le langage des fractions rationnelles, du moins à condition d'admettre la proposition 10 : soit $r \in M$ qui correspond (par la bijection du théorème 6) à $P \in U$. Alors, par cette proposition, $r \circ T \in M$ correspond au polynôme unitaire $Q = \alpha \frac{P \circ T}{T'} \in U$. Or, d'après les théorèmes 6 et 8, on sait que la correspondance entre P et r se traduit par l'existence d'une constante λ_P telle que toute racine w de P soit zéro ou pôle de r, avec pour ordre (algébrique) $\frac{\lambda_P}{P'(w)}$. On a alors $\frac{r'}{r} = \frac{\lambda_P}{P}$. De même, il existe λ_Q telle que toute racine w de Q soit zéro ou pôle de $r \circ T$, avec pour ordre (algébrique) $\frac{\lambda_Q}{Q'(w)}$; on a $\frac{(r \circ T)'}{r \circ T} = \frac{\lambda_Q}{Q}$. La relation (2) permet d'écrire :

$$\frac{\lambda_Q}{Q} = \frac{(r \circ T)'}{r \circ T} = T' \frac{r'}{r} \circ T = \frac{\lambda_P T'}{P \circ T}$$

On a donc : $\alpha = \frac{\lambda_Q}{\lambda_P}$. L'égalité (4) s'écrit alors, pour w zéro de $P(T)$ (c'est-à-dire pour w zéro de $u(P(T)) = Q$ par le lemme 4) d'ordre n_w :

$$\frac{\lambda_Q}{Q'(w)} = n_w \frac{\lambda_P}{P'(T(w))}$$

Sous cette forme, cette formule est exactement la traduction de l'égalité connue (puisque n_w est aussi l'ordre de w comme zéro de $T(X) - T(w)$, c'est-à-dire l'indice de ramification de T en w) :

$$ord_w(r \circ T) = n_w ord_{T(w)}(r)$$

Donnons enfin une troisième démonstration des propositions équivalentes 9 et 10, qui utilise les éléments de M vus comme des couples de polynômes.

DÉMONSTRATION de la proposition 10 (tirée de [14], où elle n'est qu'esquissée; elle est précisée dans [15]). Soient $(R, S) \in M$ et $T \in \mathbb{C}[X]$ non constant tels que T' divise le polynôme $P(T)$, où P est défini par l'existence d'une constante non nulle λ telle que $P = \lambda \frac{r}{r'}$. Montrons que $(R(T), S(T)) \in M$. En effet, $R(T)$ et $S(T)$ ont même degré, même coefficient dominant, sont non constants, et on a :

$$\begin{aligned}
\varrho((RS) \circ T) &= \varrho(P \circ T) \text{ car } P \text{ et } RS \text{ ont les mêmes zéros} \\
&= 1 + d(T)(\varrho(P) - 1) \text{ par le lemme 7 ci-dessous} \\
&= 1 + d(T)(d(R) - d(R - S)) \text{ car } \varrho(P) = \varrho(RS) \text{ avec } (R, S) \in M \\
&= 1 + d(R \circ T) - d((R - S) \circ T)
\end{aligned}$$

D'où le résultat.

Le lemme utilisé dans cette démonstration fait l'objet du paragraphe suivant.

4.3 Un lemme polynômial élémentaire

La troisième démonstration de la proposition 10 a utilisé le lemme suivant :

Lemme 7 *Soient P et T deux polynômes à coefficients complexes. Alors*

$$\varrho(P \circ T) \geq d(T)(\varrho(P) - 1) + 1$$

avec égalité si, et seulement si, $T' \mid P(T)$.

DÉMONSTRATION : on peut démontrer ce lemme de manière directe. On peut aussi noter E l'ensemble des racines de P; le lemme s'écrit alors :

$$\text{Card}(T^{-1}(E)) - 1 \geq d(T)(\text{Card}(E) - 1) \tag{5}$$

Pour $x \in \mathbb{C}$, notons $e_x = 1 + \omega_x$ où ω_x est l'ordre (éventuellement nul) de x comme zéro de T'; c'est la multiplicité de x comme racine du polynôme $T(X) - T(x)$. On a la relation suivante :

$$\sum_{T(x)=c} e_x = d(T) \text{ pour tout } c \in \mathbb{C} \tag{6}$$

D'autre part, la relation suivante découle aussi des définitions :

$$\sum_{x \in \mathbb{C}} e_x - 1 = d(T') = d(T) - 1 \tag{7}$$

En restreignant la somme qui figure au membre de gauche aux x tels que $T(x) \in E$, et en appliquant la relation (6) à chaque élément c de E, on obtient :

$$d(T)\,\text{Card}(E) - \text{Card}(T^{-1}(E)) \leq d(T) - 1$$

Cette inégalité est exactement celle que l'on voulait démontrer; de plus, il y a égalité si, et seulement si, on ne perd rien en restreignant la somme aux x tels que $T(x) \in E$; cela signifie que les racines

de T' sont envoyées dans E par T. Comme $E = P^{-1}(0)$, cela veut dire que les racines de T' sont racines de $P \circ T$. Il est alors immédiat qu'une racine de T' de multiplicité k est racine de $P \circ T$ avec multiplicité au moins k (et même $k+1$). Donc les cas d'égalité dans l'inégalité du lemme sont exactement les cas où T' divise $P \circ T$. Cela conclut la démonstration du lemme.

N.B. La notation e_x introduite ici fait penser à l'indice de ramification. En effet, si on considère T comme une application de $\mathbb{P}^1$ dans $\mathbb{P}^1$ (qui est le cadre dans lequel ces indices ont été définis au paragraphe 1.3), la définition donnée au cours de la démonstration du lemme est un cas particulier de celle donnée pour les fractions rationnelles. Il en va de même pour la formule (6); quant à la notation $d(T)$ pour le degré du polynôme T, elle correspond au degré $\deg(T)$ de T vu comme fraction rationnelle. Enfin, la formule (7) s'écrit, en posant $g = 1/2$:

$$(2g-2)\,\deg(T) + \sum_{x \in \mathbb{C}} (e_x - 1) = 2g - 2 \tag{8}$$

C'est donc un analogue de la formule de Riemann-Hurwitz, en "genre $1/2$". Cette formule 8, dite de Riemann-Hurwitz, est valable dans le cadre général d'une application non constante f entre deux courbes lisses X et Y de même genre g (voir [28], page 41). On en déduit, de même que dans la démonstration du lemme 7, la formule suivante :

$$\mathrm{Card}(f^{-1}(E)) - (2-2g) \geq \deg(f)\,(\mathrm{Card}(E) - (2-2g)) \tag{9}$$

Cette formule donne comme cas particulier la formule (5). D'ailleurs, la démonstration de cette formule (9) à partir de la formule de Riemann-Hurwitz est la même que celle du lemme : il s'agit de minorer la ramification totale de f par celle au-dessus de E. De plus, il y égalité si, et seulement si, f est ramifiée seulement au-dessus de E.

Considérer le genre $1/2$ dans la formule de Riemann-Hurwitz peut sembler gênant; en fait, quand on s'intéresse à la formule (9), l'invariant à considérer est $\chi = 2-2g$, qui est la caractéristique d'Euler-Poincaré. Dans le cas de $\mathbb{C}$, il prend la valeur entière 1. Cette formule est aussi intéressante dans le cas où $X = Y = \mathbb{P}^1(\mathbb{C})$; dans ce cas, le genre g vaut 0 et la caractéristique χ vaut 2.

On peut comprendre la formule (9) en disant que dans cette formule, tout se passe comme si pour χ points de E on ne pouvait rien dire (sauf qu'ils ont au moins une image réciproque chacun), et que pour les autres on était sûr que chacun avait $\deg(f)$ images réciproques. La situation n'est, bien sûr, pas celle-là en général. Cependant, le cardinal de $f^{-1}(E)$ ne dépend que de $\sum_{x \in f^{-1}(E)} e_x - 1$, donc on peut "remplacer" f par une fonction de même degré qui est non ramifiée au-dessus de E, sauf peut-être au-dessus de χ points de E. Pour une telle fonction, les points de E autres que ces χ points ont chacun $\deg(f)$ antécédents. La formule (9) est évidente pour une telle fonction.

On peut voir χ comme le nombre maximal de points de Y tel qu'il existe une fonction f par laquelle chacun de ces points n'ait qu'un seul antécédent. C'est aussi le nombre minimal de points tel qu'il existe une fonction f de degré au moins 2 ramifiée seulement au-dessus de ces points. Par exemple, que l'on prenne $X = Y = \mathbb{C}$ ou $X = Y = \mathbb{P}^1(\mathbb{C})$, la fonction X^n convient (en considérant le point 0 dans le cas de $\mathbb{C}$, et l'ensemble $\{0, \infty\}$ dans le cas de $\mathbb{P}^1(\mathbb{C})$).

La remarque ci-dessus montre qu'on peut énoncer le lemme suivant :

Lemme 8 *Posons $X = \mathbb{C}$ ou $X = \mathbb{P}^1(\mathbb{C})$. Soit E une partie finie de X, et f une fonction de X dans X (i.e. un polynôme si $X = \mathbb{C}$, une fraction rationnelle si $X = \mathbb{P}^1(\mathbb{C})$), non constante.*

Alors, en notant χ la caractéristique d'Euler de X (qui vaut 1 pour $\mathbb{C}$ et 2 pour $\mathbb{P}^1(\mathbb{C})$), on a :

$$\mathrm{Card}(f^{-1}(E)) - \chi \geq \deg(f)\,(\mathrm{Card}(E) - \chi) \tag{10}$$

De plus, on a égalité si, et seulement si, f est ramifiée seulement au-dessus de E.

Ce lemme est démontré dans la remarque ci-dessus, à partir de la formule de Riemann-Hurwitz. Voici une autre démonstration de ce résultat, à partir de la formule d'Euler sur les graphes :

DÉMONSTRATION du lemme 8 : Supposons dans un premier temps que f est ramifiée seulement au-dessus de E. Montrons que, dans ce cas, on a l'égalité dans la formule (10).

Soit Γ un graphe tracé sur X ayant pour sommets les points de E. On considère ce graphe comme étant l'ensemble formé par ses A arêtes, ses S sommets et ses F faces (il convient de compter la face "extérieure" si $X = \mathbb{P}^1(\mathbb{C})$, et de ne pas la compter si $X = \mathbb{C}$). On a alors la relation d'Euler :

$$S - \chi = A - F$$

Notons Γ' le graphe obtenu en prenant l'image réciproque par f de Γ. Notons A' (respectivement S', F') le nombre d'arêtes (respectivement de sommets, de faces) de Γ'. Comme f est non ramifiée au-dessus des arêtes (extrémités non comprises) de Γ, chaque arête a exactement $\deg(f)$ images réciproques, ce qui s'écrit :

$$A' = A \deg(f)$$

La relation analogue est vraie pour les faces. En effet, on peut choisir des "centres" des F faces de Γ, le mot "centre" désignant simplement un point qui appartient à une face, frontières non comprises. Chacun de ces F centres a exactement $\deg(f)$ antécédents par f (car f est non ramifiée, sauf au-dessus des sommets de Γ). On obtient ainsi $F \deg(f)$ points, qui appartiennent à des faces de Γ' (frontières non comprises), tels que toute face de Γ' contienne exactement un de ces points. On a donc bien la relation :

$$F' = F \deg(f)$$

On déduit des deux relations ci-dessus, et de la relation d'Euler appliquée à Γ et à Γ', la formule suivante :

$$S' - \chi = (S - \chi) \deg(f)$$

Comme S est le cardinal de E, et S' celui de $f^{-1}(E)$, la démonstration est terminée dans le cas où f est ramifiée seulement au-dessus de E.

Dans le cas général, notons D l'ensemble des points de X n'appartenant pas à E et au-dessus desquels f est ramifiée. Notons δ le cardinal de D. On peut appliquer à la réunion de E et D le résultat partiel déjà démontré. Cela donne :

$$\mathrm{Card}(f^{-1}(E \cup D)) - \chi = \deg(f)\,(\mathrm{Card}(E) + \delta - \chi)$$

En majorant $\mathrm{Card}(f^{-1}(D))$ par $\delta \deg(f)$, on obtient l'inégalité du lemme. De plus, dès que D est non vide, l'inégalité $\mathrm{Card}(f^{-1}(D)) \leq \delta \deg(f)$ est stricte, puisque f est ramifiée au-dessus de chaque point de D. Donc les cas d'égalité dans le lemme sont exactement les cas où D est vide, c'est-à-dire les cas où f est ramifiée seulement au-dessus de E.

4.4 Démonstration du théorème 9

Rappelons l'énoncé du théorème dont la démonstration fait l'objet de cette section :

Théorème 9 *Pour tout $P \in \mathbb{Z}[X]$ séparable, dont le contenu est sans facteur carré, il existe $(R, S) \in M$, avec R et S à coefficients entiers, tels que P divise $\tilde{u}(RS)$ dans $\mathbb{Z}[X]$. Si on note $r = \frac{R}{S}$, cela signifie que r est définie sur $\mathbb{Q}$, appartient à M, et que les racines de P appartiennent à l'ensemble $r^{-1}(\{0, \infty\})$ des zéros et pôles de r.*

N.B. Pour que cet énoncé soit correct, il ne faut pas exiger des polynômes R et S tels que $(R, S) \in M$ qu'ils soient unitaires, mais seulement qu'ils aient même coefficient dominant.

Démontrons d'abord l'équivalence des deux formulations.

L'une des implications est évidente : si P divise $\tilde{u}(RS)$ alors les racines de P sont des zéros ou des pôles de r. Réciproquement, supposons que les racines de P soient des zéros ou des pôles de r. Comme r est définie sur $\mathbb{Q}$, on peut choisir les polynômes R et S dans $\mathbb{Z}[X]$. Or les racines de $P \in \mathbb{Z}[X]$ sont simples, et sont des racines de RS. Donc il existe un entier α tel que P divise $\alpha\tilde{u}(RS)$ dans $\mathbb{Z}[X]$. Comme le contenu de P est sans facteur carré, on peut choisir α sans facteur

carré, et premier au contenu de RS. En posant $R_1 = \alpha R$ et $S_1 = \alpha S$, on a $\alpha\tilde{u}(RS) = \tilde{u}(R_1 S_1)$ et $(R_1, S_1) \in M$. Cela termine la démonstration de l'équivalence des deux formulations du théorème 9.

Pour démontrer ce théorème, on va utiliser les résultats du paragraphe 4.2, ainsi que les deux lemmes ci-dessous :

Lemme 9 *Pour tout $P \in \mathbb{Z}[X]$ scindé sur $\mathbb{Q}$ il existe une fraction rationnelle $r \in M$ qui envoie les racines de P dans $\{0, \infty\}$.*

Lemme 10 *Pour tout $P \in \mathbb{Z}[X]$ il existe un polynôme $T \in \mathbb{Q}[X]$ non constant, ramifié seulement au-dessus de $\mathbb{Q}$ et de l'infini, qui envoie les racines de P dans $\mathbb{Q}$.*

N.B. Dire que le polynôme T est ramifié seulement au-dessus de $\mathbb{Q}$ et de l'infini signifie simplement que les images par T des zéros de T' sont dans $\mathbb{Q}$.

DÉMONSTRATION du lemme 9 : Notons x_i les racines de P, qui sont rationnelles. Le théorème 8 montre comment choisir les exposants $n_i \in \mathbb{Z} - \{0\}$ pour que la fraction rationnelle $r = \prod_i (X - x_i)^{n_i}$ soit dans M. Cela termine la démonstration du lemme 9.

DÉMONSTRATION du lemme 10, tirée de [15] : Soit P le polynôme à coefficients entiers donné; on peut le supposer séparable. On va procéder en plusieurs étapes :

- Si P est à racines rationnelles, tout polynôme $T \in \mathbb{Q}[X]$ non constant dont la dérivée est scindée sur $\mathbb{Q}$ (ou constante) convient. On peut prendre par exemple $T(X) = X$.
- Sinon, on va construire par récurrence une suite finie de polynômes P_j (pour $j \geq 1$), avec $P_1 = P$. Si Q désigne un polynôme à coefficients entiers, on écrit $Q = i(Q)q(Q)$ où $q(Q)$ est scindé sur $\mathbb{Q}$, $i(Q)$ n'a pas de racine rationnelle, et $i(Q)$ et $q(Q)$ sont à coefficients entiers. Si on veut vraiment que ces notations $i(Q)$ et $q(Q)$ soient univoques, on peut par exemple supposer $q(Q)$ de contenu 1 et de coefficient dominant strictement positif; mais ces précisions ne seront pas utiles ici. Démontrons par récurrence qu'on peut construire des polynômes $P_1, \ldots, P_k$ tels que :

  1. $P_1 = P$.
  2. P_k est scindé sur $\mathbb{Q}$, et pour tout $j < k$ P_j n'est pas scindé sur $\mathbb{Q}$.
  3. Pour tout $1 \leq j \leq k$, P_j est séparable, à coefficients entiers.
  4. Pour tout $1 \leq j \leq k-1$, P_j et $i(P_j)'$ divisent $P_{j+1} \circ i(P_j)$.
  5. Pour tout $1 \leq j \leq k-1$, $d(i(P_{j+1})) \leq d(i(P_j)) - 1$.

  En effet, on pose bien sûr $P_1 = P$. Si $P_1, \ldots, P_j$ sont construits, posons
  $$P_{j+1} = a_{j+1}\tilde{u}(\textstyle\prod_\xi (X - i(P_j)(\xi)))$$
  où ξ décrit l'ensemble des racines de P_j ou de $i(P_j)'$, et où a_{j+1} est un entier tel que P_{j+1} soit à coefficients entiers (ce qui est possible car ses racines forment une partie de $\bar{\mathbb{Q}}$ stable par $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$). Alors l'hypothèse 4 est vérifiée (d'après le lemme 5). De plus, les racines de P_{j+1} sont les images par $i(P_j)$ des racines de P_j ou de $i(P_j)'$. Or les racines de P_j sont soit rationnelles (alors leurs images par $i(P_j) \in \mathbb{Z}[X]$ aussi), soit racines de $i(P_j)$ (alors leur image par $i(P_j)$ est nulle). Donc les racines irrationnelles de P_{j+1} sont certains des $i(P_j)(\xi)$ pour ξ racine de $i(P_j)'$: il y en a au plus $d(i(P_j)) - 1$, d'où 5, ce qui conclut la récurrence.
- Construisons à partir de cette suite de polynômes le polynôme T cherché. On peut supposer $k \geq 2$, car le lemme est démontré pour les polynômes scindés sur $\mathbb{Q}$. Posons $T = i(P_{k-1}) \circ \ldots \circ i(P_1)$[4]. Montrons que :

4. Ici il y a une faute de frappe dans [15].

1. $P = P_1$ divise $P_k \circ T$.
2. T' divise $P_k \circ T$.

En effet, P_1 divise $P_2 \circ i(P_1)$ qui divise $P_3 \circ i(P_2) \circ i(P_1)$ qui divise ... qui divise $P_k \circ T$, d'où 1. De plus, on a $T' = \prod_{j=1}^{k-1} i(P_j)' \circ i(P_{j-1}) \circ \ldots \circ i(P_1)$. Or pour $1 \leq j \leq k-1$ le polynôme $i(P_j)'$ divise $P_{j+1} \circ i(P_j)$ qui divise ... qui divise $P_k \circ i(P_{k-1}) \circ \ldots \circ i(P_{j+1}) \circ i(P_j)$. Donc $i(P_j)' \circ i(P_{j-1}) \circ \ldots \circ i(P_1)$ divise $P_k \circ T$. Ainsi : T' divise $(P_k \circ T)^k$ (où la puissance est au sens du produit usuel des polynômes). Or pour w zéro de T' d'ordre n, w est zéro d'ordre au moins $n+1$ de $P_k \circ T - P_k(T(w))$, qui est $P_k \circ T$ (car w est zéro de T' et que T' divise une puissance de $P_k \circ T$). Donc T' divise $P_k \circ T$, d'où 2.

– La démonstration du lemme est maintenant terminée. En effet, P et T' divisent $P_k \circ T$, donc T envoie les racines de P et celles de T' sur des racines de P_k, qui sont des rationnels car P_k est scindé sur $\mathbb{Q}$. De plus, comme on a supposé $k \geq 2$, T est le composé d'un nombre non nul de polynômes $i(P_j)$, avec $1 \leq j \leq k-1$. Comme chacun de ces polynômes est non constant (sinon, pour l'indice j en question, P_j serait scindé sur $\mathbb{Q}$ ce qui n'est pas le cas), leur composé T est non constant. Cela conclut la démonstration du lemme 10.

On peut maintenant démontrer le théorème 9. Cette démonstration est simplement la synthèse des résultats précédents :

DÉMONSTRATION du théorème 9 : Soit $P \in \mathbb{Z}[X]$ séparable. Le lemme 10 fournit un polynôme $T \in \mathbb{Q}[X]$ non constant qui envoie les racines de P et celles de T' dans $\mathbb{Q}$. Notons F un polynôme à coefficients entiers dont les racines, simples, sont exactement les images par T des zéros de $T'P$. Le lemme 9, appliqué à F, donne une fraction rationnelle $r \in M$ qui envoie les racines de F dans $\{0, \infty\}$. Cela signifie que $r \circ T$ envoie les racines de P et celles de T' dans $\{0, \infty\}$. De plus, d'après la proposition 10 et le lemme 6, on a $r \circ T \in M$, avec $r \circ T$ définie sur $\mathbb{Q}$. Cela termine la démonstration du théorème 9.

4.5 Liens avec le théorème de Belyi

On rappelle qu'une fonction de Belyi de $\mathbb{P}^1(\mathbb{C})$ dans $\mathbb{P}^1(\mathbb{C})$ est une fraction rationnelle non constante ramifiée seulement au-dessus de $\{0, 1, \infty\}$. En particulier, tout élément de M est une fonction de Belyi.

Le théorème de Belyi affirme que pour toute courbe algébrique projective lisse X définie sur $\bar{\mathbb{Q}}$ il existe une fonction de Belyi de X dans $\mathbb{P}^1$. Une partie essentielle de sa démonstration est le résultat suivant, qu'on appellera ici théorème de Belyi, et que Serre appelle "Théorème B" dans [25] :

Théorème 10 *Pour tout $P \in \mathbb{Z}[X]$ il existe une fonction de Belyi r définie sur $\mathbb{Q}$ qui envoie les racines de P dans $\{0, 1, \infty\}$.*

En fait, dans [25], Serre donne la formulation équivalente suivante [5] :

Théorème 11 *Pour toute partie finie S de $\mathbb{P}^1(\bar{\mathbb{Q}})$, il existe une fonction de Belyi r définie sur $\mathbb{Q}$ qui envoie S dans $\{0, 1, \infty\}$.*

Le fait que le théorème 11 implique le théorème 10 est clair : il suffit de prendre pour S l'ensemble des racines de P. Réciproquement, soit S une partie finie de $\mathbb{P}^1(\bar{\mathbb{Q}})$. Il existe un automorphisme ϕ de $\mathbb{P}^1$, défini sur $\mathbb{Q}$, qui envoie S sur une partie finie T de $\bar{\mathbb{Q}}$ (il suffit en effet de poser $\phi(X) = \frac{1}{X - x_0}$ où x_0 est un rationnel qui n'appartient pas à S). Notons $P \in \mathbb{Z}[X]$ le

5. Serre affirme seulement, dans son énoncé, que la fonction r est définie sur $\bar{\mathbb{Q}}$, ce qui lui suffit pour démontrer le théorème de Belyi; mais sa démonstration donne une fonction r définie sur $\mathbb{Q}$.

polynôme minimal sur $\mathbb{Q}$ de l'ensemble T (normalisé de telle sorte qu'il soit à coefficients entiers). Le théorème 10 fournit une fonction de Belyi r. Il est clair que $r \circ \phi$ est aussi une fonction de Belyi, et qu'elle envoie S dans $\{0, 1, \infty\}$. Cela conclut la démonstration de l'équivalence des théorèmes 10 et 11.

Dans l'énoncé du théorème 10, on peut bien sûr supposer P séparable, et de contenu sans facteur carré. C'est pourquoi le théorème 9 implique le théorème 10 de Belyi. En fait, le théorème 9 est strictement plus précis que le théorème de Belyi, car il existe des fonctions de Belyi qui n'appartiennent pas à M [6], et car le théorème 9 fournit une fonction r qui envoie les racines de P dans $\{0, \infty\}$, et pas seulement dans $\{0, 1, \infty\}$.

La démonstration du théorème de Belyi (qui se trouve dans [1] et dans [25]) se décompose en deux lemmes :

Lemme 11 *Pour tout $P \in \mathbb{Z}[X]$ scindé sur $\mathbb{Q}$ il existe une fonction de Belyi r qui envoie les racines de P dans $\{0, 1, \infty\}$.*

Lemme 12 *Pour tout $P \in \mathbb{Z}[X]$ il existe un polynôme $T \in \mathbb{Q}[X]$ non constant, ramifié seulement au-dessus de $\mathbb{Q}$ et de l'infini, qui envoie les racines de P dans $\mathbb{Q}$.*

Pour démontrer le théorème de Belyi à partir de ces deux lemmes, on applique d'abord à P le lemme 12, ce qui fournit un polynôme T. Puis on applique le lemme 11 au polynôme à coefficients entiers dont les racines sont les images par T des racines de P, auxquelles on adjoint les rationnels au-dessus desquels T est ramifié. Cela donne une fraction rationnelle r; il est alors clair que la fonction $r \circ T$ convient. Cela termine la démonstration du théorème de Belyi à partir des deux lemmes.

On peut dresser un parallèle entre, d'un côté le théorème de Belyi et les deux lemmes ci-dessus, d'un autre côté le théorème 9 et les lemmes 9 et 10. En effet, d'une part, le lemme 9 est strictement plus précis que le lemme 11. D'autre part, le lemme 12 est rigoureusement identique au lemme 10, et les démonstrations des théorèmes 9 et 10 à partir de leurs lemmes respectifs sont tout à fait analogues.

Le fait que le théorème 9 soit une version strictement plus précise du théorème 10 provient donc du fait que le lemme 9 est plus précis que le lemme 11.

Le lemme 12 est démontré dans [25] (il s'agit du passage du cas particulier que Serre envisage en premier lieu au cas général), et dans [1] (où aucun des deux lemmes n'est dégagé explicitement). Ces démonstrations fournissent de nouvelles preuves du lemme 10 (qui est identique au lemme 12) :

DÉMONSTRATION du lemme 10 d'après [25] : Elle est tout à fait similaire à la démonstration donnée plus haut de ce même lemme. Il convient seulement de changer les notations utilisées précédemment.

On suppose toujours P séparable. Mais désormais, si Q désigne un polynôme à coefficients entiers, on pose $Q = i(Q)q(Q)$ où $i(Q) \in \mathbb{Z}[X]$ est un facteur irréductible (dans $\mathbb{Z}[X]$) de Q de degré maximal, et où $q(Q)$ est à coefficients entiers. La formule donnant P_{j+1} en fonction de P_j reste inchangée (même si sa signification n'est plus la même). Dans la récurrence, les propriétés 1, 2, 3 et 4 restent valables. Seule la propriété 5 doit être modifiée. Notons $P_j = \prod_i P_j^{(i)}$ la décomposition de P_j en facteurs irréductibles dans $\mathbb{Z}[X]$ (ces facteurs sont deux à deux distincts d'après la propriété 3). Posons $d_j = \max_i d(P_j^{(i)})$ (c'est le degré de $i(P_j)$), et notons n_j le nombre de facteurs irréductibles $P_j^{(i)}$ de degré d_j. Alors la propriété 5 doit être remplacée par :

$$5BIS : \text{Pour tout } 1 \leq j \leq k-1, \text{ soit } d_{j+1} < d_j, \text{ soit } (\ d_{j+1} = d_j \text{ et } n_{j+1} < n_j\ )$$

6. Par exemple $r(\frac{1}{X})$ pour $r \in M$ telle que $r(0) = 1$.

En effet, les racines complexes de P_{j+1} sont les $i(P_j)(\xi)$ pour ξ racine de P_j ou de $i(P_j)'$. On a plusieurs cas :

- Si ξ est racine de $i(P_j)'$, son degré sur $\mathbb{Q}$ est inférieur ou égal à $d(i(P_j)') = d_j - 1$, donc celui de son image par $i(P_j)$ aussi. Donc le facteur irréductible $P_{j+1}^{(i)}$ dont $i(P_j)(\xi)$ est racine est de degré au plus $d_j - 1$.

- Si ξ est racine de $i(P_j)$, on a $i(P_j)(\xi) = 0$ donc le facteur irréductible $P_{j+1}^{(i)}$ dont $i(P_j)(\xi)$ est racine est le monôme X. Il est de degré $1 \leq d_j - 1$ (car si d_j était égal à 1, P_j serait scindé sur $\mathbb{Q}$ ce qui n'est pas le cas).

- Si ξ est racine d'un $P_j^{(i)}$ de degré strictement inférieur à d_j, alors $i(P_j)(\xi)$ est aussi de degré strictement inférieur à d_j sur $\mathbb{Q}$. Donc le facteur irréductible $P_{j+1}^{(i')}$ dont $i(P_j)(\xi)$ est racine est de degré au plus $d_j - 1$.

- Il ne reste donc que les racines ξ des $n_j - 1$ polynômes $P_j^{(i)}$ de degré d_j différents de $i(P_j)$. Pour chaque i parmi ces $n_j - 1$ valeurs, les racines ξ des $P_j^{(i)}$ sont conjuguées par $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, donc leurs images $i(P_j)(\xi)$ aussi : ces images ont toutes le même polynôme minimal sur $\mathbb{Q}$, qui est un facteur irréductible de P_{j+1} de degré au plus d_j. Les facteurs irréductibles de P_{j+1} ainsi obtenus sont au maximum au nombre de $n_j - 1$. D'après l'étude des trois cas précédents, tous les facteurs irréductibles de P_{j+1} de degré supérieur ou égal à d_j sont obtenus ainsi. Donc le nombre de facteurs de degré d_j est inférieur ou égal à $n_j - 1$, et il n'y a aucun facteur de degré strictement supérieur à d_j. Cela termine la démonstration de la propriété $5BIS$.

La fin de la démonstration est exactement la même que dans la première démonstration du lemme 10 : on définit le polynôme T par la même formule, et les mêmes vérifications montrent que T convient. La seule différence (due au fait que les notations ont changé) est que la propriété 5 a été remplacée par la propriété $5BIS$, ce qui ne change rien à la suite de la démonstration : c'est juste un argument différent pour montrer que la récurrence se termine au bout d'un nombre fini d'étapes.

La deuxième démonstration du lemme 10 est donc terminée.

DÉMONSTRATION du lemme 10, d'après [1] : On peut bien sûr supposer P non constant. Notons T_1 le polynôme minimal (sur $\mathbb{Q}$) de l'ensemble des racines de P (c'est le radical $u(P)$ de P). Si pour $i \geq 1$ on a défini le polynôme non constant $T_i \in \mathbb{Q}[X]$, alors on note T_{i+1} le polynôme minimal (sur $\mathbb{Q}$) de l'ensemble des valeurs prises par T_i aux zéros de sa dérivée T_i'. Or l'ensemble des zéros de $T_i' \in \mathbb{Q}[X]$ est stable par $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, et est de cardinal au plus $d(T_i) - 1$; donc il en est de même pour l'image par T_i de cet ensemble. C'est pourquoi T_{i+1} est de degré au plus $d(T_i) - 1$. On définit donc ainsi une suite finie $T_1, \ldots, T_k$ de polynômes à coefficients rationnels, en s'arrêtant à l'indice k tel que T_k soit de degré 1. On pose alors : $T = T_k \circ T_{k-1} \circ \ldots \circ T_1$. On vérifie aisément que ce polynôme convient. Cela conclut la troisième démonstration du lemme 10.

5 Minoration du radical dans des expressions polynômiales

Dans cette section, on cherche des conséquences de la conjecture *abc* en termes de minoration d'expressions de la forme $P(n)$ (paragraphe 5.1) ou $P(a, b)$ (paragraphe 5.2), où P désigne respectivement un polynôme à une variable et un polynôme homogène à deux variables, toujours supposé non constant.

5.1 Polynôme à une variable

On va déduire du théorème 9 le résultat suivant :

Théorème 12 (modulo *abc*) *Pour tout polynôme $P \in \mathbb{Z}[X]$ séparable et pour tout $\varepsilon > 0$ il existe une constante $c_\varepsilon > 0$ telle que pour tout entier n assez grand :*

$$|\mathrm{rad}(P(n))| > c_\varepsilon n^{d(P)-1-\varepsilon}$$

N.B. Si on ne suppose plus P séparable, le théorème est encore valable en remplaçant le $d(P)$ qui apparaît en exposant par le nombre $\varrho(P)$ de racines de P, comptées sans multiplicités.

DÉMONSTRATION : Comme on s'intéresse au radical des valeurs prises par P sur les entiers, on peut supposer que le contenu de P est sans facteur carré. D'après le théorème 9, il existe alors un couple (R, S) de polynômes à coefficients entiers qui appartient à M, et un polynôme $Q \in \mathbb{Z}[X]$, tels que $\tilde{u}(RS) = PQ$. Comme $(R, S) \in M$, on a :

$$d(R) = d(S) \text{ et } d(R) - d(R-S) + 1 = \varrho(RS) = d(PQ) = d(P) + d(Q)$$

D'autre part, l'idée essentielle dans le calcul suivant est d'appliquer, pour n grand, la conjecture *abc* à l'identité :

$$(R - S)(n) + S(n) = R(n) \tag{11}$$

Cette conjecture donne, pour tout $\varepsilon > 0$: $|\mathrm{rad}((RS(R-S))(n))| \gg_\varepsilon n^{d(R)-\varepsilon}$. En réalité, pour avoir le droit d'appliquer la conjecture *abc*, il faudrait que $R(n)$ et $S(n)$ soient premiers entre eux. Or cela n'a aucune raison d'être le cas; en fait, comme R et S sont premiers entre eux, il existe des polynômes A et B à coefficients entiers, et un entier naturel non nul d, tels que $AR+BS = d$. Alors pour tout entier n, le pgcd de $R(n)$ et de $S(n)$ est inférieur ou égal à d; on peut diviser la relation (11) par ce pgcd avant d'appliquer la conjecture *abc*, et le terme correctif qui apparaît passe dans la constante sous-jacente au symbole $\gg$. Il faut d'ailleurs noter que dans tout le raisonnement, la constante impliquée dans ce symbole dépend de ε, mais aussi de P (à travers R et S). On peut alors regrouper les formules précédentes dans le calcul suivant :

$$\begin{aligned}
|\mathrm{rad}(P(n))| &\gg n^{-d(Q)}|\mathrm{rad}((RS)(n))| &(12)\\
&\gg n^{-d(Q)}n^{-d(R-S)}|\mathrm{rad}((RS(R-S))(n))| &(13)\\
&\gg_\varepsilon n^{-d(Q)}n^{-d(R-S)}n^{d(R)-\varepsilon} &(14)\\
&\gg_\varepsilon n^{d(P)-1-\varepsilon} &(15)
\end{aligned}$$

Ce calcul termine la démonstration du théorème.

N.B. Cette démonstration utilise le théorème 9. On peut, à la place de ce théorème, utiliser le théorème 11 (qui est équivalent au théorème 10 de Belyi). En effet, le théorème 11 fournit une fraction rationnelle r, définie sur $\mathbb{Q}$, ramifiée seulement au-dessus de $\{0, 1, \infty\}$, qui envoie l'infini et les racines de P dans $\{0, 1, \infty\}$. Si on écrit $r = \frac{R}{S}$ et qu'on suppose le contenu de P sans facteur carré, on peut choisir R et S à coefficients entiers tels que P divise $\tilde{u}(RS(R-S))$ dans $\mathbb{Z}[X]$. De plus, d'après la proposition 1, on a $\varrho(RS(R-S)) = \max(d(R), d(S)) + 1$. Le polynôme $Q \in \mathbb{Z}[X]$ tel que $PQ = \tilde{u}(RS(R-S))$ est donc de degré $\max(d(R), d(S)) + 1 - d(P)$. Le calcul suivant se justifie comme dans la démonstration ci-dessus du théorème 12 :

$$\begin{aligned}
|\mathrm{rad}(P(n))| &\gg n^{-d(Q)}|\mathrm{rad}((RS(R-S))(n))|\\
&\gg_\varepsilon n^{-d(Q)}n^{\max(d(R),d(S))-\varepsilon}\\
&\gg_\varepsilon n^{d(P)-1-\varepsilon}
\end{aligned}$$

Cela conclut la démonstration du théorème 12 à partir du théorème 11.

N.B. La clef de ces deux démonstrations du théorème 12 est d'appliquer la conjecture *abc* à la relation (11). Selon qu'on part du théorème 9 ou du théorème 11, la fonction $r = \frac{R}{S}$ est un élément de M ou une fonction de Belyi. De toute façon, toute la ramification de r est concentrée au-dessus de $\{0, 1, \infty\}$, donc le cardinal de $r^{-1}(\{0, 1, \infty\})$ est le plus petit possible (à $\deg(r)$ fixé). Les points 0, 1 et ∞ ont "peu" d'antécédents par r, donc (voir le paragraphe 5.3, en particulier la proposition 12) $\mathrm{rad}(R(n))$, $\mathrm{rad}((R-S)(n))$ et $\mathrm{rad}(S(n))$ ont tendance à être petits (en valeur absolue). C'est pourquoi il est particulièrement intéressant d'appliquer la conjecture *abc* à la relation (11), puique cette conjecture affirme que le produit de ces trois radicaux ne peut pas être "trop petit".

5.2 Polynôme à deux variables

Théorème 13 (modulo *abc*) *Soit $F(X,Y)$ un polynôme homogène de degré d à deux variables, à coefficients entiers, sans facteur multiple, et tel que $F(X,0) \neq 0$. Alors pour tout $\varepsilon > 0$ il existe une constante $c_\varepsilon > 0$ telle que pour tout couple (a,b) d'entiers premiers entre eux, tels que $a > b > 0$ et $F(a,b) \neq 0$, on ait :*

$$|\mathrm{rad}(F(a,b))| > c_\varepsilon \frac{a^{d-1-\varepsilon}}{\mathrm{rad}(b)}$$

N.B. On peut supprimer l'hypothèse $a > b > 0$ en appliquant cette proposition successivement aux polynômes $F(X,-Y)$, $F(-X,Y)$, $F(Y,X)$, ...

La démonstration de ce théorème, qui figure dans [15], est analogue à la démonstration du théorème 12.

DÉMONSTRATION : On peut supposer que le pgcd des coefficients de $F(X,Y)$ est sans facteur carré. Alors, d'après le théorème 9 appliqué au polynôme $F(X,1)$, il existe un polynôme $G(X)$ à coefficients entiers et un élément (R,S) de M, avec R et S à coefficients entiers, tels que $\tilde{u}(RS) = F(X,1)G(X)$. Notons R_1, S_1, G_1 et Δ_1 les polynômes homogènes associés à R, S, G et $R-S$ respectivement. On a la relation, pour a et b entiers :

$$R_1(a,b) - S_1(a,b) = b^{d(R)-d(R-S)}\Delta_1(a,b) \tag{16}$$

Comme R et S sont premiers entre eux, il existe des polynômes A et B à coefficients entiers, et un entier naturel non nul d, tel que $AR + BS = d$. En homogénéisant cette relation, il vient (en notant A_1 et B_1 les polynômes homogènes associés à A et B) :

$$A_1(X,Y)R_1(X,Y) + B_1(X,Y)S_1(X,Y) = dY^{d(A)+d(R)} \tag{17}$$

Comme $F(X,0)$ n'est pas identiquement nul, $R_1(X,0)S_1(X,0)$ non plus, donc quitte à échanger R et S (qui jouent des rôles symétriques) on peut supposer qu'on a :

$$R_1(X,Y) = u_1X^{d(R)} + u_2X^{d(R)-1}Y + \ldots + u_{d(R)+1}Y^{d(R)} \text{ avec } u_1 \neq 0 \tag{18}$$

Montrons qu'on a :

$$pgcd(R(a,b), S(a,b)) \leq du_1^{d(A)+d(R)} \tag{19}$$

En effet, soit p un nombre premier qui divise $R(a,b)$ et $S(a,b)$. Notons n la valuation p-adique de $pgcd(R(a,b)S(a,b))$; montrons que p^n divise $du_1^{d(A)+d(R)}$. Pour cela, posons $k = v_p(b) \geq 0$, de telle sorte que la relation (17), appliquée avec $(X,Y) = (a,b)$, implique $v_p(d) + k(d(A)+d(R)) \geq n$. Si k est nul, on a terminé. Sinon, p divise b donc p est premier avec a. La relation (18) appliquée avec $(X,Y) = (a,b)$ montre que $p^{k'}$ divise u_1, en notant $k' = Min(k,n)$. Si $k' = n$ alors p^n divise u_1, donc p^n divise $du_1^{d(A)+d(R)}$ et on a terminé. Sinon, on a $k' = k$. Dans ce cas, p^n divise $p^{v_p(d)}p^{k(d(A)+d(R)}$ qui divise $du_1^{d(A)+d(R)}$, ce qu'il fallait démontrer.

La relation (19) est donc démontrée. Elle signifie qu'on peut appliquer la conjecture *abc* à l'égalité (16), puisque les termes qui jouent les rôles de a, b et c sont premiers entre eux, à un facteur près qui est borné en fonction de F seulement. On a donc pour tout $\varepsilon > 0$:

$$\max(|R_1(a,b)|, |S_1(a,b)|)^{1-\varepsilon} \quad \ll_{F,\varepsilon} \quad |\mathrm{rad}(R_1(a,b)\, S_1(a,b)\, b^{d(R)-d(R-S)}\, \Delta_1(a,b))| \tag{20}$$

Or le membre de gauche s'écrit $a^{(1-\varepsilon)d(R)} \max(|R_1(1,\frac{b}{a})|, |S_1(1,\frac{b}{a})|)$. De plus, les relations (17) et (18) montrent que $R_1(1,Y)$ et $S_1(1,Y)$ sont premiers entre eux, donc il existe une constante $\kappa > 0$ telle que pour tout $y \in \mathbb{Q}$ (et même pour tout $y \in \mathbb{C}$) on ait $\max(|R_1(1,y)|, |S_1(1,y)|) \geq \kappa$. Le membre de gauche de la formule (20) est donc minoré par $(\kappa a^{d(R)})^{1-\varepsilon}$. Quant au membre de droite, on peut le majorer en utilisant le fait que $\mathrm{rad}(R_1S_1(a,b)) = \mathrm{rad}(G_1F(a,b))$, avec G_1

homogène de degré $\varrho(RS) - d$ (où d désigne le degré de F) et $a > b > 0$. On obtient donc, pour tout $\varepsilon > 0$:

$$\begin{aligned} a^{d(R)-\varepsilon} &\ll_{F,\varepsilon} |\mathrm{rad}(F(a,b))|\, a^{\varrho(RS)-d}\, \mathrm{rad}(b)\, a^{d(R-S)} \\ &\ll_{F,\varepsilon} a^{d(R)+1-d}\, \mathrm{rad}(b)\, |\mathrm{rad}(F(a,b))| \end{aligned}$$

Cela conclut la démonstration du théorème.

N.B. La démonstration précédente permet d'exprimer explicitement la constante c_ε en fonction de F et de la constante qui apparaît dans la conjecture *abc*.

N.B. Ici, on a démontré que la conjecture *abc* implique le théorème 13. En fait, il y a équivalence puisqu'on retrouve la conjecture *abc* en appliquant le théorème 13 au polynôme $F(X,Y) = XY(X+Y)$.

De ce théorème on peut déduire le corollaire suivant :

Corollaire 2 (modulo *abc*) *Soient $P \in \mathbb{Z}[X]$ séparable de degré d et $\varepsilon > 0$. Alors il existe une constante $c_\varepsilon > 0$ telle que pour tout couple (a,b) d'entiers premiers entre eux tels que $a > b > 0$ et $P(\frac{a}{b}) \neq 0$ on a :*

$$|\mathrm{rad}(P(\frac{a}{b}))| > c_\varepsilon \frac{a^{d-1-\varepsilon}}{\mathrm{rad}(b)} \gg a^{d-2-\varepsilon}$$

N.B. La conclusion de ce corollaire peut aussi se formuler de la manière suivante : pour tout $x \in \mathbb{Q}$ qui n'est pas zéro de P, on a $|\mathrm{rad}(P(x))| > c_\varepsilon H(x)^{d-2-\varepsilon}$. C'est sous cette forme (légèrement plus faible) que cet énoncé apparaît dans [6]; il y est formulé dans le cadre plus général d'un corps de nombres K, avec $P \in K[X]$ et $x \in K$; la constante c_ε dépend alors aussi de K.

DÉMONSTRATION du corollaire : Notons P_1 le polynôme homogène associé à P. Alors P_1 est sans facteur multiple, donc on peut lui appliquer le théorème 13, ce qui permet d'écrire :

$$\begin{aligned} |\mathrm{rad}(P(\frac{a}{b}))| &= |\mathrm{rad}(b^{-d} P_1(a,b))| \\ &= |\mathrm{rad}(b^{d-1} b P_1(a,b))| \\ &\geq \frac{|\mathrm{rad}(bP_1(a,b))|}{\mathrm{rad}(b^{d-1})} \\ &> c_\varepsilon \frac{a^{d-1-\varepsilon}}{\mathrm{rad}(b)} \end{aligned}$$

Cela conclut la démonstration du corollaire.

N.B. Dans [6], Elkies mentionne ce corollaire comme une application des méthodes qu'il emploie (voir le paragraphe 5.3). Il n'en donne pas la démonstration, mais on peut imaginer qu'Elkies obtient ce résultat, comme ici, à partir du théorème 13. Or Elkies ne mentionne dans son article que les fonctions de Belyi, et pas l'ensemble M ni le théorème 9. Cela conduit à chercher une démonstration du théorème 13 à l'aide seulement de fonctions de Belyi, ou de leur analogue polynômial que sont les cas d'égalité dans le théorème 2 (d'après la proposition 1).

DÉMONSTRATION du théorème 13 à partir des fonctions de Belyi : Appliquons le théorème 11 (qui est équivalent au théorème de Belyi appliqué à $\mathbb{P}^1$, voir le paragraphe 4.5) à l'ensemble S formé par l'infini et les racines du polynôme $F(X,1)$. On obtient une fonction de Belyi $r = \frac{R}{S}$ qui envoie l'infini et les zéros de $F(X,1)$ dans $\{0,1,\infty\}$. Quitte à permuter $\{0,1,\infty\}$ à l'arrivée, ce qui revient à changer r en $\frac{1}{r}$ ou en $\frac{1}{1-r}$, on peut supposer $r(\infty) = \infty$. On a alors $d(R) > d(S)$ et, d'après la proposition 1, $\varrho(RS(R-S)) = d(R)+1$. Quitte à supposer que le pgcd des coefficients de $F(X,Y)$ est sans facteur carré, le fait que r envoie les zéros de $F(X,1)$ dans

$\{0,1,\infty\}$ se traduit par l'existence de $G(X) \in \mathbb{Z}[X]$ tel que $\tilde{u}(RS(R-S)) = F(X,1)G(X)$. Comme $d(R) = d(R-S) > d(S)$, on a (en gardant les notations de la première démonstration du théorème 13) :

$$R_1(X,Y) - Y^{d(R)-d(S)} S_1(X,Y) = \Delta_1(X,Y) \tag{21}$$

On montre de même que le pgcd des trois termes qui interviennent est borné. On applique de même la conjecture *abc*; la seule différence est que dans le calcul qui suit, on fait apparaître le radical de $R_1 S_1 \Delta_1$ qui vaut $G_1 F$. Le calcul se termine sans problèmes.

N.B. En fait, on peut aussi formuler cette démonstration sans utiliser la proposition 1, en utilisant la définition du radical d'un nombre rationnel non nul.

5.3 Liens entre radical et nombre de racines

La proposition suivante constitue le point central de [6] :

Proposition 11 *Soit C une courbe définie sur $\mathbb{Q}$, r une fonction rationnelle de C dans $\mathbb{P}^1$ de degré d définie sur $\mathbb{Q}$. Posons $k = \mathrm{Card}(\{x \in C \mid r(x) = 0\})$. Alors pour tout point $P \in C(\mathbb{Q})$ qui n'est ni zéro ni pôle de r on a :*

$$\log(\mathrm{rad}(r(P))) < \frac{k}{d} \log(H(r(P))) + O(1 + \sqrt{\log(H(r(P)))})$$

N.B. Dans ce lemme, la constante sous-jacente au symbole O dépend de C, de r, mais pas de P.

L'énoncé de cette proposition utilise les notions de hauteur et de radical d'un nombre rationnel :

DÉFINITION : Soit $x = \frac{p}{q}$ un rationnel non nul écrit comme quotient de deux entiers relatifs premiers entre eux. On appelle *hauteur* de x l'entier

$$H(x) = \max(|p|, |q|)$$

En supposant de plus $q > 0$, on définit le radical de x par la formule :

$$\mathrm{rad}(x) = \mathrm{rad}(p)$$

La proposition 11 est une majoration du radical de $r(P)$ en fonction de la hauteur de $r(P)$, avec un facteur $\frac{k}{d}$ qui dépend du nombre de zéros de r, comptés sans multiplicité. Cette proposition établit donc un lien entre le fait que les zéros de r aient des multiplicités élevées et le fait que des exposants élevés apparaissent dans la décomposition en facteurs premiers du numérateur de $r(P)$.

Elkies énonce et démontre cette proposition dans le cas plus général où $\mathbb{Q}$ est remplacé par un corps de nombres quelconque. Les notions de radical et de hauteur se généralisent par l'utilisation des places du corps de nombres.

La démonstration de cette proposition n'est pas élémentaire dans le cas général; elle utilise la théorie des hauteurs relatives à des diviseurs de degré zéro, exposée par exemple dans [25].

Dans [6], Elkies applique cette proposition successivement à r, $r-1$ et $\frac{1}{r}$. C'est le fait de faire la synthèse des trois minorations obtenues qui va relier la proposition précédente à la conjecture *abc*. On a besoin de la notation suivante :

NOTATION : Pour $x \in \mathbb{Q} - \{0,1\}$ on pose :

$$N(x) = \mathrm{rad}(x)\ \mathrm{rad}(x-1)\ \mathrm{rad}(\tfrac{1}{x})$$

Cette notation permet de traduire la conjecture *abc*. En effet, on établit une bijection entre les triplets (a,b,c) d'entiers relatifs non nuls premiers entre eux tels que $a+b=c$ (avec $a>0$) et

les nombres rationnels x différents de 0 et de 1 en posant $x = \frac{-a}{b}$. On a alors $\mathrm{rad}(a) = -\mathrm{rad}(x)$, $\mathrm{rad}(b) = \mathrm{rad}(\frac{1}{x})$, $\mathrm{rad}(c) = -\mathrm{rad}(x-1)$ donc

$$\mathrm{rad}(abc) = N(x)$$

On a donc la formulation suivante de la conjecture *abc*:

Conjecture 2 (*abc*, formulation équivalente) *Pour tout $\varepsilon > 0$ il existe $c_\varepsilon > 0$ tel que pour tout $x \in \mathbb{Q} - \{0,1\}$ on ait*

$$N(x) > c_\varepsilon H(x)^{1-\varepsilon}$$

Appliquons (comme le fait Elkies dans [6]) la proposition 11 successivement à r, $r-1$ et $\frac{1}{r}$. A une fonction bornée près, on a $\log(H(r(P))) = \log(H(r(P)-1)) = \log(H(\frac{1}{r(P)}))$. En additionnant les trois inégalités obtenues, et en posant $m = \mathrm{Card}(r^{-1}(\{0,1,\infty\}))$, on obtient donc pour $P \in C(\mathbb{Q}) - r^{-1}(\{0,1,\infty\})$:

$$\log(N(r(P))) < \frac{m}{d}\log(H(r(P))) + O(1+\sqrt{\log(H(r(P)))}) \tag{22}$$

Il est d'autant plus intéressant d'appliquer cette formule que le terme $\frac{m}{d}$ est petit. On a donc tout intérêt à considérer des fonctions r par lesquelles $\{0,1,\infty\}$ a le moins d'antécédents possible, à degré d fixé. Ces fonctions sont celles dont toute la ramification se situe au-dessus de $\{0,1,\infty\}$: ce sont les fonctions de Belyi.

Démontrons (comme dans [6]) la conjecture de Mordell à partir de la conjecture *abc*. Soit C une courbe de genre au moins 2. On se limite au cas où C est projective et lisse. Alors le théorème de Belyi (cité au paragraphe 4.5) affirme qu'il existe une fonction r de Belyi sur C. Notons d le degré de r. La formule de Riemann-Hurwitz s'écrit dans ce cas (voir [28], page 41):

$$\sum_{x \in C}(e_x - 1) = 2d + 2g - 2$$

Comme r est une fonction de Belyi, on en déduit:

$$\mathrm{Card}(r^{-1}(\{0,1,\infty\})) = d - 2g + 2$$

Comme $g \geq 2$, ce cardinal est strictement inférieur à d, donc la conjonction de la conjecture *abc* (formulée comme ci-dessus) et de la formule (22) montre que $H(r(P))$ est borné. Donc $r(P)$ ne peut prendre qu'un nombre fini de valeurs; comme chaque point de $\mathbb{P}^1$ n'a qu'un nombre fini d'antécédents par r, cela montre qu'il n'y a qu'un nombre fini de points $P \in C(\mathbb{Q}) - r^{-1}(\{0,1,\infty\})$. Donc $C(\mathbb{Q})$ est fini. Ainsi, la conjecture *abc* implique celle de Mordell (qui a été démontrée par Faltings).

Dans le cas particulier où la courbe C est $\mathbb{P}^1$, la proposition 11 se démontre de façon élémentaire, et le terme d'erreur devient $0(1)$. On peut la formuler comme suit:

Proposition 12 *Soit r une fraction rationnelle de degré d définie sur $\mathbb{Q}$. Notons k le nombre de zéros de r dans $\mathbb{P}^1(\mathbb{C})$, comptés sans multiplicités. Alors il existe une constante μ telle que pour tout $x \in \mathbb{Q}$ qui n'est ni zéro ni pôle de r on ait:*

$$|\mathrm{rad}(r(x))| < \mu H(x)^k$$

DÉMONSTRATION : Dans ce cas particulier, la démonstration est élémentaire. Soit R et S deux polynômes à coefficients entiers, premiers entre eux, tels que $r = \frac{R}{S}$. Posons $k' = \varrho(R)$; alors $k' = k$ si $d(S) \leq d(R)$, et $k' = k - 1$ si $d(S) > d(R)$ (c'est le cas où l'infini est zéro de r). Notons $R = \prod_i P_i^{m_i}$ la décomposition de R en facteurs premiers dans $\mathbb{Z}[X]$; on a $k' = \sum_i d(P_i)$.

Notons R_1 et S_1 les polynômes homogènes associés à R et S. En notant Q_i le polynôme homogène associé à P_i, on obtient $R_1 = \prod_i Q_i^{m_i}$. D'autre part, écrivons x comme fraction irréductible $\frac{a}{b}$. On a alors :

$$r(x) = b^{d(S)-d(R)} \frac{R_1(a,b)}{S_1(a,b)}$$

Or on a le calcul suivant, où le symbole $\ll$ signifie que la majoration est vraie pour tout couple (a,b) d'entiers premiers entre eux tels que $R_1(a,b) \neq 0$, à une constante multiplicative près qui ne dépend que de r :

$$\begin{aligned} |\mathrm{rad}(R_1(a,b))| &= |\mathrm{rad}(\prod_i Q_i(a,b)^{m_i})| \\ &\leq |\mathrm{rad}(\prod_i Q_i(a,b))| \\ &\leq |\prod_i Q_i(a,b)| \\ &\ll H(x)^{k'} \end{aligned}$$

On distingue alors deux cas. D'une part, si $d(S) \leq d(R)$, on a :

$$|\mathrm{rad}(r(x))| \leq |\mathrm{rad}(R_1(a,b))| \ll H(x)^{k'} = H(x)^k$$

D'autre part, si $d(S) > d(R)$, on a $k' = k - 1$ d'où :

$$|\mathrm{rad}(r(x))| \leq |\mathrm{rad}(b)\mathrm{rad}(R_1(a,b))| \ll H(x)H(x)^{k'} = H(x)^k$$

Cela conclut la démonstration.

N.B. Si on applique cette proposition dans le cas où r est un polynôme P et x un entier naturel n, on obtient :

$$|\mathrm{rad}(P(n))| \ll n^{\varrho(P)}$$

On peut interpréter cette majoration en disant que si P a "beaucoup de multiplicité" alors $P(n)$ a aussi "beaucoup de multiplicité" quand n est grand. En effet, si P a "beaucoup de multiplicité" (c'est-à-dire si $\varrho(P)$ est sensiblement plus petit que $d(P)$), alors le radical de $P(n)$, qui est en $n^{\varrho(P)}$, est petit devant la valeur absolue de $P(n)$, qui est en $n^{d(P)}$.

Deuxième partie

Liens avec les courbes elliptiques.

6 Une conséquence de la conjecture de Szpiro sur les courbes elliptiques

NOTATIONS : Soit E une courbe elliptique. On note Δ (ou Δ_E) son discriminant minimal, j (ou j_E) son invariant modulaire, et N (ou N_E) son conducteur (pour la définition du conducteur d'une courbe elliptique, voir [28], page 361). Soit de plus n un entier naturel; on note E_n le groupe des points de n-torsion de $E(\bar{\mathbb{Q}})$ (qui est le sous-groupe de $E(\bar{\mathbb{Q}})$ formé des points dont l'ordre divise n).

Soit p un nombre premier. Alors E_p est un espace vectoriel de dimension 2 sur $\mathbb{Z}/p\mathbb{Z}$ (voir [28], page 89). Le groupe $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ agit sur E_p; cette action fournit une représentation $\rho_p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to Aut(E_p)$. Le groupe E_p est ainsi muni d'une structure de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-module.

Si E et E' sont deux courbes elliptiques définies sur $\mathbb{Q}$, isogènes sur $\mathbb{Q}$, alors E_p et E'_p sont isomorphes comme $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules pour tout nombre premier p qui ne divise pas le degré de l'isogénie. Le problème soulevé ici, et dont l'origine remonte à Mazur [16], est de savoir dans quelle mesure les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p peuvent être isomorphes sans que les courbes E et E' soient isogènes sur $\mathbb{Q}$.

On dit que les représentations $\rho_p^{(E)}$ et $\rho_p^{(E')}$ de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ dans E_p et E'_p respectivement sont isomorphes si les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p le sont.

Si on fixe les deux courbes elliptiques E et E', on a le résultat suivant :

Proposition 13 *Soit E et E' deux courbes elliptiques définies sur $\mathbb{Q}$ telles que, pour une infinité de nombres premiers p, les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p soient isomorphes. Alors les courbes elliptiques E et E' sont isogènes sur $\mathbb{Q}$.*

DÉMONSTRATION : Soit S l'ensemble des nombres premiers en lesquels l'une au moins des courbes, E ou E', a mauvaise réduction. Pour un nombre premier l n'appartenant pas à S, notons a_l et a'_l les traces des endomorphismes de Frobenius des courbes réduites modulo l (voir [28]). Alors pour p premier tel que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p soient isomorphes, et pour $l \notin S$, on a : $a_l \equiv a'_l \ mod(p)$ (d'après [22], 5.2). Pour l fixé, cette congruence est vraie par hypothèse pour une infinité de nombres premiers p. On a donc $a_l = a'_l$ pour tout nombre premier $l \notin S$. D'après [7], §5, cor.2, cela implique que E et E' sont isogènes sur $\mathbb{Q}$, d'où la proposition.

La proposition précédente décrit ce qui se passe quand on fixe E et E'. Si maintenant on fixe une courbe elliptique E et un nombre premier p, on peut chercher s'il existe des courbes elliptiques E', non isogènes à E sur $\mathbb{Q}$, telles que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p soient isomorphes. On a la proposition suivante :

Proposition 14 *Soit E une courbe elliptique définie sur $\mathbb{Q}$ et p un nombre premier. Alors :*

- *Si $p \in \{2, 3, 5\}$, il y a une infinité de classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques E' définies sur $\mathbb{Q}$ telles que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p soient isomorphes.*
- *Si $p \geq 7$, il n'y a qu'un nombre fini de classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques E' définies sur $\mathbb{Q}$ telles que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p soient isomorphes.*

Cette proposition est démontrée dans [9], en considérant une tordue galoisienne de la courbe modulaire $X(p)$.

Si $p \in \{2, 3, 5\}$, comme le nombre de classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques E' isogènes à E sur $\mathbb{Q}$ est fini (voir [28], page 264), cette proposition montre qu'il existe des courbes E' définies sur $\mathbb{Q}$, non isogènes à E sur $\mathbb{Q}$, et telles que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p soient isomorphes. Il existe même une infinité de telles courbes, deux à deux non isomorphes sur $\mathbb{Q}$.

En revanche, si $p \geq 7$, on ne sait pas a priori s'il existe de telles courbes elliptiques E'; et s'il en existe, elles sont en nombre fini (à $\mathbb{Q}$-isomorphisme près).

On note A_E l'ensemble des nombres premiers p pour lesquels il existe une courbe elliptique $E^{(p)}$ définie sur $\mathbb{Q}$, non isogène à E sur $\mathbb{Q}$, telle que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p soient isomorphes.

On sait déjà que A_E contient toujours les entiers 2, 3 et 5. Dans la section 7, on s'intéressera à des courbes pour lesquelles $7 \in A_E$. A l'heure actuelle, pour chaque nombre premier $p \leq 13$, on connaît des exemples de courbes elliptiques E pour lesquels $p \in A_E$. Mais la question de savoir s'il existe une courbe elliptique E et un nombre premier $p \geq 17$ tel que $p \in A_E$ est toujours ouverte.

Dans cette section, on va démontrer que pour toute courbe elliptique E définie sur $\mathbb{Q}$, l'ensemble A_E est fini, en admettant la conjecture suivante, qui est une conséquence de la conjecture *abc*:

Conjecture 3 (Szpiro) *Il existe deux constantes absolues α et β telles que, pour toute courbe elliptique E définie sur $\mathbb{Q}$, on ait:*

$$|\Delta_E| < \alpha N_E^{\beta}$$

Théorème 14 *La conjecture de Szpiro implique que pour toute courbe elliptique E définie sur $\mathbb{Q}$, l'ensemble A_E est fini.*

Pour démontrer ce théorème, on commence par considérer (pour E et p fixés) la représentation ρ_p donnant l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur le groupe des points de p-torsion de la courbe elliptique E. A cette représentation, J.P. Serre associe dans [24] un poids k et un conducteur $N(\rho_p)$, qui sont deux entiers vérifiant les propriétés suivantes (où on note v la valuation p-adique, normalisée par $v(p) = 1$):

Proposition 15 *Le poids k associé à la représentation ρ_p vérifie les assertions suivantes:*

- *On a $k \equiv 2\ mod(p-1)$.*
- *Si E a bonne réduction en p alors $k = 2$.*
- *Si E a mauvaise réduction en p de type multiplicatif alors, en notant j l'invariant modulaire de E, le poids k vaut 2 si p divise $v(j)$, $p+1$ si p ne divise pas $v(j)$ et $p \neq 2$, et enfin 4 si p ne divise pas $v(j)$ et $p = 2$.*

Cette proposition est démontrée dans [24], au 2.9, proposition 5. De plus, J.P. Serre détermine la valeur de k dans un cas particulier où E a une réduction de type additif en p. Dans le cas général, la valeur de k est donnée par un théorème de [10], page 6. De ce théorème on déduit la proposition suivante:

Proposition 16 *Si E admet une réduction de type additif en p avec $p > 7$ alors $k > 2$.*

Passons maintenant au conducteur $N(\rho_p)$ associé par Serre à la représentation ρ_p. Il est intéressant de le rapprocher du conducteur N de la courbe elliptique E. Pour cela, on écrit la décomposition en facteurs premiers $N = \prod_l l^{f_l}$ où l'exposant f_l est nul si, et seulement si, E a bonne réduction en l, vaut 1 si, et seulement si, E a mauvaise réduction de type multiplicatif en l, et est supérieur ou égal à 2 si, et seulement si, E a mauvaise réduction de type additif en l.

Notons $v_l(\Delta)$ la valuation l-adique du discriminant minimal de la courbe elliptique E. On a le résultat suivant:

Proposition 17 *Soit l un nombre premier. Alors la valuation l-adique de $N(\rho_p)$ vaut:*

- *0 si E a bonne réduction en l, ou si $l = p$.*
- *1 si E a mauvaise réduction de type multiplicatif en l et si p ne divise pas $v_l(\Delta)$.*
- *0 si E a mauvaise réduction de type multiplicatif en l et si p divise $v_l(\Delta)$.*
- *f_l si E a mauvaise réduction de type additif et si $p \geq 5$.*

N.B. En particulier, le conducteur de la représentation ρ_p est un entier premier à p qui divise le conducteur de la courbe elliptique E.

Cette proposition résulte de la définition du conducteur donnée par Serre dans [24]; voir aussi [10], page 28.

On peut maintenant énoncer et démontrer la proposition centrale de cette section:

Proposition 18 *Soient p un nombre premier, E et E' deux courbes elliptiques telles que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et E'_p soient isomorphes.*

Notons $\rho_p^{(E)}$ et $\rho_p^{(E')}$ les représentations donnant l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur les points de p-torsion de E et E' respectivement.

Supposons $p > 7$ et $N(\rho_p^{(E)}) = N_E$.

Alors il existe un entier naturel non nul u tel que $N_{E'} = uN_E$ et u^p divise $\Delta_{E'}$.

De plus, pour tout nombre premier l qui divise u, E' a une réduction multiplicative en l et p divise $v_l(\Delta_{E'})$.

N.B. L'hypothèse $N(\rho_p^{(E)}) = N_E$ équivaut, d'après la proposition 17, au fait que E ait bonne réduction en p et qu'il n'existe aucun nombre premier l divisant Δ_E en lequel E ait réduction multiplicative avec $p \mid v_l(\Delta_E)$.

N.B. On verra dans la démonstration qu'en fait l'hypothèse $p > 7$ peut être remplacée par : $p \geq 5$ et E' n'a pas une réduction additive en p. En effet, cette hypothèse n'intervient qu'à la fin de la démonstration, pour éliminer un cas.

DÉMONSTRATION : On a $N_E = N(\rho_p^{(E)}) = N(\rho_p^{(E')})$, par hypothèse et car $\rho_p^{(E)}$ et $\rho_p^{(E')}$ sont isomorphes. Comme $N(\rho_p^{(E')})$ divise $N_{E'}$ (d'après la proposition 17), on en déduit que N_E divise $N_{E'}$. Notons u le quotient. Soit l un nombre premier divisant u. Distinguons deux cas :

1. Premier cas : Si $l \neq p$: comme $v_l(N(\rho_p^{(E')}) < v_l(N_{E'})$, la réduction de E' en l (qui est mauvaise puisque $l \mid N_{E'}$) ne peut pas être de type additif (d'après la proposition 17, puisque $p \geq 5$). Donc E' admet en l une réduction de type multiplicatif, d'où $v_l(N_{E'}) = 1$ puis $v_l(N_E) = v_l(N(\rho_p^{(E')})) = 0$ et $v_l(u) = 1$. Enfin, comme $v_l(N(\rho_p^{(E')})) = 0$ et que la réduction de E' en l est de type multiplicatif, la proposition 17 montre que $v_l(\Delta_{E'})$ est un multiple non nul de p.

2. Deuxième cas : si $l = p$. L'hypothèse $N(\rho_p^{(E)}) = N_E$ implique $p \nmid N_E$, donc E a bonne réduction en p, et le poids de $\rho_p^{(E)}$ vaut 2 (par la proposition 15). Donc $\rho_p^{(E')}$, qui lui est isomorphe, a aussi pour poids 2. Tout dépend alors du type de réduction de E' en p :

   - Si E' a bonne réduction en p, alors p ne divise pas $N_{E'}$ donc p ne divise pas u et il n'y a rien à démontrer.
   - Si E' a mauvaise réduction de type multiplicatif en p alors $v_p(u) = 1$. De plus, comme le poids de $\rho_p^{(E')}$ vaut 2, la proposition 15 implique que p divise $v_p(j_{E'})$, donc $v_p(\Delta_{E'})$ est un multiple (non nul) de p.
   - Si E' a mauvaise réduction de type additif en p, il y a contradiction avec la proposition 16 puisque $p > 7$ et que le poids de $\rho_p^{(E')}$ est 2.

N.B. En fait, quand $p > 7$ (ou quand $p \geq 5$ et que E' n'a pas de réduction additive en p), cette proposition montre aussi que l'entier u est sans facteur carré.

On peut maintenant démontrer le théorème 14 :

DÉMONSTRATION du théorème 14 : Raisonnons par l'absurde. Soit E une courbe elliptique telle que l'ensemble A_E soit infini. Cela signifie qu'il existe des nombres premiers p arbitrairement grands pour lesquels on peut trouver des courbes elliptiques $E^{(p)}$ telles que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_p et $E_p^{(p)}$ soient isomorphes, sans que les courbes elliptiques E et $E^{(p)}$ ne soient isogènes sur $\mathbb{Q}$. Or, d'après la proposition 17, il existe une constante c_E ne dépendant que de E telle que pour $p > c_E$ on ait $N(\rho_p^{(E)}) = N_E$. Quitte à supposer $c_E \geq 7$, on peut donc appliquer la proposition 18 à E et $E^{(p)}$, pour $p > c_E$. On en déduit l'existence d'un entier u_p tel que $N_{E^{(p)}} = u_p N_E$ et

$u_p^p \mid \Delta_{E^{(p)}}$, d'où $u_p^p \leq \Delta_{E^{(p)}}$. La conjecture 3 (de Szpiro) appliquée à la courbe elliptique $E^{(p)}$ donne :

$$u_p^p \leq \Delta_{E^{(p)}} < \alpha N_{E^{(p)}}^{\beta} = \alpha N_E^{\beta} u_p^{\beta}$$

On a donc : $u_p^{p-\beta} < \alpha N_E^{\beta}$. Cette inégalité a un sens (et est vraie) pour une infinité de nombres premiers p. Elle démontre que, pour p assez grand (à partir d'un rang qui ne dépend que de E, puisque les constantes α et β sont absolues), on a $u_p = 1$ c'est-à-dire $N_{E^{(p)}} = N_E$. Or il n'y a qu'un nombre fini de classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques définies sur $\mathbb{Q}$ ayant même conducteur que E. Comme la relation $N_{E^{(p)}} = N_E$ est vraie pour une infinité de valeurs de p, il existe une classe d'isomorphisme $\mathcal{C}$ de courbes elliptiques à laquelle appartiennent une infinité de courbes $E^{(p)}$. Soit $E' \in \mathcal{C}$. Alors, pour une infinité de p, $\rho_p^{(E)}$ et $\rho_p^{(E')}$ sont isomorphes (car, pour chacun de ces p, E' est isomorphe à $E^{(p)}$). La proposition 13 montre que E est isogène à E', donc à certaines courbes $E^{(p)}$, ce qui contredit la définition de ces courbes. Cette contradiction termine la démonstration du théorème 14.

7 Quelques pistes dans le cas où p vaut 7

Dans cette section, on considérera principalement le cas où $p = 7$. On cherche des moyens de trouver des paires de courbes elliptiques (E, E') non isogènes sur $\mathbb{Q}$ et telles que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_7 et E_7' soient isomorphes.

7.1 Critère d'isomorphisme des représentations

Tout d'abord, on a besoin d'un critère permettant de savoir si un couple (E, E') convient. Un tel critère, applicable dans de nombreux cas, est donné par la proposition suivante (dans laquelle p désigne un nombre premier quelconque) :

Proposition 19 *Supposons que E et E' soient des courbes de Weil. Notons S l'ensemble des nombres premiers l en lesquels l'une des courbes a une réduction multiplicative déployée et l'autre une réduction multiplicative non déployée.*

Posons $M = ppcm(N_E, N_{E'}) \prod_{l \in S} l$
et $\mu(M) = M \prod_{l \mid M,\, l\ premier} (1 + l^{-1})$.

Alors les conditions suivantes sont équivalentes :

1. *Les représentations $\rho_p^{(E)}$ et $\rho_p^{(E')}$ ont des semi-simplifiées isomorphes.*
2. *Pour tout nombre premier $l \leq \mu(M)/6$ ne divisant pas $N_E N_{E'}$ on a $a_l \equiv a_l' \ mod(p)$ et pour tout nombre premier $l \leq \mu(M)/6$ tel que $l \mid N_E N_{E'}$ et $l^2 \nmid N_E N_{E'}$ on a $a_l a_l' \equiv l + 1 \ mod(p)$.*

N.B. Cette proposition est démontrée dans [11]; elle y apparaît avec une erreur, l'inégalité large $l \leq \mu(M)/6$ y étant notée stricte.

Une courbe de Weil (aussi appelée courbe modulaire) est une courbe elliptique telle que la série $\sum_n a_n q^n$ (où les a_n sont les coefficients de la fonction L de Hasse-Weil de la courbe elliptique) définisse une forme parabolique primitive (c'est-à-dire une "newform" au sens d'Atkin-Lehner) de poids 2 et de niveau N_E. La conjecture de Taniyama-Weil affirme que toute courbe elliptique sur $\mathbb{Q}$ est de Weil. Elle a été démontrée par Wiles, Diamond, Taylor et Conrad dans le cas où 27 ne divise pas le conducteur de la courbe elliptique (voir [30]).

Quelques définitions sont nécessaires sur les représentations linéaires de groupes. Elles sont faites ici dans le cas particulier de ρ_p, où l'espace vectoriel considéré est de dimension 2 sur $\mathbb{Z}/p\mathbb{Z}$. Elles se généralisent bien sûr aux autres représentations linéaires.

La représentation ρ_p est dite irréductible (ou simple) s'il n'existe aucun sous-espace strict (c'est-à-dire aucune droite) stable par l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. Dans le cas contraire, ρ_p est dite réductible.

La représentation ρ_p est dite semi-simple si elle est somme directe de représentations simples. Deux cas peuvent se présenter : que ρ_p elle-même soit irréductible, ou bien qu'elle soit somme directe de deux représentations de dimension 1 (qui sont nécessairement irréductibles). Le deuxième cas signifie qu'on peut décomposer l'espace vectoriel E_p en somme directe de deux droites, chacune étant stable par l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

La semi-simplifiée de ρ_p est ρ_p elle-même si elle est irréductible. Sinon, on peut décomposer E_p en une somme directe $F \oplus G$ de deux droites telle que F soit stable par ρ_p. Dans une base de E_p respectant cette somme directe, la matrice de $\rho_p(\sigma)$ est triangulaire supérieure, pour tout $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. La semi-simplifée ρ'_p de ρ_p est alors définie ainsi : pour tout $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, $\rho'_p(\sigma)$ est (dans la base citée ci-dessus) la matrice diagonale obtenue en remplaçant par 0 le coin supérieur droit de la matrice de $\rho_p(\sigma)$. Cette construction ne dépend ni du choix de la base, ni du choix éventuel de la décomposition de E_p en somme directe.

Ainsi définie, la semi-simplifiée de ρ_p est toujours une représentation semi-simple. De plus, la représentation ρ_p est irréductible si, et seulement si, sa semi-simplifiée l'est. En particulier, si $\rho_p^{(E)}$ et $\rho_p^{(E')}$ ont des semi-simplifiées isomorphes et que l'une est irréductible, alors l'autre aussi et elles sont isomorphes.

Cette remarque permet de déduire de la proposition précédente le corollaire suivant :

Corollaire 3 *Supposons que E et E' soient des courbes de Weil, et que $\rho_p^{(E)}$ soit irréductible. Notons S l'ensemble des nombres premiers l en lesquels l'une des courbes a une réduction multiplicative déployée et l'autre une réduction multiplicative non déployée.*

Posons $M = ppcm(N_E, N_{E'}) \prod_{l \in S} l$
et $\mu(M) = M \prod_{l \mid M,\ l\ premier} (1 + l^{-1})$.

Alors les conditions suivantes sont équivalentes :

1. *Les représentations $\rho_p^{(E)}$ et $\rho_p^{(E')}$ sont isomorphes.*
2. *Pour tout nombre premier $l \leq \mu(M)/6$ ne divisant pas $N_E N_{E'}$ on a $a_l \equiv a'_l \ mod(p)$ et pour tout nombre premier $l \leq \mu(M)/6$ tel que $l \mid N_E N_{E'}$ et $l^2 \nmid N_E N_{E'}$ on a $a_l a'_l \equiv l + 1 \ mod(p)$.*

7.2 Critères d'irréductibilité de ρ_p

La proposition précédente donne donc un critère d'isomorphisme de $\rho_p^{(E)}$ et $\rho_p^{(E')}$, à condition que les courbes soient de Weil et que l'une au moins des représentations soit irréductible. Ce critère se présente sous la forme d'un nombre fini de vérifications d'identités faisant intervenir les coefficients a_n et a'_n des fonctions L de Hasse-Weil des courbes elliptiques E et E' : il se prête à une vérification informatique. Quant au fait que les courbes soient de Weil, on peut souvent le déduire des travaux de Wiles, Diamond, Taylor et Conrad. Quand 27 divise le conducteur de la courbe, on admettra que la courbe est de Weil. Il reste alors un problème : comment montrer que l'une des représentations est irréductible ?

Dans le reste de cette section, on s'intéressera surtout au cas où p vaut 7. Mais pour p assez grand, le problème de l'irréductibilité de la représentation ρ_p ne se pose pas. En effet, on a la proposition suivante :

Proposition 20 *Soit E une courbe elliptique et p un nombre premier strictement supérieur à* 163. *Alors $\rho_p^{(E)}$ est irréductible.*

Par définition, $\rho_p^{(E)}$ est irréductible si, et seulement si, il n'existe pas de sous-groupe d'ordre p stable par l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. Cette proposition est alors le théorème 1′ de [23].

Ce problème d'irréductibilité de ρ_p s'interprète à l'aide de la courbe modulaire $Y_0(p)$ utilisée, par exemple, dans [23]. Cette courbe est la courbe algébrique sur $\mathbb{Q}$ dont les points paramètrent (c'est-à-dire sont en bijection avec) les couples (E, A) formés d'une courbe elliptique E et d'un sous-groupe A d'ordre p de E, à $\bar{\mathbb{Q}}$-isomorphisme près de ces couples (un $\bar{\mathbb{Q}}$-isomorphisme de (E, A) dans (E', A') étant un isomorphisme des courbes elliptiques E et E', défini sur $\bar{\mathbb{Q}}$, qui envoie A sur A'). Si K est un corps de nombres, un point (E, A) de $Y_0(p)(K)$ est formé par une courbe elliptique E définie sur K et un sous-groupe A de E, d'ordre p, lui aussi défini sur K, c'est-à-dire stable par l'action de $Gal(\bar{\mathbb{Q}}/K)$. En particulier, si $K = \mathbb{Q}$, un point rationnel sur la courbe $Y_0(p)$ est un couple formé par une courbe elliptique E définie sur $\mathbb{Q}$ et un sous-groupe A de E, d'ordre p, stable par l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. Ce sous-groupe, étant d'ordre p, est formé de points de p-torsion donc est un sous-groupe (et un sous-espace vectoriel) de E_p. La représentation $\rho_p^{(E)}$ associée à une telle courbe elliptique E est réductible; réciproquement, si une courbe elliptique E définie sur $\mathbb{Q}$ est telle que $\rho_p^{(E)}$ soit réductible alors il existe un point rationnel sur la courbe $Y_0(p)$ dont la première composante est E.

Or dans [23], Serre donne, pour chaque nombre premier p, le nombre de points rationnels de la courbe $Y_0(p)$. Ce nombre (s'il est fini) est un majorant du nombre de courbes elliptiques E telles que $\rho_p^{(E)}$ soit réductible. A priori, ce peut être un majorant strict car une courbe elliptique E peut avoir plusieurs sous-groupes d'ordre p ne se correspondant pas par des automorphismes de E, donc correspondant à des points différents de $Y_0(p)$. Ces résultats sont regroupés dans la proposition suivante :

Proposition 21 *1. Si $p \in \{2, 3, 5, 7, 13\}$, la courbe $Y_0(p)$ est de genre zéro; elle a une infinité de points rationnels.*

2. Si $p \in \{19, 43, 67, 163\}$, la courbe $Y_0(p)$ a exactement un point rationnel, qui correspond à une courbe elliptique E à multiplications complexes par l'anneau des entiers de $\mathbb{Q}(\sqrt{-p})$.

3. Si $p \in \{17, 37\}$, la courbe $Y_0(p)$ est de genre 1 (c'est une courbe elliptique); elle a exactement 2 points rationnels, échangés par l'involution d'Atkin-Lehner.

4. Si $p = 11$, la courbe $Y_0(p)$ a exactement trois points rationnels, deux du type 3 et un du type 2.

5. Si p n'appartient à aucun des ensembles ci-dessus, ce qui est le cas dès que $p > 163$, alors la courbe $Y_0(p)$ n'a aucun point rationnel, donc pour toute courbe elliptique E définie sur $\mathbb{Q}$ la représentation $\rho_p^{(E)}$ est irréductible.

N.B. L'involution d'Atkin-Lehner s'interprète dans ce cadre de la façon suivante (voir [11], Appendice I, 1.3) : à un couple (E, A) elle associe le couple formé de la courbe elliptique quotient E/A et de son sous-groupe d'ordre p E_p/A.

Pour $p \notin \{2, 3, 5, 7, 13\}$, la courbe $Y_0(p)$ n'a donc que quelques points rationnels, qui peuvent être de deux natures :

- Des points correspondant à des courbes à multiplications complexes par $\mathbb{Q}(\sqrt{-p})$. De telles courbes n'existent que pour $p \in \{2, 3, 7, 11, 19, 43, 67, 163\}$, et sont connues explicitement. Si E est à multiplications complexes par $\mathbb{Q}(\sqrt{-p})$, il existe une isogénie $\phi : E \to E$ de degré p, définie sur $\mathbb{Q}$, dont le noyau est un sous-groupe A de E_p, d'ordre p, stable par $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. A cette courbe correspond donc un point $(E, A) \in Y_0(p)(\mathbb{Q})$.

- Des points "exceptionnels". Ils existent pour $p \in \{11, 17, 37\}$, et pour chacune de ces valeurs de p constituent une paire de points échangés par l'involution d'Atkin-Lehner. Pour $p \in \{11, 17\}$, les courbes elliptiques correspondantes sont données explicitement dans [2], pages 78 à 80. Pour $p = 37$, l'étude est menée dans [18], §5.

Le problème de savoir si, étant donnés un nombre premier p et une courbe elliptique E, la représentation $\rho_p^{(E)}$ est irréductible est donc résolu pour de nombreuses valeurs de p: dès que $p \notin \{2,3,5,7,13\}$, la proposition ci-dessus montre que $\rho_p^{(E)}$ est irréductible, à quelques exceptions près qui sont connues explicitement.

Si maintenant $p \in \{2,3,5,7,13\}$, la courbe $Y_0(p)$ est unicursale, c'est-à-dire qu'il existe une fonction définie sur $\mathbb{Q}$ $f : Y_0(p)(\bar{\mathbb{Q}}) \to \bar{\mathbb{Q}}$ telle que pour tout corps de nombres K, f induise une paramétrisation bijective $Y_0(p)(K) \to K$. Pour $p = 7$, une telle fonction, notée v, est définie dans [11], Appendice I, 1.4. Elle vérifie la relation suivante: $(v^2 + 5v + 1)^3(v^2 + 13v + 49) - jv = 0$, où j est l'invariant modulaire $Y_0(7)(\bar{\mathbb{Q}}) \to \bar{\mathbb{Q}}$ qui à un couple (E, A) associe l'invariant modulaire j_E de la courbe elliptique E. Comme la fonction v est définie sur $\mathbb{Q}$, si on se donne une courbe elliptique E définie sur $\mathbb{Q}$ telle que $\rho_7^{(E)}$ soit réductible, ce qui correspond à un point rationnel $P = (E, A)$ de la courbe $Y_0(7)$, l'image $v(P)$ de P par v sera un nombre rationnel vérifiant: $(v(P)^2 + 5v(P) + 1)^3(v(P)^2 + 13v(P) + 49) - j_E v(P) = 0$. On a donc le critère suivant:

Proposition 22 *Soit E une courbe elliptique d'invariant modulaire j_E telle que le polynôme $(X^2 + 5X + 1)^3(X^2 + 13X + 49) - j_E X$ n'ait aucune racine rationnelle. Alors la représentation $\rho_7^{(E)}$ est irréductible.*

Des critères analogues existent pour $p \in \{2,3,5,13\}$. En effet, il suffit de connaître l'expression de j comme fraction rationnelle en v, où v désigne une paramétrisation de $Y_0(p)(\bar{\mathbb{Q}})$ par $\mathbb{P}^1(\bar{\mathbb{Q}})$. Or cette expression de trouve dans [8].

La proposition 22 présente l'avantage d'être très facile à tester sur chaque exemple. Une autre possibilité est d'utiliser les tables de [4], si la courbe E y figure (c'est-à-dire si le conducteur de E est inférieur à 1000 pour la version publiée, à 5000 pour la version informatique). En effet, ces tables donnent la liste des nombres premiers p tels qu'il existe une isogénie de degré p, définie sur $\mathbb{Q}$, de E vers une courbe elliptique E'. Ce sont exactement les nombres premiers tels que E admette un sous-groupe d'ordre p stable par $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, c'est-à-dire tels que $\rho_p^{(E)}$ soit réductible. Ainsi, pour les courbes E figurant dans ces tables, la vérification de la surjectivité de $\rho_7^{(E)}$ est immédiate.

Une autre façon de démontrer que $\rho_p^{(E)}$ est irréductible (pour une courbe elliptique E et un nombre premier p quelconques) est de démontrer qu'elle est surjective (vue comme application de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ dans le groupe $GL(E_p)$ des automorphismes linéaires de l'espace vectoriel E_p). Il est clair que toute représentation surjective est irréductible, la réciproque étant fausse en général. Elle est cependant vraie pour les courbes elliptiques semi-stables, d'après la proposition 21 (page 306) de [22]. Cette proposition donne comme corollaire immédiat le résultat suivant:

Proposition 23 *Soit E une courbe elliptique semi-stable définie sur $\mathbb{Q}$ et p un nombre premier supérieur ou égal à 7. Si $a_l \equiv 1 + l \ mod(p)$ pour tout nombre premier l sauf un nombre fini, alors $\rho_p^{(E)}$ est réductible.*

On a aussi la proposition suivante, démontrée dans [16]:

Proposition 24 *Soit E une courbe elliptique semi-stable définie sur $\mathbb{Q}$ et p un nombre premier supérieur ou égal à 11. Alors $\rho_p^{(E)}$ est surjective.*

7.3 Recherche de couples, avec $p = 7$

Dans cette section, on cherche une méthode pour essayer de trouver (sans aucune garantie d'en trouver réellement) des couples (E, E') de courbes elliptiques définies sur $\mathbb{Q}$ telles que les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_7 et E'_7 soient isomorphes; dans la suite, il est sous-entendu qu'on cherche de tels couples où E et E' ne sont pas isogènes sur $\mathbb{Q}$. De plus, on cherche bien sûr les courbes E et E' à isomorphisme près.

On se limite à chercher des couples (E, E') tels que $\rho_7^{(E)}$, donc $\rho_7^{(E')}$, soient irréductibles. En effet, ce n'est que sous cette hypothèse que le corollaire 3 permet de savoir si $\rho_7^{(E)}$ et $\rho_7^{(E')}$ sont isomorphes. De plus, on admet que toutes les courbes elliptiques qu'on rencontrera sont de Weil.

Dans la suite de cette partie, "tester" un couple (E, E') signifie appliquer la vérification directe dans les tables de [4] (ou à défaut la proposition 22) à E (pour montrer que $\rho_7^{(E)}$ est irréductible), puis le corollaire 3 (pour montrer que $\rho_7^{(E)}$ et $\rho_7^{(E')}$ sont isomorphes). Ce test se programme sans problèmes; s'il réussit, il démontre que $\rho_7^{(E)}$ et $\rho_7^{(E')}$ sont isomorphes. Sinon (du moins si la courbe E figure dans les tables de [4]), c'est que $\rho_7^{(E)}$ est réductible, ou que $\rho_7^{(E)}$ et $\rho_7^{(E')}$ ne sont pas isomorphes.

Si E ne figure pas dans les tables de [4], on n'a pas de condition nécessaire et suffisante d'irréductibilité de $\rho_7^{(E)}$. On applique la proposition 22, qui permet en général de montrer que $\rho_7^{(E)}$ est irréductible. Mais il pourrait arriver que cette proposition ne permette pas de conclure, même avec une représentation $\rho_7^{(E)}$ irréductible.

CONVENTION : Si E et E' sont de conducteurs différents, on notera E' celle qui a le conducteur le plus grand.

Dans la suite de cette section, on considère uniquement le cas où $p = 7$.

7.3.1 En partant de E'

Soit E' une courbe elliptique définie sur $\mathbb{Q}$. On cherche des courbes elliptiques E telles que $\rho_7^{(E)}$ et $\rho_7^{(E')}$ soient isomorphes. Avec la convention ci-dessus, seul un nombre fini de courbes elliptiques peuvent jouer le rôle de E : ce sont les courbes elliptiques de conducteur inférieur ou égal à $N_{E'}$. De plus, si $N_{E'} \leq 5000$, ces courbes sont données explicitement par les tables de [4] (qui ne sont publiées que pour des conducteurs inférieurs ou égaux à 1000, mais sont disponibles informatiquement jusqu'à 5000).

Supposons donc E' donnée, de conducteur inférieur ou égal 5000. On suppose que $\rho_7^{(E')}$ est irréductible. Alors une méthode simple consiste à tester successivement toutes les courbes E de conducteur inférieur ou égal à $N_{E'}$, en utilisant la liste donnée dans [4]. Cette méthode permet de trouver, parmi tous les couples (E, E') ainsi formés, ceux qui conviennent. Mais il se peut (et, en pratique, c'est souvent le cas) qu'aucune courbe elliptique E ne convienne.

D. Bernardi a mené cette recherche exhaustive pour toute courbe E' de conducteur inférieur ou égal à 5000, grâce aux tables de [4], et pour $p \in \{7, 11, 13, 17, 19, 23, 29\}$. Pour $p = 7$, il a trouvé environ 400 couples (E, E') tels que $\rho_7^{(E)}$ et $\rho_7^{(E')}$ soient isomorphes (avec la convention $N_E \leq N_{E'}$). Pour $p = 11$, il a trouvé 16 couples qui conviennent; pour $p = 11$, il en a trouvé 2. Enfin, pour $p \in \{13, 19, 23, 29\}$, il n'a trouvé aucun couple (E, E') de courbes elliptiques définies sur $\mathbb{Q}$, non isogènes sur $\mathbb{Q}$, de conducteurs inférieurs à 5000, et telles que $\rho_p^{(E)}$ et $\rho_p^{(E')}$ soient isomorphes.

Ici, on souhaite mener une recherche systématique dans le même esprit, c'est-à-dire une recherche qui permette, en testant de nombreux couples, d'espérer (sans garantie a priori de succès) en trouver quelques-uns qui conviennent. Toutefois, tester tous les couples (E, E') (comme D. Bernardi l'a fait) nécessite un long temps de calcul, et de bonnes connaissances informatiques. C'est pourquoi on se limite à tester les couples (E, E') qui vérifient les hypothèses de la proposition 18 (et du N.B. qui la suit), avec en plus $u > 1$ (en reprenant les notations de cette proposition). On cherche donc des couples (E, E') tels que $\rho_7^{(E)}$ et $\rho_7^{(E')}$ soient isomorphes, que E' n'ait pas une réduction additive en 7 et que $N(\rho_7^{(E)}) = N_E < N_{E'}$. De plus, on conserve l'hypothèse $N_{E'} \leq 5000$ pour pouvoir utiliser les tables de [4], ainsi que l'hypothèse d'irréductibilité de $\rho_7^{(E)}$. Alors, par la proposition 18, dans la décomposition en facteurs premiers du discriminant minimal de E', au

moins l'un des exposants qui apparaît est un multiple non nul de 7. De plus, si un tel exposant est relatif à un nombre premier l, alors E' admet une réduction multiplicative en l. En résumé, le type de Kodaira de E' en l est I_k, avec k multiple non nul de 7. Cette condition présente le double avantage d'être synthétique et d'apparaître dans les tables de [4]. De plus, le théorème de Mazur-Ribet (voir [20], III) entraîne que l'entier $u = N_{E'}/N_E$ est le produit des nombres premiers en lesquels E' admet un type de Kodaira I_k, avec k multiple non nul de 7.

Ces restrictions permettent d'obtenir une méthode à la fois simple et rapide :

- pour chaque courbe E' (tirée des tables de [4]) qui présente en au moins un nombre premier l un type de Kodaira I_k, avec k multiple non nul de 7,
- pour chaque courbe E (tirée des tables de [4]) de conducteur $N_{E'}/u$, où u est le produit des nombres premiers en lesquels E' admet un type de Kodaira I_k, avec k multiple non nul de 7,
- tester si $\rho_7^{(E)}$ et $\rho_7^{(E')}$ sont isomorphes.

Grâce à cette méthode, on trouve facilement quelques exemples de couples (E, E') qui conviennent (même si a priori on ne pouvait pas être sûr d'en trouver). Mais on s'aperçoit qu'il faut tester beaucoup de courbes E' (même parmi celles présentant un Kodaira de type I_k, avec k multiple non nul de 7) pour que l'une d'elles donne naissance à un couple (E, E') qui convienne.

Il est à noter que pour certains couples (E, E'), alors que le test d'isomorphisme des représentations donné par le corollaire 3 consiste à vérifier qu'on a $a_l \equiv a'_l \ mod(7)$ pour certains nombres premiers l et $a_l a'_l \equiv l + 1 \ mod(7)$ pour certains autres, ces congruences sont vérifiées au signe près. Précisément, il arrive qu'en remplaçant a_l par $\varepsilon_l a_l$, où ε_l est une suite bien choisie de 1 et de -1 (indexée par les nombres premiers l inférieurs ou égaux à $\mu(M)/6$), les congruences soient vérifiées sans problème de signe. Supposons de plus qu'il existe un entier n tel que la suite $\varepsilon_l = (\frac{n}{l})$ convienne (où $(\frac{n}{l})$ est le caractère de Dirichlet, qui vaut 1 si n est un carré non nul modulo l, -1 si ce n'est pas un carré, et 0 si l divise n). Alors la fonction L de Hasse-Weil de la tordue $E(n)$ de E par $\sqrt{n}$ a pour coefficients les entiers $(\frac{n}{l})a_l$ (du moins pour les nombres premiers l en lesquels E a bonne réduction). Donc le critère d'isomorphisme des représentations s'applique au couple formé par cette tordue et par E'. Bien entendu, on aurait aussi pu considérer le couple formé par E et la tordue de E' par $\sqrt{n}$.

7.3.2 Par la méthode de Darmon et Granville

Dans [5], H. Darmon et A. Granville remarquent qu'on peut construire des couples de courbes elliptiques ayant même représentation dans les points de p-torsion à partir de solutions d'une équation diophantienne. Le but de ce paragraphe est d'exposer cette méthode.

Soient p un nombre premier supérieur ou égal à 5 et a, b, c trois entiers non nuls tels que $a^2 + b^3 = c^p$. A cette solution d'équation diophantienne on associe une courbe elliptique E', dite de Frey, d'équation :

$$y^2 = x^3 + 3bx + 2a$$

Le discriminant de cette équation de Weierstrass est $-16(4b^3 + 27a^2) = -1728c^p$. La présence d'une puissance $p$ième dans le discriminant incite (au vu de la méthode proposée au paragraphe 7.3.1, en particulier du théorème de Mazur-Ribet) à considérer les couples formés par E' et par une courbe elliptique E de conducteur $N_{E'}/c$. Pour chacune de ces courbes E, qui sont données par les tables de [4] si $N_{E'} \leq 5000$, on applique au couple (E, E') le test expliqué au début de la section 7.3. On espère trouver ainsi au moins une courbe E telle que $\rho_7^{(E)}$ soit isomorphe à $\rho_7^{(E')}$; mais on n'a aucune certitude a priori d'en trouver.

Pour $p = 7$, une liste de solutions non triviales de l'équation diophantienne $a^2 + b^3 = c^p$ se trouve dans [5], page 515. Ce sont les suivantes :

$$21063928^2 - 76271^3 = 17^7$$

$$2213459^2 + 1414^3 = 65^7$$

$$15312283^2 + 9262^3 = 113^7$$

On pourrait y rajouter la solution $3^2 - 2^3 = 1^7$, mais celle-ci est trop particulière pour être utile dans la suite.

Ces solutions conduisent respectivement aux courbes de Frey suivantes :

$$y^2 = x^3 - 228813x + 42127856 \quad (23)$$

$$y^2 = x^3 + 4242x + 4426918 \quad (24)$$

$$y^2 = x^3 + 27786x + 30624566 \quad (25)$$

La courbe (23) a pour conducteur $864 \cdot 17$ et pour discriminant $-2^6 3^3 17^7$, ce qui suggère de tester les courbes E de conducteur $N_{E'}/17 = 864$. Parmi celles-ci, on trouve la courbe suivante, qui convient :

$$y^2 = x^3 - 3x - 6 \quad (23')$$

La courbe (24) a pour conducteur $1728 \cdot 65$, et pour discriminant $-2^6 3^3 5^7 13^7$. Cela suggère de tester les courbes E de conducteur 1728. Parmi celles-ci, on trouve la courbe suivante, qui convient :

$$y^2 = x^3 - 12x + 48 \quad (24')$$

La courbe (25) a pour conducteur $576 \cdot 113$, et pour discriminant $-2^6 3^3 113^7$, ce qui suggère de tester les courbes E de conducteur 576. Parmi celles-ci, on trouve la courbe suivante, qui convient :

$$y^2 = x^3 - 3x \quad (25')$$

Enfin, la solution particulière $3^2 - 2^3 = 1$ de l'équation diophantienne conduit à la courbe d'équation $y^2 = x^3 - 6x + 6$, qui est de conducteur 1728, et a pour discriminant $-2^6 3^3 = -1728$; dans ce discriminant ne figure aucune puissance septième, ce qui était prévu car le terme noté c dans l'équation diophantienne vaut 1. Pour espérer trouver un couple (E, E') qui convient et qui vérifie les hypothèses de la proposition 18, on doit chercher E et E' de même conducteur. Mais on ne trouve aucune courbe qui convienne.

On remarque que les courbes (23') et (24') sont tordues l'une de l'autre par $\sqrt{-2}$. Or, si on part de deux courbes elliptiques ayant même représentation dans les points de p-torsion, et qu'on les tord toutes les deux par $\sqrt{d}$ (avec $d \in \mathbb{Z} - \{0\}$), on obtient deux nouvelles courbes qui ont même représentation dans les points de p-torsion. Ainsi, on peut tordre (23), (24), (23') et (24') par les racines carrées d'entiers bien choisis, pour obtenir les trois courbes suivantes, qui ont des représentations isomorphes dans les points de 7-torsion :

$y^2 = x^3 - 228813x - 42127856$	qui est (23) tordue par i
$y^2 = x^3 + 16968x + 35415344$	qui est (24) tordue par $\sqrt{2}$
$y^2 = x^3 - 3x + 6$	qui est tordue de (23') et de (24')

Ce triplet de courbes elliptiques, ainsi que la paire formée par (25) et (25'), apparaissent dans [5].

La méthode exposée ici a permis de trouver, à partir de chacune des trois solutions de l'équation diophantienne citées plus haut (pour lesquelles c vaut respectivement 17, 65 et 113), un couple (E, E') qui convient. En cela, cette méthode est remarquable; elle contraste avec la méthode exposée au paragraphe 7.3.1, par laquelle on ne réussit à trouver un couple (E, E') de courbes elliptiques qui convient qu'en testant plusieurs dizaines de courbes E'.

7.3.3 Par la méthode de Kraus et Oesterlé

Dans [11], A. Kraus et J. Oesterlé exhibent le couple (E, E') suivant (où on a inversé les rôles de E et E', pour que le conducteur de E' soit plus grand que celui de E) :

(E)	$y^2 = x^3 + x^2 - x + 3$	de conducteur $2^3 \cdot 19 = 152$
(E')	$y^2 = x^3 + 7x^2 + 28$	de conducteur $2^3 \cdot 7^2 \cdot 19 = 7448$

Ils démontrent que les représentations $\rho_7^{(E)}$ et $\rho_7^{(E')}$ sont isomorphes, et que l'isomorphisme est compatible avec les accouplements de Weil. Pour démontrer l'isomorphisme des représentations, ils utilisent le critère donné par le corollaire 3.

Ils expliquent ensuite comment ils ont trouvé cet exemple.

On cherche une courbe elliptique E' définie sur $\mathbb{Q}$ telle que $\rho_7^{(E')}$ soit irréductible, de poids 2, de conducteur $N(\rho_7^{(E')})$ différent de $N_{E'}$ et inférieur ou égal à 5000 (pour pouvoir utiliser la version informatique des tables de [4]). Une conjecture de Serre (énoncée en toute généralité dans [24], numéro 3.2.4 page 196, et démontrée dans [26] dans le cas particulier de la représentation $\rho_p^{(E')}$ quand E' est de Weil) affirme que dans cette situation il existe une forme parabolique normalisée $f = q + \sum_{n\geq 2} a_n(f)q^n$, primitive (i.e. newform au sens d'Atkin-Lehner), de poids 2, de niveau $N(\rho_7^{(E')})$, qui est fonction propre des opérateurs de Hecke T_l pour $l \nmid N(\rho_7^{(E')})$, et où les a_n sont des entiers algébriques (éléments de $\bar{\mathbb{Z}}$, anneau des entiers de $\bar{\mathbb{Q}}$) tels qu'il existe un idéal premier $\mathcal{P}$ de $\bar{\mathbb{Z}}$ au-dessus de $7\mathbb{Z}$ avec, pour tout l premier ne divisant pas $7N(\rho_7^{(E')})$: $a_l(E') = a_l(f) \ mod(\mathcal{P})$. Supposons que, par chance, les coefficients $a_n(f)$ puissent être choisis dans $\mathbb{Z}$. Alors un théorème de Weil (voir [20], début du 4.D) affirme que f est la fonction de Hasse-Weil d'une courbe elliptique E définie sur $\mathbb{Q}$, de conducteur $N_E = N(\rho_7^{(E')})$. Pour connaître explicitement cette courbe elliptique E, il suffit de tester l'une après l'autre les courbes de conducteur $N(\rho_7^{(E')})$, comme expliqué au début du paragraphe 7.3. Si on n'en trouve aucune qui convienne, c'est que l'hypothèse selon laquelle on peut choisir les $a_n(f)$ dans $\mathbb{Z}$ est erronnée.

Pour trouver une courbe elliptique E' à laquelle appliquer le raisonnement précédent, on peut la chercher sous la forme :

$$y^2 = x^3 + 7ax^2 + 7b \text{ avec } a, b \in \mathbb{Z}$$

Le discriminant de cette équation de Weierstrass est $\Delta_{E'} = -2^4 7^2 (28a^3 + 27b^2)$, donc E' est bien une courbe elliptique pour $(a, b) \neq (0, 0)$. Elle a une réduction additive en 7. Donc 7 (et même 7^2) divise $N_{E'}$; comme $N(\rho_7^{(E')})$ est premier à 7 et divise $N_{E'}$, on a bien $N(\rho_7^{(E')}) < N_{E'}$. De plus, si b est premier à 7, le poids de $\rho_7^{(E')}$ est 2 (d'après [10], page 6).

En prenant $(a, b) = (1, 4)$ on trouve l'exemple cité en introduction de ce paragraphe.

8 Extension à $p = 8$

Dans cette section, on mène une recherche analogue à celle de la section précédente, mais en remplaçant le nombre premier 7 par 8 : on cherche des couples (E, E') de courbes elliptiques définies sur $\mathbb{Q}$, non isogènes sur $\mathbb{Q}$, telles que les représentations $\rho_8^{(E)}$ et $\rho_8^{(E')}$ soient isomorphes.

Le groupe E_8 des points de 8-torsion d'une courbe elliptique E ne forme plus un espace vectoriel, mais un $\mathbb{Z}/8\mathbb{Z}$-module libre de rang 2. La notion d'irréductibilité de $\rho_8^{(E)}$ n'a donc pas de sens; celle de surjectivité en conserve un.

Etant donné deux courbes elliptiques E et E', montrer que $\rho_8^{(E)}$ et $\rho_8^{(E')}$ sont isomorphes est difficile. L'essentiel de cette section sera consacré à essayer de déterminer des conditions suffisantes d'isomorphisme de ces représentations. Un résultat dû à Mazur permet de généraliser le critère d'isomorphisme obtenu pour $p = 7$ à la section précédente. C'est l'objet du paragraphe suivant.

8.1 Utilisation d'un résultat de Mazur

Dans [17], page 254, est démontré le résultat suivant :

Proposition 25 *Soient A un anneau local fini, ρ et ρ' deux représentations continues de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ dans $GL_2(A)$, non ramifiées en-dehors d'un ensemble fini E de places ultramétriques de $\mathbb{Q}$.*

Supposons que ρ soit résiduellement absolument irréductible
et qu'on ait $Trace(\rho(Frob_l)) = Trace(\rho'(Frob_l))$ pour tout nombre premier $l \notin E$.
Alors ρ et ρ' sont isomorphes.

N.B. En fait, Mazur démontre cette proposition dans le cas plus général où les représentations sont à valeurs dans $GL_N(A)$, et où A est un anneau local noethérien, complet, de corps résiduel fini. Ici, on appliquera cette proposition avec $N = 2$ et $A = \mathbb{Z}/8\mathbb{Z}$, donc la version citée ci-dessus suffit.

Pour comprendre l'énoncé de cette proposition, on a besoin de la définition suivante :

DÉFINITION : Soit A un anneau local de corps résiduel k, et ρ une représentation de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ dans $GL_2(A)$. Alors ρ induit une représentation $\rho_1 : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(k)$, puis par extension des scalaires une représentation $\rho_2 : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\bar{k})$. On dit que ρ est résiduellement absolument irréductible si ρ_1 est absolument irréductible, c'est-à-dire si ρ_2 est irréductible.

Grâce à cette proposition, on va démontrer le théorème suivant :

Théorème 15 *Soient E et E' des courbes de Weil. Notons S l'ensemble des nombres premiers l en lesquels l'une des courbes a une réduction multiplicative déployée et l'autre une réduction multiplicative non déployée.*

Posons $M = ppcm(N_E, N_{E'}) \prod_{l \in S} l$
et $\mu(M) = M \prod_{l|M,\, l\ premier} (1 + l^{-1})$.

Supposons que :

1. *Pour tout nombre premier $l \leq \mu(M)/6$ ne divisant pas $N_E N_{E'}$ on a $a_l \equiv a'_l \ mod(8)$*
2. *Pour tout nombre premier $l \leq \mu(M)/6$ tel que $l \mid N_E N_{E'}$ et $l^2 \nmid N_E N_{E'}$ on a $a_l\, a'_l \equiv l + 1 \ mod(8)$*
3. *La représentation $\rho_8^{(E)}$ est surjective.*

Alors $\rho_8^{(E)}$ et $\rho_8^{(E')}$ sont isomorphes.

DÉMONSTRATION du théorème : Les relations de congruence vérifiées par les coefficients a_l et a'_l montrent (par un raisonnement analogue à la démonstration de la proposition 4 de [11]) que pour tout nombre premier l qui ne divise pas $N_E N_{E'}$ on a $a_l \equiv a'_l \ mod(8)$. Compte tenu du lemme 13 ci-dessous, la proposition 25 permet de conclure.

Lemme 13 *Soit E une courbe elliptique telle que $\rho_8^{(E)}$ soit surjective. Alors $\rho_8^{(E)}$ est résiduellement absolument irréductible.*

DÉMONSTRATION du lemme : Par projection sur le quotient, le $\mathbb{Z}/8\mathbb{Z}$-module libre E_8 de rang 2 s'envoie sur le $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel E_2 de dimension 2 par l'application qui à un point P associe $4P$. Cette projection commute aux actions de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur E_8 et sur E_2, donc la représentation induite par $\rho_8^{(E)}$ sur le quotient est $\rho_2^{(E)}$. Or $\rho_2^{(E)}$ est surjective (car $\rho_8^{(E)}$ l'est), donc elle est absolument irréductible. Cela conclut la démonstration du lemme.

Le théorème 15 sert de critère pour tester l'isomorphisme des représentations $\rho_8^{(E)}$ et $\rho_8^{(E')}$ associées à deux courbes elliptiques E et E'. En cela, il remplace le corollaire 3, qui n'était valable que pour p premier. Il est à noter que dans ce théorème, l'hypothèse d'irréductibilité (qui apparaissait dans le corollaire 3, et qui n'a plus de sens quand $p = 8$) est remplacée par l'hypothèse de surjectivité de $\rho_8^{(E)}$. Le test concernant les relations de congruence vérifiées par les coefficients des fonctions L de Hasse-Weil des courbes elliptiques ne change pas. C'est pourquoi la méthode exposée au paragraphe 7.3.1 est toujours valable, en remplaçant simplement 7 et 8.

Cependant, un problème majeur se pose : étant donnée une courbe elliptique E, il est difficile de vérifier la surjectivité de $\rho_8^{(E)}$. Il s'agit de démontrer que l'image de $\rho_8^{(E)}$ est $GL_2(\mathbb{Z}/8\mathbb{Z})$ en entier, qui est de cardinal $1536 = 3 \cdot 2^9$. Cela signifie que le corps laissé fixe par le noyau de $\rho_8^{(E)}$, qui est l'extension de $\mathbb{Q}$ engendrée par les coordonnées des points de $E_8(\bar{\mathbb{Q}})$, est de degré 1536 sur $\mathbb{Q}$. Dans chaque cas particulier, on pourrait en théorie effectuer cette vérification par ordinateur, en calculant le degré sur $\mathbb{Q}$ de ce corps. Mais en l'absence de propriétés permettant de le rendre plus rapide, un tel calcul dépasse les capacités informatiques actuelles. On doit donc chercher à comprendre la structure de cette extension de $\mathbb{Q}$. Pour les points d'ordre 8, c'est une question trop difficile pour être abordée ici. On se limitera aux points d'ordre 4, ce qui permet de savoir si $\rho_4^{(E)}$ est surjective.

L"objectif du paragraphe suivant est d'obtenir une description de l'extension de $\mathbb{Q}$ engendrée par les coordonnées des points de 4-torsion, de façon à savoir si $\rho_4^{(E)}$ est surjective.

8.2 Etude de la surjectivité de $\rho_4^{(E)}$

8.2.1 Calculs préliminaires

Les notations et les résultats de ce paragraphe sont tirés de [13], pages 218 à 220.

Soit E une courbe elliptique donnée par une équation de Weierstrass de la forme

$$y^2 = x^3 + ax + b$$

Le groupe E_4 des points de 4-torsion forme un $\mathbb{Z}/4\mathbb{Z}$-module libre de rang 2. Notons (P, Q) une base de ce module. Alors les points d'ordre 4 exactement sont les $\lambda P + \mu Q$ avec $(\lambda, \mu) \in (\mathbb{Z}/4\mathbb{Z})^\star \times (\mathbb{Z}/4\mathbb{Z})^\star$. Les points d'ordre 2 exactement sont $2P$, $2Q$ et $2(P+Q)$. Compte tenu de la forme de l'équation de Weierstrass, ils ont une ordonnée nulle. Définissons e_1, e_2 et e_3 comme les abscisses respectives de ces trois points. On a ainsi :

$$2P = (e_1, 0) \quad 2Q = (e_2, 0) \quad 2(P+Q) = (e_3, 0)$$

Dans l'équation de Weierstrass, les e_i sont les racines du membre de droite, donc ils sont liés par la relation :

$$e_1 + e_2 + e_3 = 0$$

Notons $\delta = 4(e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$. On a alors : $\delta^2 = \Delta$ où Δ est le discriminant de l'équation de Weierstrass qui définit E.

N.B. Dans [13], les notations P et Q n'apparaissent pas : on part des abscisses e_i des points d'ordre 2. L'inconvénient de la présentation adoptée ici est qu'elle est moins symétrique, et qu'elle dépend du choix d'une base. Son avantage est que tout est décrit en fonction des points P et Q, donc si on sait comment un élément donné de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ agit sur P et Q, alors on en déduira facilement comment il agit sur tous les objets que l'on va construire.

Si M désigne un point de E, on note (x_M, y_M) ses coordonnées. La forme de l'équation de Weierstrass montre qu'on a :

$$x_{-M} = x_M \text{ et } y_{-M} = -y_M$$

Si $M_i = (x_i, y_i)$ sont trois points de la courbe (pour $1 \leq i \leq 3$) tels que $M_1 + M_2 + M_3 = 0$ et $M_1 \neq \pm M_2$ alors la formule d'addition s'écrit :

$$x_1 + x_2 + x_3 = (\frac{y_1 - y_2}{x_1 - x_2})^2$$

Dans ce cas, on a aussi :

$$\frac{y_1 - y_2}{x_1 - x_2} = \frac{y_2 - y_3}{x_2 - x_3} = \frac{y_3 - y_1}{x_3 - x_1}$$

De plus, on a pour tout point M tel que $2M \neq 0$:

$$x_{2M} = \frac{x_M^4 - 2ax_M^2 - 8bx_M + a^2}{4y_M^2} = \frac{x_M^4 - 2ax_M^2 - 8bx_M + a^2}{4x_M^3 + 4ax_M + 4b}$$

On a le lemme suivant :

Lemme 14 *Soit A un point d'ordre 4 et B un point d'ordre 2 différent de $2A$. Alors :*

$$2x_{2A} - x_A = x_{A+B}$$

DÉMONSTRATION : Les points M tels que $2M = 2A$ sont exactement ceux tels que $x_{2M} = x_{2A}$, car $2A$ est le seul point de la courbe d'abscisse x_{2A}. Ce sont donc les points M dont l'abscisse vérifie l'équation polynômiale $x_M^4 - 2ax_M^2 - 8bx_M + a^2 = x_{2A}(4x_M^3 + 4ax_M + 4b)$. Or ces points M sont exactement A, $-A$, $A + B$ et $-A + B$. La formule donnant la somme des racines d'un polynôme s'écrit donc : $x_A + x_{-A} + x_{A+B} + x_{-A+B} = 4x_{2A}$. Or dans le membre de gauche, les deux premiers termes sont égaux, ainsi que le deux derniers. On en déduit le lemme.

On adopte les notations suivantes :

$$\begin{array}{ccc} u_1 = x_P - x_{2P} & u_2 = x_Q - x_{2Q} & u_3 = x_{P+Q} - x_{2P+2Q} \\ v_1 = y_P & v_2 = y_Q & v_3 = y_{-P-Q} \\ v_1' = y_{-P+2Q} & v_2' = y_{2P+Q} & v_3' = y_{-P+Q} \end{array}$$

Grâce au lemme, on a les égalités suivantes :

$$\begin{array}{rcccccl} e_1 - u_1 & = & 2x_{2P} - x_P & = & x_{P+2Q} & = & x_{-P+2Q} \\ e_2 - u_2 & = & 2x_{2Q} - x_Q & = & x_{2P+Q} & & \\ e_3 - u_3 & = & 2x_{2(P+Q)} - x_{P+Q} & = & x_{-P+Q} & & \end{array}$$

Ces égalités s'écrivent :

$$-P + 2Q = (e_1 - u_1, v_1') \quad 2P + Q = (e_2 - u_2, v_2') \quad -P + Q = (e_3 - u_3, v_3')$$

De plus, de la définition des e_i et des u_i découlent immédiatement les relations suivantes (où il convient de noter le signe moins qui apparaît devant v_3) :

$$P = (e_1 + u_1, v_1) \quad Q = (e_2 + u_2, v_2) \quad P + Q = (e_3 + u_3, -v_3)$$

Malgré les apparences, ces notations sont tout à fait symétriques; on a en particulier la relation suivante, vraie pour $i \in \{1, 2, 3\}$ à condition de poser $e_4 = e_1$ et de considérer que l'addition utilisée est celle de E :

$$(e_i + u_i, v_i) + (e_{i+1}, 0) + (e_i - u_i, v_i') = 0$$

Appliquons à cette relation la formule d'addition; on obtient :

$$e_i - e_{i-1} = 2e_i + e_{i+1} = (\frac{v_i - v_i'}{2u_i})^2$$

On pose donc

$$w_i = \frac{v_i - v_i'}{2u_i}$$

et

$$W = w_1 w_2 w_3$$

Ainsi, on a $4W^2 = -\delta$ d'où :

$$(2W)^4 = \Delta$$

On a donc construit explicitement, en fonction des coordonnées des points de 4-torsion, une racine quatrième du discriminant Δ de E. Cette construction est résumée dans le résultat suivant :

Théorème 16 *Soit E une courbe elliptique donnée par une équation de Weierstrass de la forme $y^2 = x^3 + ax + b$. Soit (P, Q) une base du $\mathbb{Z}/4\mathbb{Z}$-module E_4. Alors*

$$W' = \frac{(y_P - y_{-P+2Q})(y_Q - y_{2P+Q})(-y_{P+Q} - y_{-P+Q})}{4(x_P - x_{2P})(x_Q - x_{2Q})(x_{P+Q} - x_{2P+2Q})}$$

est une racine quatrième du discriminant de cette équation de Weierstrass.

Ce théorème permet de décrire le corps des points de 4-torsion de E en fonction (entre autres) des racines quatrièmes de Δ. C'est l'objet du paragraphe suivant.

8.2.2 Description du corps des points de 4-torsion d'une courbe elliptique

Soit E une courbe elliptique sur $\mathbb{Q}$; elle admet une équation de Weierstrass minimale de la forme $y^2 = x^3 + ax + b$ avec $a, b \in \mathbb{Q}$, donc les résultats du paragraphe précédent s'appliquent.

On appelle *corps des points de 4-torsion de E*, et on note $\mathbb{Q}(E_4)$, le plus petit corps de nombres contenant les coordonnées de tous les points de 4-torsion de $E(\bar{\mathbb{Q}})$. De plus, on note Δ le discriminant de E.

Démontrons le résultat suivant :

Théorème 17 *Soient E une courbe elliptique sur $\mathbb{Q}$ et P un point de $E(\bar{\mathbb{Q}})$ d'ordre 4 exactement. Alors :*

$$\mathbb{Q}(E_4) = \mathbb{Q}(x_P, y_P, \sqrt{-1}, \Delta^{\frac{1}{4}})$$

DÉMONSTRATION : Montrons tout d'abord que x_P, y_P, $i = \sqrt{-1}$ et $\Delta^{\frac{1}{4}}$ appartiennent bien à $\mathbb{Q}(E_4)$. Pour les deux premiers, c'est évident. Pour i, c'est une conséquence des propriétés de l'accouplement de Weil (voir [28], Chapitre III, Corollaire 8.1.1., page 98); on peut aussi le démontrer directement en construisant une racine carrée de -1 à l'aide des notations introduites au paragraphe précédent : voir [13], page 219. Enfin, le fait que $\Delta^{\frac{1}{4}}$ appartienne à $\mathbb{Q}(E_4)$ n'est pas ambigu (i.e. ne dépend pas de la racine quatrième choisie) car $i \in \mathbb{Q}(E_4)$, et résulte du théorème 16.

Montrons maintenant l'inclusion réciproque. Cela revient à montrer que tout automorphisme $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ qui fixe x_P, y_P, i et $\Delta^{\frac{1}{4}}$ fixe aussi les autres points de 4-torsion. Soit donc σ un tel automorphisme. Notons Q un point de 4-torsion tel que (P, Q) constitue une base de E_4. Comme σ fixe P, il suffit de montrer qu'il fixe aussi Q pour montrer qu'il fixe tous les points de 4-torsion. Raisonnons par l'absurde, en supposant que $\sigma(Q) \neq Q$. Or dans la base (P, Q), la matrice de $\rho_4(\sigma)$ est $\begin{bmatrix} 1 & k \\ 0 & \chi(\sigma) \end{bmatrix}$ où χ est le caractère cyclotomique donnant l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur les racines quatrièmes de l'unité (voir [22], 1.11) et k est un élément non nul de $\mathbb{Z}/4\mathbb{Z}$. Comme σ fixe i, on a $\chi(\sigma) = 1$. En composant σ avec lui-même un nombre convenable de fois (une ou deux selon la valeur de k), on construit un élément $\tau \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ qui fixe x_P, y_P, i et $\Delta^{\frac{1}{4}}$ et qui est tel que la matrice de $\rho_4(\tau)$ dans la base (P, Q) soit $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$. L'élément W' défini dans le théorème 16

est une racine quatrième de Δ; il s'écrit comme le produit de $\Delta^{\frac{1}{4}}$ par une certaine puissance de i. Donc τ le laisse fixe. Mais cela contredit le calcul direct de $\tau(W')$ qu'on effectue à partir de la formule explicite donnant W' en fonction des coordonnées des points de 4-torsion, et de la matrice de $\rho_4(\tau)$ (qui décrit comment τ permute les points de 4-torsion). En effet, ce calcul s'écrit :

$$\tau(W') = \frac{(y_P - y_{-P+2Q})(y_{2P+Q} - y_Q)(-y_{-P+Q} - y_{P+Q})}{4(x_P - x_{2P})(x_{2P+Q} - x_{2Q})(x_{-P+Q} - x_{2P+2Q})}$$

On remarque que le numérateur est l'opposé de celui de W'. En ce qui concerne le dénominateur, le facteur 4 et le premier terme sont les mêmes que pour W'. Le deuxième terme $x_{2P+Q} - x_{2Q}$ s'écrit aussi $x_{2Q} - x_Q$ d'après le lemme 14 appliqué avec $A = Q$ et $B = 2P$. Ce terme est donc l'opposé du deuxième terme du dénominateur de W'. Enfin, le troisième terme $x_{-P+Q} - x_{2P+2Q}$ qui apparaît au dénominateur de $\tau(W')$ s'écrit $x_{2P+2Q} - x_{P+Q}$, d'après le même lemme appliqué avec $A = P + Q$ et $B = -2P$. Encore une fois, c'est l'opposé du terme qui apparaît au même emplacement dans la formule de W'. Finalement, on a donc :

$$\tau(W') = -W'$$

Comme W' est non nul, cela contredit le fait que τ fixe W'. De cette contradiction résulte le théorème 17.

8.2.3 Application à la surjectivité de $\rho_4^{(E)}$

On sait que $\rho_4^{(E)}$ est surjective si, et seulement si, le degré de $\mathbb{Q}(E_4)$ sur $\mathbb{Q}$ est égal au cardinal de $GL_2(\mathbb{Z}/4\mathbb{Z})$, qui vaut 96. Or le théorème 17 donne une description de $\mathbb{Q}(E_4)$ qu'on peut exploiter pour calculer son degré.

Tout d'abord, il est clair qu'on a : $[\mathbb{Q}(i, \Delta^{\frac{1}{4}}) : \mathbb{Q}] \leq 8$; de plus, on montre facilement qu'il y a égalité si, et seulement si, Δ n'est ni un carré, ni l'opposé d'un carré (dans $\mathbb{Q}$).

Ensuite, on se donne $P \in E(\bar{\mathbb{Q}})$ d'ordre 4 et on teste informatiquement si $[\mathbb{Q}(x_P, y_P) : \mathbb{Q}]$ vaut 12, et si les extensions $\mathbb{Q}(i, \Delta^{\frac{1}{4}})/\mathbb{Q}$ et $\mathbb{Q}(x_P, y_P)/\mathbb{Q}$ sont linéairement disjointes. Si ces deux tests s'avèrent positifs, et si Δ n'est ni un carré ni l'opposé d'un carré dans $\mathbb{Q}$, alors $\rho_4^{(E)}$ est surjective.

Si l'un des deux tests s'avère négatif, ou bien si Δ est un carré ou l'opposé d'un carré dans $\mathbb{Q}$, alors $[\mathbb{Q}(E_4) : \mathbb{Q}] < 96$, donc $\rho_4^{(E)}$ n'est pas surjective.

On a donc ramené le calcul du degré de $\mathbb{Q}(E_4)$ sur $\mathbb{Q}$ à des calculs réalisables sur ordinateur. Dans chaque cas particulier, on peut donc démontrer si $\rho_4^{(E)}$ est surjective, ou si elle ne l'est pas.

Toutefois, il semble difficile d'adapter la méthode utilisée ici pour tester la surjectivité de $\rho_8^{(E)}$, car en général $\Delta^{\frac{1}{8}}$ n'appartient pas à $\mathbb{Q}(E_8)$.

Une manière complètement différente de montrer que deux courbes elliptiques ont des représentations isomorphes dans les points de 4-torsion est donnée au paragraphe suivant; elle n'utilise pas le résultat de Mazur vu au paragraphe 8.1.

8.3 Utilisation de l'article de Silverberg

Dans [27], on trouve l'énoncé suivant :

Proposition 26 *Soit E une courbe elliptique d'équation $y^2 = x^3 + ax + b$ avec $a, b \in \mathbb{Q}$. Pour $t \in \mathbb{Q}$, notons $\mathcal{E}_t$ la courbe (éventuellement singulière) d'équation $y^2 = x^3 + a(t)x + b(t)$, où les expressions de $a(t)$ et $b(t)$ sont données ci-dessous. Alors, pour tout $t \in \mathbb{Q}$ tel que $\mathcal{E}_t$ soit non singulière, les $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules E_4 et $\mathcal{E}_{t_4}$ sont isomorphes.*

En posant $J = j_E/1728$, les formules donnant $a(t)$ et $b(t)$ sont les suivantes :

$$\begin{aligned} a(t) \quad = a \cdot (\quad & (J-1)^4(144J^2 - 56J - 7)t^8 \\ & -48(J-1)^4(4J+1)t^7 \\ & +28(J-1)^3(4J+5)t^6 \\ & +224(J-1)^3t^5 \\ & +42(J-1)^2(4J-5)t^4 \\ & -112(J-1)^2t^3 \\ & +28(J-1)t^2 + 1) \end{aligned}$$

$$\begin{aligned} b(t) \quad = b \cdot (\quad & (J-1)^6(1728J^3 - 144J^2 + 116J + 1)t^{12} \\ & -12(J-1)^5(288J^3 - 128J^2 + 82J + 1)t^{11} \\ & +66(J-1)^5(48J^2 - 56J - 1)t^{10} \\ & -44(J-1)^4(208J^2 - 176J - 5)t^9 \\ & -99(J-1)^4(48J^2 - 104J - 5)t^8 \\ & +792(J-1)^3(8J^2 - 10J - 1)t^7 \\ & -924(J-1)^3(4J+1)t^6 \\ & +792(J-1)^2t^5 \\ & -99(J-1)^2(4J-5)t^4 \\ & +44(J-1)(6J-5)t^3 \\ & -66(J-1)t^2 \\ & +12t + 1) \end{aligned}$$

N.B. Même si cela n'est pas formulé explicitement dans [27], un intérêt majeur de cette proposition est le fait que (si $a \neq 0$ et $b \neq 0$) toutes les courbes E' ayant même représentation que E dans les points de 4-torsion sont obtenues, c'est-à-dire s'écrivent (à isomorphisme près) sous la forme $\mathcal{E}_t$ pour un certain $t \in \mathbb{Q}$.

Etant donné un couple (E, E') de courbes elliptiques, cette proposition permet de dire si $\rho_4^{(E)}$ et $\rho_4^{(E')}$ sont isomorphes. En effet, on écrit une équation de E sous la forme $y^2 = x^3 + ax + b$ avec $a, b \in \mathbb{Q}$ (ce qui est toujours possible puisque E est définie sur $\mathbb{Q}$), puis il suffit d'exhiber un rationnel t tel que E' soit isomorphe (sur $\mathbb{Q}$) à la courbe $\mathcal{E}_t$. Pour trouver un tel rationnel, on résout l'équation $j_{\mathcal{E}_t} = j_{E'}$, puis on vérifie que l'isomorphisme entre E' et $\mathcal{E}_t$ est défini sur $\mathbb{Q}$.

Par exemple, soient les courbes elliptiques définies par les équations suivantes :

$$\begin{aligned} (E) \quad y^2 + y = \quad & x^3 - x^2 - 19x + 39 \\ (E') \quad y^2 + y = \quad & x^3 + x^2 + 1815x + 141239 \end{aligned}$$

La méthode décrite ci-dessus permet de trouver la valeur $t = 129/17735$, qui permet de vérifier que $\rho_4^{(E)}$ et $\rho_4^{(E')}$ sont isomorphes.

Ce couple de courbes elliptiques a été trouvé par la recherche exhaustive exposée au paragraphe 7.3.1, avec $p = 8$. Une autre méthode pour trouver des couples dont on peut raisonnablement espérer qu'ils aient même représentation dans les points de 8-torsion (même si, ici, on ne peut le vérifier qu'en admettant la surjectivité de $\rho_8^{(E)}$) est donnée par l'article de Darmon et Granville; c'est l'objet du paragraphe suivant.

8.4 Darmon et Granville pour $p = 8$

On peut appliquer avec $p = 8$ la méthode utilisée au paragraphe 7.3.2 pour $p = 7$. Cette fois, il s'agit de considérer l'équation diophantienne $a^2 + b^3 = \pm c^8$ (le signe $\pm$ était inutile quand l'exposant p était impair; ici il devient essentiel pour ne pas perdre la deuxième solution ci-dessous). Elle admet les solutions suivantes (citées dans [5], page 515) :

$$30042907^2 - 96222^3 = 43^8$$

$$1549034^2 - 15613^3 = -33^8$$

En ce qui concerne l'équation $a^2 + b^3 = -c^8$, la solution donnée ici est la seule non triviale d'après [3].

De même qu'au paragraphe 7.3.2, on considère les courbes de Frey associées, données par l'équation $y^2 = x^3 + 3bx + 2a$. Ici, ces équations sont respectivement :

$$y^2 = x^3 - 288666x + 60085814 \quad (26)$$

$$y^2 = x^3 - 46839x + 3098068 \quad (27)$$

Pour la courbe (26), de conducteur 74304, de discriminant $-2^6 3^3 43^8$, on est amené à chercher une courbe E de conducteur $74304/43 = 1728$. Parmi les courbes (listées dans les tables de [4]) de conducteur 1728, celle notée $1728i1$ dans [4] convient; elle admet l'équation de Weierstrass suivante :

$$y^2 = x^3 + 54x + 54$$

Quant à la courbe (27), de conducteur 6336, son discriminant est $2^6 3^{11} 11^8$ donc on cherche une courbe E de conducteur $576 = 6336/11$. On trouve les deux courbes suivantes, qui sont tordues l'une de l'autre par i et ont même représentation dans les points de 8-torsion entre elles et avec la courbe (27) :

$y^2 = x^3 - 39x - 92$	notée $576B1$ dans les tables de [4]
$y^2 = x^3 - 39x + 92$	notée $576C1$ dans les tables de [4]

Comme pour $p = 7$, à chaque solution (non triviale) de l'équation diophantienne on a réussi à associer un couple (E, E') de courbes elliptiques (et même un triplet pour l'une des deux solutions). Toutefois, on n'a réussi à démontrer l'isomorphisme de $\rho_8^{(E)}$ et $\rho_8^{(E')}$ qu'en admettant la surjectivité de $\rho_8^{(E)}$.

Conclusion

On a donc vu quelques-unes des très nombreuses applications de la conjecture *abc*. Au vu de la puissance de cette conjecture, il est tentant de chercher un analogue de *abc* dans d'autres contextes. On pense naturellement à remplacer $\mathbb{Z}$ par l'anneau des polynômes à une variable sur un corps, par exemple sur $\mathbb{C}$. Si on traduit ainsi l'énoncé de la conjecture *abc*, on obtient le théorème de Mason (qui est vrai aussi pour $\varepsilon = 0$, alors qu'il faut supposer $\varepsilon > 0$ dans la conjecture *abc*).

On peut aussi traduire l'énoncé du "théorème" 13, dont on a vu qu'il est équivalent à la conjecture *abc*. On obtient alors la conjecture suivante, due à J. Oesterlé :

Conjecture 4 *Soit $P(T, X, Y)$ un polynôme à coefficients complexes, à trois indéterminées T, X et Y. Supposons que P, vu comme polynôme en X et Y à coefficients dans $\mathbb{C}[T]$, soit homogène de degré d et sans facteur multiple.*

Alors il existe une constante c, ne dépendant que de P, telle que, pour tous polynômes $A, B \in \mathbb{C}[T]$ premiers entre eux, on ait :

$$\varrho(P(T, A(T), B(T))) > (d-2)\max(d(A), d(B)) - c$$

En appliquant cette conjecture au polynôme $P(T, X, Y) = XY(X+Y)$, on retrouve le théorème de Mason.

On ne peut pas traduire la démonstration du théorème 13 à partir de la conjecture *abc* pour obtenir une démonstration de la conjecture 4 à partir du théorème de Mason; en effet, le théorème de Belyi, donc le théorème 9, ne se généralisent pas de $\mathbb{Z}$ à $\mathbb{C}[T]$.

Références

[1] G.V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izv. 14 (1980), 247-256.

[2] B.J. Birch, W. Kuyk, *Modular functions of one variable IV*, Lecture Notes 476, Springer-Verlag, 1975.

[3] N. Bruin, *The diophantine equations* $x^2 \pm y^4 = \pm z^6$ *and* $x^2 + y^8 = z^3$, preprint, Math. Institute Univ. of Leiden (1997).

[4] J.E. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, 1992.

[5] H. Darmon, A. Granville, *On the equations* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27 (1995), 513-543.

[6] N. Elkies, *(abc) implies Mordell*, Intern. Math. Research Notices 7 (1991), 99-109.

[7] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, in *Arithmetic geometry*, G. Cornell & J.H. Silverman eds., Springer-Verlag, 1986.

[8] R. Fricke, *Lehrbuch der Algebra, 3. Band: algebraische zahlen*, Vieweg, 1928.

[9] A. Kraus, *Sur les modules galoisiens des points de torsion des courbes elliptiques*, non publié.

[10] A. Kraus, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique*, Dissertationes Mathematicae CCCLXIV (1997).

[11] A. Kraus, J. Oesterlé, *Sur une question de B. Mazur*, Math. Annalen 293 (1992), 259-275.

[12] S. Lang, *Algebra*, 3ème édition, Addison-Wesley, 1993.

[13] S. Lang, H. Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes 504, Springer-Verlag, 1976.

[14] M. Langevin, *Cas d'égalité pour le théorème de Mason et applications de la conjecture (abc)*, Comptes Rendus de l'Académie des Sciences, Série I, 317 (1993), 441-444.

[15] M. Langevin, *Partie dans facteur carré de* $F(a,b)$ *modulo la conjecture (abc)*, Séminaire de Théorie des Nombres de l'Université de Caen, 1994.

[16] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129-162.

[17] B. Mazur, *Deformation theory of Galois representations*, in *Modular forms and Fermat's last theorem*, G. Cornell, J.H. Silverman & G. Stevens eds., Springer-Verlag, 1997.

[18] B. Mazur, H.P.F. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. 25 (1974), 1-61.

[19] A. Nitaj, *La conjecture (abc)*, L'Enseignement Math. 42 (1996), 3-24.

[20] J. Oesterlé, *Nouvelles approches du "théorème de Fermat"*, Séminaire Bourbaki 694 (Février 1988).

[21] E. Rees, C.J. Smyth, *On the constant in the Tarry-Escott problem*, in *Cinquante ans de polynômes*, M. Langevin & M. Waldschmidt eds., Lecture Notes 1415, Springer-Verlag, 1990, 196-208.

[22] J.P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259-331.

[23] J.P. Serre, *Points rationnels des courbes modulaires* $X_0(N)$, Séminaire Bourbaki 511 (Novembre 1977).

[24] J.P. Serre, *Sur les représentations modulaires de degré 2 de* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math. Journal 54 (1987), 179-230.

[25] J.P. Serre, *Lectures on the Morwell-Weil theorem*, M. Brown trad., Aspects of Math. E015, Vieweg, 1990.

[26] J.P. Serre, *Travaux de Wiles (et Taylor,...), Partie I*, Séminaire Bourbaki 803 (Juin 1995).

[27] A. Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, non publié.

[28] J.H. Silverman, *The Arithmetic of elliptic curves*, G.T.M. 106, Springer-Verlag, 1986.

[29] C.L. Stewart, K. Yu, *On the (abc) conjecture*, Math. Annalen 291 (1991), 225-230.

[30] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141 (1995), 443-551.