ACTA ARITHMETICA
110.4 (2003)

# Familles de polynômes liées aux courbes modulaires $X_1(l)$ unicursales et points rationnels non-triviaux de courbes elliptiques quotient

par

Franck Leprévost (St-Martin d'Hères), Michael Pohst (Berlin)
et Andreas Schöpp (Berlin)

**1. Introduction.** L'étude du rang des courbes elliptiques définies sur $\mathbb{Q}$ et $\mathbb{Q}(t)$ 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 $\mathbb{Q}$ de grand rang et de groupe de torsion rationnel arbitraire parmi la liste des quinze groupes possibles, à savoir $\mathbb{Z}/l\mathbb{Z}$ pour $1 \le l \le 10$ ou $l = 12$, ou bien $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2l\mathbb{Z}$ pour $1 \le l \le 4$. Dans plusieurs travaux ([8], [13], [14], [20]), on construit des courbes elliptiques de rang élevé ayant un groupe de torsion non-réduit à l'élément neutre.

Considérons ici $3 \le l \le 10$ ou $l = 12$, et soit $E_{c,l}$ la famille de Kubert ([17]) des courbes elliptiques définies sur $\mathbb{Q}$ 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 $\mathbb{Q}$ de la courbe modulaire $X_1(l)$, qui est isomorphe à $\mathbb{P}^1$ 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 $\mathbb{Q}$-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 $\langle A \rangle$ désigne le groupe engendré par $A$, notons $F_{c,l}$ la courbe elliptique quotient $E_{c,l}/\langle A \rangle$, et $\varphi_l$ l'isogénie de $E_{c,l}$ sur $F_{c,l}$. On a ainsi la suite exacte suivante de $G_{\mathbb{Q}}$-modules galoisiens (où $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) :

$$1 \to \mathbb{Z}/l\mathbb{Z} \simeq \langle A \rangle \to E_{c,l}(\overline{Q}) \xrightarrow{\varphi_l} F_{c,l}(\overline{Q}) \to 1.$$

Connaissant une équation de $E_{c,l}$ et les coordonnées de $A$, les formules

2000 *Mathematics Subject Classification*: 11Y40, 11R21, 14H52, 11G05.
*Key words and phrases*: modular curves, dihedral extensions, cyclic extensions, units.

de Vélu ([29]) permettent d'obtenir explicitement une équation de $F_{c,l}$ et de $\varphi_l$.

Bien évidemment, l'image par $\varphi_l$ de points de $E_{c,l}(\mathbb{Q})$ fournit des points de $F_{c,l}(\mathbb{Q})$, 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 $F_{c,l}(\mathbb{Q})/\varphi_l(E_{c,l}(\mathbb{Q}))$, autrement dit, de points explicites de $F_{c,l}(\mathbb{Q})$ qui ne sont l'image par $\varphi_l$ d'aucun élément de $E_{c,l}(\mathbb{Q})$. En général les représentants de ces points dans $F_{c,l}(\mathbb{Q})$ sont d'ordre infini. Ceci dit, et bien que les courbes elliptiques $E_{c,l}(\mathbb{Q})$ et $F_{c,l}(\mathbb{Q})$ aient même rang, nous n'utilisons pas les constructions de [8], [13], [14], [20] qui ne fourniraient, dans notre terminologie, que des points triviaux de $F_{c,l}(\mathbb{Q})$, 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 $P_{n,c,l} \in \mathbb{Z}[n,c][x]$ pour lequel nous montrons que son corps de décomposition sur $\mathbb{Q}(n,c)$ 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 $\mathbb{Q}(n,c)$ devient isomorphe au groupe $\mathbb{Z}/l\mathbb{Z}$.

Dans la partie 5, nous montrons que ces conditions reviennent à la construction d'éléments non-triviaux de $F_{c,l}(\mathbb{Q})/\varphi_l(E_{c,l}(\mathbb{Q}))$. 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, on peut construire explicitement, pour des paramétrisations convenables de $c$, des éléments non-triviaux de $F_{c,l}(\mathbb{Q})/\varphi_l(E_{c,l}(\mathbb{Q}))$. Ces points sont en général d'ordre infini.*

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

COROLLAIRE 1. *Pour $l = 3, 4, 5$ et 6, et pour les paramétrisations de $c$ du théorème précédent, le groupe de cohomologie*

$$\mathrm{H}^1(G_{\mathbb{Q}}, \mathbb{Z}/l\mathbb{Z}) = \mathrm{Hom}(G_{\mathbb{Q}}, \mathbb{Z}/l\mathbb{Z})$$

*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

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

**2.1.** *Les cas $l = 3$ et $l = 5$.* Étant donné que notre stratégie est suffisamment générale, nous la développons pour $l \geq 5$ impair, la détaillons sur le cas $l = 5$, et serons plus succincts 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 $\mathbb{Q}$ 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 $\alpha_l, \beta_l$ et $\gamma_l$ sont les éléments de $\mathbb{Z}[c]$ 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 :

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

Cas $l = 5$ : Comme nous l'avons souligné plus haut, le degré en $c$ de $A_5(c)$ est $\leq 2$. 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 $F_{c,l}(\mathbb{Q})$ 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 $\varphi_l$ d'un point rationnel de $E_{c,l}$. Cette dernière question sera considérée de nouveau dans la partie 5.

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

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

Si l'on choisit $x_{a_1,a_3,3} = u_1a_3 + (a_1u_1 + 1)/u_1^2$, 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 $G_3(a_1, a_3) = (u_1^3a_3 - u_1a_1 - 2)/u_1^3$. L'équation $A_l(c) = z^2$ est linéaire en $a_3$, et il suffit de prendre $a_3 = (z^2 - (u_1a_1 + 1)^2)/(4u_1^3)$. 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 succincts 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 $\mathbb{Z}[c]$ 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 $\leq 2$. Mais pour cela, on exploite tout d'abord la factorisation de $f_{c,l}(x)$, en prenant $x_{c,l} = (\alpha_l(c) + u^2)/4$, 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 $l = 6$ :

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

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 $\varphi_6$.

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 $\varphi_4$.

**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 $\mathbb{Z}[n, c][x]$ défini par

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

où $P$ désigne un point non $\mathbb{Q}$-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 $P_{n,c,l}(x) \in \mathbb{Z}[n, c][x]$, 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 $\mathbb{Q}(n, c)$, et le groupe de Galois sur $\mathbb{Q}(n, c)$ 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 Chebotarev ([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, apparemment obtenue de manière indépendante, est également l'objet de l'article [28]. À partir de la caractérisation dûe à Weber et Chebotarev, 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

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

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 $(x, n, c) \mapsto (s/x, -u, s)$ redonne la famille générique de Brumer ([3]) citée par Martinais et Schneps ([24, p. 151]) :

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

Cette famille est générique dans le sens où Brumer ([24, p. 151]) affirme que, si $F$ est un corps contenant $\mathbb{Q}$ 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 $(x, s, u) \mapsto (-x, S+3, T+2S+5)$. 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 $\mathbb{Q}$ reste donc *a priori* encore ouverte pour les cas $l \neq 5$.

**5. Une application : construction de certaines extensions cycliques de $\mathbb{Q}$.** Pour $3 \leq l \leq 10$ ou $l = 12$, il paraît 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 $\mathbb{Z}/l\mathbb{Z}$. 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 $\mathbb{Q}$, 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 $\mathbb{Q}$, à groupe de Galois cyclique d'ordre $l$. Ces familles sont indexées par un point d'ordre infini sur une courbe elliptique définie sur $\mathbb{Q}$.*

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 $\mathbb{Z}/l\mathbb{Z}$ 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 $F_{c,l}(\mathbb{Q})$. La condition d'irréductibilité de $P_{n,c,l}$ équivaut à ce que cet élément de $F_{c,l}(\mathbb{Q})$ ne soit l'image par $\varphi_{c,l}$ d'aucun élément de $E_{c,l}(\mathbb{Q})$. 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 $\mathrm{Hom}(G_{\mathbb{Q}}, \mathbb{Z}/l\mathbb{Z})$ correspond une extension galoisienne de $\mathbb{Q}$ à groupe de Galois $\mathbb{Z}/l\mathbb{Z}$, du moins si $l$ est premier, celle-ci s'obtenant comme la fibre de $\varphi_l$.

Il est à noter que plusieurs familles remarquables de polynômes existent fournissant des extensions cycliques de $\mathbb{Q}$. Les corps cubiques les plus simples ont ainsi été introduits par D. Shanks ([27]). E. Lehmer ([21], voir également [26]) 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, [18] et [19].

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 $\widetilde{P}_{n,c,3}(x) = x^3 + ux^2 - nx + v$. 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 $\widetilde{P}_{n,c,4}(x) = x^4 - 2x^3 + (1-n)x^2 + nx - c$. Le calcul montre, pour une spécialisation de $(n, c) = \left(\frac{t^2+32}{2t^2}, \frac{3t^4-1024}{16t^4}\right)$, que

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

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

**Références**


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

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

[3] A. Brumer, communication personnelle, 2001.

[4] N. Chebotarev [N. Tschebotaröw], *Grundzüge der Galoisschen Theorie*, Noordhoff, Groningen, 1950.

[5] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, *KANT V4*, J. Symbolic Comput. 24 (1997), 267–283.

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

[7] —, communication personnelle, 2002.

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

[9] M. D. Fried, *Introduction to modular towers*: *Generalizing dihedral group-modular curve connections*, in: M. D. Fried *et al.* (eds.), Recent Developments in the Inverse Galois Problem (Seattle, WA, 1993), Contemp. Math. 186, Amer. Math. Soc., 1995, 111–171.

[10] M.-N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré* 4 *de* $\mathbb{Q}$, Publ. Math. Fac. Sci. Besançon 1977-78, no. 2.

[11] —, *Familles d'unités dans les extensions cycliques réelles de degré* 6 *de* $\mathbb{Q}$, Publ. Math. Fac. Sci. Besançon 1984-85–1985-86, no. 2.

[12] C. U. Jensen and N. Yui, *Polynomials with* $D_p$ *as Galois group*, J. Number Theory 15 (1982), 347–375.

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

[14] —, *On an elliptic curves over* $\mathbb{Q}(t)$ *with a non-trivial* 2*-torsion point*, ibid. 77 (2001), 11–12.

[15] O. Kihel, *Groupe des unités pour des extensions diédrales complexes de degré* 10 *sur* $\mathbb{Q}$, J. Théor. Nombres Bordeaux 13 (2001), 469–482.

[16] —, *Extensions diédrales et courbes elliptiques*, Acta Arith. 102 (2002), 309–314.

[17] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. 33 (1976), 193–237.

[18] O. Lecacheux, *Unités d'une famille de corps cycliques réels de degré* 6 *liés à la courbe modulaire* $X_1(13)$, J. Number Theory 31 (1989), 54–63.

[19] —, *Unités d'une famille de corps liés à la courbe* $X_1(25)$, Ann. Inst. Fourier (Grenoble) 40 (1990), 237–254.

[20] —, *Rang de courbes elliptiques sur* $\mathbb{Q}$ *avec un groupe de torsion isomorphe à* $\mathbb{Z}/5\mathbb{Z}$, C. R. Acad. Sci. Paris Sér. I 332 (2001), 1–6.

[21] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. 50 (1988), 535–541.

[22] F. Leprévost, M. Pohst et A. Schöpp, en préparation, 2002.

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

[24] D. Martinais et L. Schneps, *Polynômes à groupe de Galois diédral*, Sém. Théor. Nombres Bordeaux 4 (1992), 141–153.
[25] G. Roland, N. Yui and D. Zagier, *A parametric family of quintic polynomials with Galois group $D_5$*, J. Number Theory 15 (1982), 137–142.
[26] R. Schoof and L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. 50 (1988), 543–556.
[27] D. Shanks, *The simplest cubic fields*, ibid. 28 (1974), 1137–1152.
[28] B. K. Spearman and K. S. Williams, *Characterization of solvable quintics $x^5+ax+b$*, Amer. Math. Monthly 101 (1994), 986–992.
[29] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris 273 (1971), 238–241.
[30] H. Weber, *Lehrbuch der Algebra*, Vieweg, Braunschweig, 1898.

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

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

*Reçu le 26.11.2002* (4417)