FAMILLES DE POLYNÔMES LIÉES AUX COURBES MODULAIRES $X_1(l)$ UNICURSALES ET POINTS RATIONNELS NON-TRIVIAUX DE COURBES ELLIPTIQUES QUOTIENT

par

Franck Leprévost, Michael Pohst & Andreas Schöpp

Résumé. — Soit l un entier et $E_{c,l}$ la famille de Kubert des courbes elliptiques définies sur $\mathbf{Q}$ munies d'un point rationnel A d'ordre l. On note $F_{c,l}$ la courbe elliptique quotient de $E_{c,l}$ par le groupe engendré par A, et φ_l l'isogénie de $E_{c,l}$ sur $F_{c,l}$. Pour $l = 3, 4, 5$ et 6, nous construisons explicitement, pour des paramétrisations convenables de c, des éléments non-triviaux de $F_{c,l}(\mathbf{Q})/\varphi_l(E_{c,l}(\mathbf{Q}))$, autrement dit, des points explicites de $F_{c,l}(\mathbf{Q})$ qui ne sont l'image par φ_l d'aucun élément de $E_{c,l}(\mathbf{Q})$. Ces points sont en général d'ordre infini. Nous donnons des applications de cette méthode à la construction d'extensions cycliques de $\mathbf{Q}$ de degré l, et retrouvons certains corps obtenus par Shanks et Gras. Dans un article ultérieur, nous étudierons les propriétés arithmétiques de certaines des extensions obtenues ici.

1. Introduction

L'étude du rang des courbes elliptiques définies sur $\mathbf{Q}$ et $\mathbf{Q}(t)$ a connu ces dernières années de nombreux progrès, initiés par les travaux de Mestre. En fait, il est (verbalement) conjecturé l'existence de courbes elliptiques sur $\mathbf{Q}$ de grand rang et de groupe de torsion rationnel arbitraire parmi la liste des quinze groupes possibles, à savoir $\mathbf{Z}/l\mathbf{Z}$ pour $1 \leq l \leq 10$ ou $l = 12$, ou bien $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2l\mathbf{Z}$ pour $1 \leq l \leq 4$. Dans plusieurs travaux ([**8**], [**13**], [**14**], [**21**]), l'on construit des courbes elliptiques de rang élevé ayant un groupe de torsion non-réduit à l'élément neutre.

Mots clefs. — Courbes modulaires, extensions diédrales, extensions cycliques, unités
2000 Mathematics Subject Classification : 11 Y 40, 11 R 21, 14 H 52, 11 G 05
Article submitted to Acta Arithmetica.

Considérons ici $3 \leq l \leq 10$ ou $l = 12$, et soit $E_{c,l}$ la famille de Kubert ([**17**]) des courbes elliptiques définies sur $\mathbf{Q}$ munies d'un point rationnel A d'ordre l (dans le cas $l = 3$, c désigne en réalité un couple de paramètres). En d'autres termes, $(E_{c,l}, A)$ paramétrise les points rationnels sur $\mathbf{Q}$ de la courbe modulaire $X_1(l)$, qui est isomorphe à $\mathbf{P}^1$ pour ces valeurs de l (elle est encore unicursale pour $l = 1, 2$, valeurs qui n'ont guère d'intérêt dans le cadre qui nous occupe). Avec ces notations, les travaux cités plus haut exhibent, via des paramétrisations ingénieuses de c, des familles explicites de courbes du type $E_{c,l}$ de $\mathbf{Q}$-rang différent de 0. Les méthodes employées exploitent essentiellement le fait que le paramètre c intervient avec un degré relativement *petit* dans des équations bien choisies de $E_{c,l}$.

Si $< A >$ désigne le groupe engendré par A, notons $F_{c,l}$ la courbe elliptique quotient $E_{c,l}/ < A >$, et φ_l l'isogénie de $E_{c,l}$ sur $F_{c,l}$. On a ainsi la suite exacte suivante de $G_{\mathbf{Q}}$-modules galoisiens (où $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$) :

$$1 \longrightarrow \mathbf{Z}/l\mathbf{Z} \simeq < A > \longrightarrow E_{c,l}(\overline{\mathbf{Q}}) \xrightarrow{\varphi_l} F_{c,l}(\overline{\mathbf{Q}}) \longrightarrow 1.$$

Connaissant une équation de $E_{c,l}$ et les coordonnées de A, les formules de Vélu ([**29**]) permettent d'obtenir explicitement une équation de $F_{c,l}$ et de φ_l.

Bien évidemment, l'image par φ_l de points de $E_{c,l}(\mathbf{Q})$ fournit des points de $F_{c,l}(\mathbf{Q})$, que nous appelons ici des points rationnels triviaux de la courbe elliptique quotient $F_{c,l}$.

Le problème, auquel nous nous intéressons dans la partie 2, consiste en la construction, via des paramétrisations convenables ou des spécialisations de c, d'éléments non-triviaux de $F_{c,l}(\mathbf{Q})/\varphi_l(E_{c,l}(\mathbf{Q}))$, autrement dit, de points explicites de $F_{c,l}(\mathbf{Q})$ qui ne sont l'image par φ_l d'aucun élément de $E_{c,l}(\mathbf{Q})$. En général les représentants de ces points dans $F_{c,l}(\mathbf{Q})$ sont d'ordre infini. Ceci dit, et bien que les courbes elliptiques $E_{c,l}(\mathbf{Q})$ et $F_{c,l}(\mathbf{Q})$ aient même rang, nous n'utilisons pas les constructions de [**8**], [**13**], [**14**], [**21**] qui ne fourniraient, dans notre terminologie, que des points triviaux de $F_{c,l}(\mathbf{Q})$, comme remarqué plus haut. Le problème traité ici devient rapidement délicat (au regard de l), puisque le degré du paramètre c dans les équations de $F_{c,l}$ est, comme nous le verrons en particulier dans les cas considérés, notablement plus élevé que dans les équations de $E_{c,l}$. Dans la partie 3, nous construisons, à partir de la donnée $(E_{c,l}, A)$, un polynôme $P_{n,c,l} \in \mathbf{Z}[n, c][x]$, pour lequel nous montrons que son corps de décomposition sur $\mathbf{Q}(n, c)$ est génériquement le groupe diédral D_l à $2l$ éléments. Dans la partie 4, nous considérons plus spécifiquement le cas $l = 5$, et montrons que notre construction permet de retrouver la famille générique de Brumer, qui est isomorphe à celle obtenue, indépendamment, par Darmon (voir les références données dans cette partie). Il est tentant de regarder sous quelles conditions sur les paramètres (n, c) le groupe de Galois de $P_{n,c,l}$ sur $\mathbf{Q}(n, c)$ devient isomorphe au groupe $\mathbf{Z}/l\mathbf{Z}$. Dans la partie 5, nous montrons que ces conditions reviennent à la construction d'éléments non-triviaux de $F_{c,l}(\mathbf{Q})/\varphi_l(E_{c,l}(\mathbf{Q}))$. Les résultats de la partie 2 permettent alors de construire explicitement de telles extensions cycliques. Nous retrouvons également les *simplest cubic fields* de Shanks et les *simplest quartic fields* de M.-N. Gras. Dans [**22**], nous étudierons des propriétés arithmétiques d'extensions construites ici.

Les calculs effectués pour cet article ont nécessité un usage très important des logiciels de calcul formel KANT ([**5**]), MAGMA ([**2**]), MAPLE ([**23**]) et PARI ([**1**]).

2. Points non-triviaux de courbes elliptiques quotient

Nous montrons ici le résultat suivant :

Théorème 1. — *Pour* $l = 3, 4, 5$ *et* 6*, nous construisons explicitement, pour des paramétrisations convenables de* c*, des éléments non-triviaux de* $F_{c,l}(\mathbf{Q})/\varphi_l(E_{c,l}(\mathbf{Q}))$*. Ces points sont en général d'ordre infini.*

Par un argument de cohomologie galoisienne classique, comme $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ opère trivialement sur $< A >$, on établit aisément le :

Corollaire 1. — *Pour* $l = 3, 4, 5$ *et* 6*, et pour les paramétrisations de* c *du théorème précédent, le groupe de cohomologie* $\mathrm{H}^1(G_{\mathbf{Q}}, \mathbf{Z}/l\mathbf{Z}) = \mathrm{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/l\mathbf{Z})$ *est non réduit à* 0.

Bien entendu, la suite exacte longue en cohomologie se poursuivant, nous obtenons de la sorte plus précisément des éléments non-triviaux du noyau de l'application

$$\mathrm{H}^1(G_{\mathbf{Q}}, \mathbf{Z}/l\mathbf{Z}) = \mathrm{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/l\mathbf{Z}) \longrightarrow \mathrm{H}^1(G_{\mathbf{Q}}, E_{c,l}(\overline{\mathbf{Q}})).$$

2.1. Les cas $l = 3$ et $l = 5$. — Etant donné que notre stratégie est suffisament générale, nous la développons pour $l \geq 5$ impair, la détaillons sur le cas $l = 5$, et serons plus succints pour le cas $l = 3$. Nous indiquons dans une remarque les limites de notre approche. La différence de traitement du cas $l = 3$ correspond essentiellement au fait que la famille des courbes elliptiques définies sur $\mathbf{Q}$ munies d'un point d'ordre 3 est paramétrisée par deux paramètres, et non pas un, ce qui alourdit quelque peu les notations.

Soit donc $l \geq 5$ impair. Les formules de Vélu permettent d'obtenir une équation de $F_{c,l}$ de la forme :

$$y^2 = f_{c,l}(x) = 4x^3 + \alpha_l(c)x^2 + \beta_l(c)x + \gamma_l(c),$$

où α_l, β_l et γ_l sont les éléments de $\mathbf{Z}[c]$ donnés dans le tableau suivant pour $l = 5$:

$\alpha_5(c)$	$c^2 - 30c + 1$
$\beta_5(c)$	$-2c(3c+1)(4c-7)$
$\gamma_5(c)$	$-c(4c^4 - 4c^3 - 40c^2 + 91c - 4)$

On cherche alors $x_{c,l}$ sous la forme d'un polynôme en c, de petit degré, de sorte que l'on ait une identité :

$$f_{c,l}(x_{c,l}) = A_l(c)G_l^2(c),$$

où A_l, G_l sont des polynômes en c tels que le degré de A_l en c soit égal à 1 ou à 2. Pour réaliser cela, on calcule le discriminant par rapport à c de $f_{c,l}(x_{c,l})$, qui est un polynôme en les coefficients de c de $x_{c,l}$. Il s'agit alors de l'annuler. De tels $x_{c,l}$, et les $G_l(c)$ et $A_l(c)$ associés, sont donnés dans le tableau suivant pour $l = 5$:

$x_{c,5}$	$-(u_0+1)c^2 + (11u_0+8)c + u_0$
$G_5(c)$	$c^2 - 11c - 1$
$A_5(c)$	$-(4u_0+3)(u_0+1)^2c^2 + 2(2u_0+1)(11u_0^2 + 11u_0 + 2)c + u_0^2(4u_0+1)$

Il reste alors à paramétriser, à l'aide d'un choix approprié des paramètres restants la conique en (c, z) d'équation :

$$A_l(c) = z^2.$$

<u>Cas $l = 5$</u> : Comme nous l'avons souligné plus haut, le degré en c de $A_5(c)$ est ≤ 2. Par conséquent, plusieurs cas se présentent, selon que l'on choisisse le degré en c de $A_5(c)$ égal à 1 ou à 2, et qui peuvent simplifier les calculs. Le tableau suivant résume les choix et calculs effectués. Les deux premières lignes correspondent à l'annulation du coefficient de degré 2 en c de $A_5(c)$, et la troisième assure que le point de coordonnées $(c, z) = (0, u_0 t)$ appartient à la conique d'équation $A_5(c) = z^2$.

$u_0 = -1$	$c = \frac{z^2-3}{4}$	$x_{c,5} = \frac{5-3z^2}{4}$
$u_0 = -\frac{3}{4}$	$c = 16z^2 + 18$	$x_{c,5} = -64z^4 - 148z^2 - \frac{345}{4}$
$u_0 = \frac{t^2-1}{4}$	$c = \frac{11t^6+33t^4-8mt^3+21t^2+8mt-1}{t^6+8t^4+21t^2+16m^2+18}$	$x_{c,5} = -\frac{t^2+3}{4}c^2 + \frac{11t^2+21}{4}c + \frac{t^2-1}{4}$

Il découle de ce qui précède que, pour ces choix des paramètres, la courbe elliptique quotient $F_{c,l}(\mathbf{Q})$ possède le point de coordonnées $(x_{c,l}, zG_l(c))$. Le calcul montre que le point ainsi construit est génériquement d'ordre infini. Le calcul montre également que ce point n'est génériquement pas l'image par l'isogénie φ_l d'un point rationnel de $E_{c,l}$. Cette dernière question sera considérée de nouveau dans la partie 5.

<u>Cas $l = 3$</u> : Les formules de Vélu permettent d'obtenir une équation de $F_{a_1,a_3,l}$ de la forme :

$$y^2 = f_{a_1,a_3,3}(x) = 4x^3 + a_1^2 x^2 - 18a_1a_3x - a_3(4a_1^3 + 27a_3).$$

Si l'on choisit $x_{a_1,a_3,3} = u_1a_3 + \frac{a_1u_1+1}{u_1^2}$, le calcul montre que

$$f_{a_1,a_3,3}(x_{a_1,a_3,3}) = A_3(a_1,a_3)G_3^2(a_1,a_3),$$

où $A_3(a_1,a_3) = 4u_1^3a_3 + (u_1a_1+1)^2$ et $G_3(a_1,a_3) = \frac{u_1^3a_3-u_1a_1-2}{u_1^3}$. L'équation $A_l(c) = z^2$ est linéaire en a_3, et il suffit de prendre $a_3 = \frac{z^2-(u_1a_1+1)^2}{4u_1^3}$. On obtient alors $x_{a_1,a_3,3} = \frac{z^2-(a_1u_1+1)(a_1u_1-3)}{4u_1^2}$, et l'on conclut comme dans le cas $l = 5$.

Remarque : Pour les autres valeurs impaires de l, la méthode décrite ici trouve ses limites essentiellement dans le calcul du discriminant de $f_{c,l}(x_{c,l})$ par rapport à c. Les logiciels de calcul formel ne permettent pas de factoriser en toute généralité cette quantité. Cependant, on constate que celle-ci s'exprime comme un produit d'un *gros* facteur par un *petit* facteur, ce dernier intervenant à la puissance l. On peut, par spécialisation et interpolation, calculer explicitement ce petit facteur, du moins l'avons nous fait pour $l = 7$. Nous ne sommes en revanche malheureusement pas parvenus à l'annuler de manière utile dans le cadre que nous considérons ici.

2.2. Les cas $l = 4$ et $l = 6$. — Dans le cas où l est pair, l'approche est légèrement différente. Cependant, là également, nous la décrivons pour $l \geq 6$ pair, la détaillons sur le cas $l = 6$, et serons plus succints pour le cas $l = 4$.

Les formules de Vélu permettent de nouveau d'obtenir une équation de $F_{c,l}$, qui est de la forme :

$$y^2 = f_{c,l}(x) = (4x - \alpha_l(c))(x^2 + \beta_l(c)x + \gamma_l(c)),$$

où $\alpha_l(c), \beta_l(c), \gamma_l(c)$ sont des éléments de $\mathbf{Z}[c]$ donnés dans le tableau suivant pour $l = 6$:

$\alpha_6(c)$	$19c^2 + 14c - 1$
$\beta_6(c)$	$2c(2c+1)$
$\gamma_6(c)$	$c(4c^3 + 4c^2 + c + 4)$

On cherche de nouveau $x_{c,l}$ sous la forme d'un polynôme en c de sorte que l'on ait une identité

$$f_{c,l}(x_{c,l}) = A_l(c)G_l(c)^2,$$

où A_l est un polynôme en c de degré ≤ 2. Mais pour cela, on exploite tout d'abord la factorisation de $f_{c,l}(x)$, en prenant $x_{c,l} = \frac{\alpha_l(c)+u^2}{4}$, ce qui assure que $4x_{c,l} - \alpha_l(c) = u^2$. Ensuite, on cherche u sous la forme d'un polynôme de degré petit en c, de sorte que $x_{c,l}^2 + \beta_l(c)x_{c,l} + \gamma_l(c)$ admette de nouveau des facteurs carrés. En pratique, on prend $u = v_1c + v_0$, et l'on cherche à spécialiser les paramètres v_0, v_1 pour avoir la factorisation $f_{c,l}(x_{c,l}) = A_l(c)G_l(c)^2$ voulue. De tels $x_{c,l}$, et les $G_l(c)$ et $A_l(c)$ associés, sont donnés dans le tableau suivant pour $l = 6$:

$x_{c,6}$	$\frac{19c^2+14c-1+v_0^2(9c+1)^2}{4}$
$G_6(c)$	$\frac{v_0(9c+1)^2}{4}$
$A_6(c)$	$9(3v_0^2+1)^2c^2 + 2(3v_0^2+1)(3v_0^2+5)c + (v_0^2-1)^2$

Cas $l = 6$: La conique d'équation $A_6(c) = z^2$ contient le point rationnel de coordonnées $(c, z) = (0, v_0^2 - 1)$, et donc se paramétrise, et l'on trouve finalement

$$c = 2\frac{9v_0^4 + 18v_0^2 - v_0^2z + z + 5}{(z + 3 + 9v_0^2)(z - 3 - 9v_0^2)}.$$

On vérifie alors que le point de $F_{c,6}$ d'abscisse $x_{c,6}$ ainsi construit ne provient pas d'un point de $E_{c,6}$ via l'isogénie φ_6.

Cas $l = 4$: Dans ce cas, les formules de Vélu donnent une équation de $F_{4,c}$ de la forme :

$$y^2 = f_{c,4}(x) = (x + c)(4x^2 + x + c).$$

On choisit $x_{c,4} = u^2 - c$, si bien que

$$f_{c,4}(x_{c,4}) = u^2(4c^2 - 8u^2c + u^2(4u^2 + 1)).$$

La conique d'équation $4c^2 - 8u^2c + u^2(4u^2+1) = z^2$ se paramétrise aisément, et l'on trouve

$$c = \frac{u^2(4u^2 + 1) - v^2}{4v + 8u^2}.$$

De même, on vérifie alors que le point de $F_{c,4}$ d'abscisse $x_{c,4}$ ainsi construit ne provient pas d'un point de $E_{c,4}$ via l'isogénie φ_4.

3. Courbes elliptiques et polynômes à groupe de Galois diédral

Avec les notations de la partie précédente, soit $P_{n,c,l}(x)$ le polynôme de $\mathbf{Z}[n,c][x]$ défini par

$$P_{n,c,l}(x) = \prod_{i=0}^{l-1}(x - x(P + iA)) = x^l - nx^{l-1} + \cdots ,$$

où P désigne un point non $\mathbf{Q}$-rationnel de $E_{c,l}$, A un point fixé d'ordre l, et $x(P+iA)$ l'abscisse du point $P+iA \in E_{c,l}$. Les logiciels de calcul formel permettent d'obtenir l'équation explicite [(1)] de $P_{n,c,l}(x) \in \mathbf{Z}[n,c][x]$, et d'établir le résultat suivant :

Théorème 2. — *Soit l un entier tel que $3 \leq l \leq 10$ ou $l = 12$. Le polynôme $P_{n,c,l}$ construit ci-dessus est génériquement irréductible sur le corps $\mathbf{Q}(n,c)$, et le groupe de Galois sur $\mathbf{Q}(n,c)$ de son corps de décomposition est génériquement le groupe diédral D_l à $2l$ éléments.*

4. Le cas D_5

Plusieurs auteurs se sont intéressés à la construction de polynômes quintiques de groupe de Galois D_5. Ainsi Weber ([**30**], p. 676) et Cebotarev ([**4**], p. 344) donnent une condition nécessaire et suffisante, sous la forme d'une paramétrisation explicite des coefficients a et b, pour que $x^5 + ax + b$ soit résoluble par radicaux. Une telle caractérisation, apparament obtenue de manière indépendante, est également l'objet de l'article [**28**]. A partir de la caractérisation dûe à Weber et Cebotarev, Roland, Yui et Zagier ([**25**]) donnent la paramétrisation des polynômes quintiques $x^5 + ax + b$ ayant D_5 pour groupe de Galois. D'autres auteurs se sont intéressés à ces questions (sans prétendre en aucune manière à l'exclusivité, citons [**12**] pour les groupes D_p, où p est premier, et [**9**] pour une théorie sur les relations entre tours modulaires et groupes diédraux).

Dans le cas particulier $l = 5$, la construction décrite dans la partie 3 donne le polynôme

$$P_{n,c,5}(x) = x^5 - nx^4 - (-c^3 - 2nc + c^2 + c)x^3 - (c^3 + nc^2 - 3c^2)x^2 - (-c^4 + 3c^3)x + c^4.$$

La substitution $(x,n,c) \longrightarrow (\frac{s}{x}, -u, s)$ redonne la famille générique de Brumer ([**3**]) citée par Martinais et Schneps ([**24**], p. 151) :

$$B_{s,u}(x) = x^5 + (s-3)x^4 + (u - s + 3)x^3 + (s^2 - s - 2u - 1)x^2 + ux + s.$$

[(1)] On peut récupérer les équations de $P_{n,c,l}(x)$ sur http ://www.math.tu-berlin.de/∼ kant/publications/papers/polynomes.txt

Cette famille est générique dans le sens où Brumer ([**24**], p. 151) affirme que, si F est un corps contenant $\mathbf{Q}$ et K est une extension galoisienne de F de groupe de Galois D_5, alors K est le corps de décomposition d'un polynôme de la forme $B_{s,u}(x)$ pour des valeurs de s et u appartenant à F. Malheureusement, à l'heure actuelle, nous ne disposons pas de la preuve de ce fait. Par ailleurs, Kihel ([**15**], p. 471) rappelle la construction de Darmon ([**6**]) de la famille

$$D_{S,T}(x) = x^5 - Sx^4 + (T+S+5)x^3 - (S^2+S-2T-5)x^2 + (T+2S+5)x - (S+3).$$

Cette famille est encore isomorphe à celle de Brumer, comme on le constate à l'aide de la transformation $(x, s, u) \longrightarrow (-x, S+3, T+2S+5)$. Les constructions de Brumer, de Darmon et celle présentée ici produisent donc la même famille de polynômes, obtenue de manière indépendante par les différents auteurs : nous avons découvert l'article [**15**] et l'existence des notes [**6**], dont l'original ne semble plus disponible [**7**] mais que l'article [**15**] décrit pour l'essentiel, après avoir démontré le théorème 2 en toute généralité, ce qui inclut en particulier le cas $l = 5$. Le cas $l = 5$ est également repris dans [**16**]. Par ailleurs, nous n'avons malheureusement pas eu d'informations concrètes concernant la construction de Brumer et la preuve de son résultat de généricité, qui n'est explicite ni dans [**24**], ni dans [**3**]. La question d'étendre le résultat de Brumer aux autres cas, c'est-à-dire de décrire explicitement les extensions diédrales d'ordre $2l$ de $\mathbf{Q}$ reste donc *a priori* encore ouverte pour les cas $l \neq 5$.

5. Une application : construction de certaines extensions cycliques de Q

Pour $3 \leq l \leq 10$ ou $l = 12$, il parait naturel de chercher, par spécialisation des paramètres dans $P_{n,c,l}(x)$, des familles ou des exemples de polynômes dont le groupe de Galois est isomorphe à $\mathbf{Z}/l\mathbf{Z}$. Nous montrons ici les résultats suivants :

Théorème 3. — *Pour* $3 \leq l \leq 6$, *il existe une famille explicite de polynômes de degré* l, *définie sur* $\mathbf{Q}$, *à groupe de Galois cyclique d'ordre* l. *Ces familles sont indexées sur, d'une part, un paramètre rationnel, d'autre part, un point d'ordre infini d'une famille de courbes elliptiques.*

Théorème 4. — *Pour* $7 \leq l \leq 10$ *et* $l = 12$, *il existe une famille explicite de polynômes de degré* l, *définie sur* $\mathbf{Q}$, *à groupe de Galois cyclique d'ordre* l. *Ces familles sont indexées par un point d'ordre infini sur une courbe elliptique définie sur* $\mathbf{Q}$.

La stratégie que nous adoptons est la suivante : sachant que le groupe de Galois de $P_{n,c,l}$ est génériquement D_l, il existe un élément $\mathfrak{D}_l$, appelé fonction d'indicateur de l'extension, qui s'exprime a priori en fonction des racines de $P_{n,c,l}$, et qui satisfait une equation quadratique :

$$\mathfrak{D}_l^2 + U_l(n,c)\mathfrak{D}_l + V_l(n,c) = 0.$$

Le groupe de Galois de $P_{n,c,l}$ est isomorphe à $\mathbf{Z}/l\mathbf{Z}$ si et seulement si $\mathfrak{D}_l$ est un rationnel, et si $P_{n,c,l}$ est irréductible. La condition de rationnalité de $\mathfrak{D}_l$ équivaut précisément à trouver un élément de $F_{c,l}(\mathbf{Q})$. La condition d'irréductibilité de $P_{n,c,l}$ équivaut à ce que cet élément de $F_{c,l}(\mathbf{Q})$ ne soit l'image par $\varphi_{c,l}$ d'aucun élément de $E_{c,l}(\mathbf{Q})$. Les résultats de la partie 2 permettent de conclure.

Cette approche est cohérente avec l'interprétation cohomologique donnée dans la partie 2. En effet, à un point fermé de $\mathrm{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/l\mathbf{Z})$ correspond une extension galoisienne de $\mathbf{Q}$ à groupe de Galois $\mathbf{Z}/l\mathbf{Z}$, du moins si l est premier, celle-ci s'obtenant comme la fibre de φ_l.

Il est à noter que plusieurs familles remarquables de polynômes existent fournissant des extensions cycliques de $\mathbf{Q}$. Les corps cubiques les plus simples ont ainsi été introduits par D. Shanks ([**27**]). E. Lehmer ([**18**]) a construit des corps quintiques cycliques simples, et M.-N. Gras des corps quartiques cycliques simples ([**10**]) et des corps sextiques cycliques simples ([**11**]). D'autres extensions cycliques de degré 6 et 10 ont été considérées par O. Lecacheux dans, respectivement, [**19**] et [**20**].

Notre construction permet de retrouver certaines de ces extensions *simples.* En effet, dans le cas $l = 3$, le corps engendré par $P_{n,c,3}(x)$ l'est aussi (via des transformations élémentaires constituées de translation et homothétie) par $\tilde{P}_{n,c,3}(x) = x^3+ux^2-nx+v$. Il suffit alors de prendre $(u,v,n) = (-t,-1,t+3)$ pour retrouver la famille cubique cyclique

$$X^3 - tX^2 - (t+3)X - 1$$

de Shanks. Dans le cas $l = 4$, on constate, à l'aide de transformations élémentaires (translation et homothétie) que le corps engendré par $P_{n,c,4}(x)$ l'est aussi par $\tilde{P}_{n,c,4}(x) = x^4 - 2x^3 + (1-n)x^2 + nx - c$. Le calcul montre, pour une spécialisation de $(n,c) = (\frac{t^2+32}{2t^2}, \frac{3t^4-1024}{16t^4})$, que

$$\text{Résultant}(\tilde{P}_{n,c,4}(x), X - (\frac{t}{2}x^2 - \frac{t^2+32}{8t}), x) = X^4 - tX^3 - 6X^2 + tX + 1,$$

et l'on retrouve ainsi la famille quartique cyclique de Gras.

The authors thank the FNR (project FNR/04/MA6/11) for their support.

Références

[1] *C. Batut, D. Bernardi, H. Cohen, M. Olivier :* User's guide to PARI-GP (version 1.39). Laboratoire A2X, Université de Bordeaux I, Bordeaux (1995)

[2] *W. Bosma, J. Cannon, C. Playoust :* The Magma algebra system. I : The user language. J. Symb. Comput. 24(3), 235-265 (1997)

[3] *A. Brumer :* Communication personnelle (2001)

[4] *N. Cebotarev :* Grundzüge der Galoisschen Theorie. Noordhoff, Groningen (1950)

[5] *M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, K. Wildanger :* KANT V4. J. Symb. Comput., 24(3), 267-283 (1997)

[6] *H. Darmon :* Une famille de polynômes liée à $X_0(5)$. Notes non publiées (1993)

[7] *H. Darmon :* Communication personnelle (2002)

[8] *S. Fermigier :* Exemples de courbes elliptiques de grand rang sur $\mathbf{Q}(t)$ et sur $\mathbf{Q}$ possédant des points d'ordre 2. C. R. Acad. Sc. Paris 322, Série I, p. 949-952 (1996)

[9] *M. D. Fried :* Introduction to Modular Tower : Generalizing dihedral group-modular curve connections. Fried, Michael D. (ed.) et al., Recent developments in the inverse Galois problem. A joint summer research conference, July 17-23, 1993, University of Washington, Seattle, WA, USA. Providence, RI : American Mathematical Society. Contemp. Math. 186, 111-171 (1995)

[10] *M.-N. Gras :* Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 sur $\mathbf{Q}$. Publ. Math. Fac. Sci. Besançon (Années 1977-78)

[11] *M.-N. Gras :* Familles d'unités dans les extensions cycliques réelles de degré 6 sur $\mathbf{Q}$. Publ. Math. Fac. Sci. Besançon, Fasc. 2 (Années 1984-85-1985-86)

[12] *Ch. U. Jensen, N. Yui :* Polynomials with D_p as Galois group. Journal of Number Theory 15, p. 347-375 (1982)

[13] *S. Kihara :* On the rank of elliptic curves with a rational point of order 3. Proc. Japan Acad., 76, Ser. 4, p. 126-127 (2000)

[14] *S. Kihara :* On an elliptic curves over $\mathbf{Q}(t)$ with a non-trivial 2-torsion point. Proc. Japan Acad., 77, Ser. 4, p. 11-12 (2001)

[15] *O. Kihel :* Groupe des unités pour des extensions diédrales complexes de degré 10 sur $\mathbf{Q}$. Journal de Théorie des Nombres de Bordeaux, 13, p. 469-482 (2001)

[16] *O. Kihel :* Extensions diédrales et courbes elliptiques. Acta Arithmetica 102.4, p. 309-314 (2002)

[17] *D. S. Kubert :* Universal bounds on the torsion of elliptic curves. Proc. Lond. Math. Soc., III. Ser. 33, 193-237 (1976)

[18] *E. Lehmer :* Connection between Gaussian periods and cyclic units. Math. Comp. 50, p. 535-541 (1988)

[19] *O. Lecacheux :* Unités d'une famille de corps cycliques réels de degré 6 liés à la courbe modulaire $X_1(13)$. Journal of Number Theory, Vol. 31, No. 1, p. 54-63 (1989)

[20] *O. Lecacheux :* Unités d'une famille de corps liés à la courbe $X_1(25)$. Ann. Inst. Fourier, Grenoble, Vol. 40, 2, p. 237-254 (1990)

[21] *O. Lecacheux :* Rang de courbes elliptiques sur $\mathbf{Q}$ avec un groupe de torsion isomorphe à $\mathbf{Z}/5\mathbf{Z}$. C. R. Acad. Sc. Paris 332, Série I, p. 1-6 (2001)

[22] *F. Leprévost, M. Pohst, A. Schöpp :* En préparation (2002)

[23] *http ://www.maplesoft.com*

[24] *D. Martinais, L. Schneps :* Polynômes à groupe de Galois diédral. Séminaire de Théorie des Nombres de Bordeaux, 4, p. 141-153 (1992)

[25] *G. Roland, N. Yui, D. Zagier :* A parametric family of quintic polynomials with Galois group D_5. Journal of Number Theory 15, p. 137-142 (1982)

[26] *R. Schoof, L. C. Washington :* Quintic polynomials and real cyclotomic fields with large class numbers. Math. Comp. 50, p. 543-556 (1988)

[27] *D. Shanks :* The simplest cubic fields. Math. Comp. 28, p. 1137-1152 (1974)

[28] *B. K. Spearman, K. S. Williams :* Characterization of solvable quintics $x^5 + ax + b$. Am. Math. Mon. 101, No. 10, p. 986-992 (1994)

[29] *J. Vélu :* Isogénies entre courbes elliptiques. C. R. Acad. Sc. Paris 273, p. 238-241 (1971)

[30] *H. Weber :* Lehrbuch der Algebra. Chelsea, New York

Franck Leprévost, Université Joseph Fourier, UFR de Mathématiques, 100, rue des Maths - B.P. 74 - F-38402 St-Martin d'Hères Cedex, France
E-mail : `Franck.Leprevost@ujf-grenoble.fr`

Michael Pohst, Technische Universität Berlin, Fakultät II - Mathematik MA 8-1 - Straße des 17. Juni 136, D-10623 Berlin, Allemagne
E-mail : `pohst@math.tu-berlin.de`

Andreas Schöpp, Technische Universität Berlin, Fakultät II - Mathematik MA 8-1 - Straße des 17. Juni 136, D-10623 Berlin, Allemagne
E-mail : `schoepp@math.tu-berlin.de`