ACTA ARITHMETICA
102.4 (2002)

Extensions diédrales et courbes elliptiques

par

Omar Kihel (Lethbridge)

1. Introduction. À partir d'une observation faite par J. Conway sur une suite récurrente (1) H. Darmon dans un travail non publié [1] a exhibé un polynôme de degré 5 à coefficients dans le corps de fonctions $\mathbb{Q}(S,T)$. Le calcul du discriminant du polynôme $p(x)$ fait apparaître une courbe elliptique E_S sur le corps de fonctions $\mathbb{Q}(S)$. Dans la première partie de ce travail, on reconstruit le polynôme $p(x)$ et la courbe elliptique E_S trouvés par H. Darmon. Nous montrons ensuite que le corps de décomposition du polynôme $p(x)$ est une extension diédrale de degré 10 sur le corps de fonctions $\mathbb{Q}(S,T)$. Dans la seconde partie de ce travail, nous visualisons d'abord cette courbe elliptique E_S comme une courbe elliptique sur le corps de fonctions $\mathbb{Q}(S)$; puis, nous spécialisons S en $S_0 \in \mathbb{Q}$ avec $S_0 \neq -3$, et nous montrons que cette courbe elliptique est munie d'une isogénie rationnelle de degré 5. Finalement, nous montrons que lorsque S parcourt $\mathbb{Q}(\zeta_5)$, la famille de ces courbes elliptiques est paramétrée par les points rationnels de $X_1(5)(\mathbb{Q}(\zeta_5))$.

2. Polynômes de degré 5 et extensions diédrales. Soit $\{x_i\}_{i\in\mathbb{N}}$ une suite d'éléments non nuls satisfaisant la récurrence

$$x_{i-1}x_{i+1} = x_i + 1. \tag{1}$$

Alors x_i est périodique, de période 5. Cette affirmation se vérifie par un calcul direct.

Soit

$$p(x) = \prod_{i=1}^{5}(x - \omega_i)$$

un polynôme de degré 5 dont les racines $\omega_1, \ldots, \omega_5$ satisfont la récurrence (1), les indices étant lus modulo 5. Posons

$$S = \omega_1 + \omega_2 + \omega_3 + \omega_4 + \omega_5, \quad T = \omega_1\,\omega_2 + \omega_2\,\omega_3 + \omega_3\,\omega_4 + \omega_4\,\omega_5 + \omega_5\,\omega_1.$$

2000 *Mathematics Subject Classification*: 11R09, 11G05.

Le polynôme $p(x)$ s'exprime en fonction de S et T. Si h est une expression en fonction des ω_i, notons par $[h]$ la somme des cinq expressions obtenues à partir de h en permutant cycliquement les indices des ω_i. Par exemple, $T = [\omega_1\omega_2]$ et $S = [\omega_1]$. Avec cette notation, on a

$$S^2 = [\omega_1^2] + 2[\omega_1\omega_2] + 2[\omega_1\omega_3] = [\omega_1^2] + 2T + 2S + 10,$$

ce qui entraîne

$$[\omega_1^2] = S^2 - 2T - 2S - 10.$$

Soient $\sigma_1, \ldots, \sigma_5$ les fonctions symétriques élémentaires de Newton. On a alors

$$\begin{aligned}
\sigma_1 &= S,\\
\sigma_2 &= [\omega_1\omega_2] + [\omega_1\omega_3] = T + S + 5,\\
\sigma_3 &= [\omega_1\omega_2\omega_3] + [\omega_1\omega_2\omega_4] = [\omega_2^2 + \omega_2] + [\omega_1\omega_3 + \omega_1]\\
&= (S^2 - 2T - 2S - 10) + 3S + 5 = S^2 + S - 2T - 5,\\
\sigma_4 &= [\omega_1\omega_2\omega_3\omega_4] = [(\omega_2 + 1)(\omega_3 + 1)] = T + 2S + 5,\\
\sigma_5 &= \omega_1\omega_2\omega_3\omega_4\omega_5 = (\omega_2 + 1)(\omega_3 + 1)\omega_5 = (\omega_2 + 1)(\omega_4 + \omega_5 + 1) = S + 3.
\end{aligned}$$

Donc les racines du polynôme

$$p(x) = x^5 - Sx^4 + (T+S+5)x^3 - (S^2+S-2T-5)x^2 + (T+2S+5)x - (S+3)$$

satisfont la récurrence (1), quelles que soient les valeurs de S et T. Ici S et T sont des polynômes invariants par l'action de Galois. De plus, $p(x)$ est le polynôme le plus général de cette sorte, dépendant des deux paramètres S et T. Soit G le groupe de Galois du polynôme $p(x)$. Comme le polynôme $p(x)$ est de degré 5, alors l'ordre de G est un multiple de 5.

THÉORÈME 1. *Le groupe de Galois G du polynôme $p(x)$ est égale à D_5, le groupe diédral d'ordre* 10.

Par un théorème bien connu de la théorie de Galois, le groupe de Galois de $p(x)$ est donc un sous-groupe résoluble du groupe S_5. On sait qu'un sous-groupe résoluble de S_5 est de cardinalité au plus égale à 20. Soit J l'unique sous-groupe (à conjugaison près) résoluble de S_5 contenant 20 éléments. Alors J est engendré par α et β, où

$$\alpha = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,5\,1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,1\,5 \end{pmatrix}.$$

Supposons que le groupe de Galois G soit égal à J tout entier. Appliquant l'élément β à la relation

$$\omega_3\omega_5 = \omega_4 + 1,$$

nous avons alors

$$\omega_4\omega_5 = \omega_1 + 1.$$

Puisque

$$\omega_2\omega_5 = \omega_1 + 1,$$

nous obtenons alors que $\omega_2 = \omega_4$, ce qui donne une contradiction. Ainsi G est un sous-groupe de D_5. On montre par spécialisation que le groupe G est en fait D_5 tout entier. Il suffit de spécialiser par exemple en $S = -2$ et $T = 1$ pour trouver que le groupe de Galois du polynôme $p(x)$ obtenu est le groupe diédral D_5 tout entier. Le corps de décomposition $\widetilde{L}$ de $p(x)$ est donc une extension diédrale de degré dix sur le corps de fonctions $\mathbb{Q}(S,T)$.

Appelons $\widetilde{K}$ le sous-corps de $\widetilde{L}$ fixé par le sous-groupe distingué H de D_5 d'ordre 5. Le corps quadratique $\widetilde{K}$ est engendré par l'élément

$$D = ([\omega_1^2\omega_2] - [\omega_2^2\omega_1]).$$

3. Courbes elliptiques munie d'une 5-isogénie. Un calcul fait sur ordinateur donne que

$$\begin{aligned} D^2 = \Delta(T,S) = &-4T^3 - (-S^2 + 48S + 140)T^2 \\ &-(-28S^3 - 48S^2 + 370S + 800)T \\ &-(4S^5 + 4S^4 - 104S^3 - 160S^2 + 700S + 1375). \end{aligned}$$

Un autre calcul nous permet d'ailleurs de constater que le discriminant de $p(x)$ est égal à

$$(S+3)^2\Delta(T,S)^2.$$

Le corps $\widetilde{K}$ est donc le corps de fonctions de la courbe

$$E_S : \quad y^2 = \Delta(T,S)$$

dont l'invariant modulaire est

$$j(E_S) = \frac{(S^4 + 240S^3 + 2600S^2 + 9000S + 10000)^3}{(S+3)(S^2 - 5S - 25)^5}, \tag{2}$$

où E_S est vue comme courbe elliptique sur $\mathbb{Q}(S)$. Le corps $\widetilde{L}$ est une extension régulière de $\mathbb{Q}$, c'est-à-dire que la clôture algébrique de $\mathbb{Q}$ dans $\widetilde{L}$ est égale à $\mathbb{Q}$. Le corps $\widetilde{L}$ peut être vu comme le corps de fonctions d'une courbe projective lisse C (absolument irréductible sur $\mathbb{Q}$). Spécialisons S en $S_0 \in \mathbb{Q}$ avec $S_0 \neq -3$; et dénotons par L le corps de décomposition du polynôme $p(x)$ obtenu, à coefficients dans $\mathbb{Q}(T)$, et par K son sous-corps quadratique. Il est facile de voir que le dénominateur de $j(E_{S_0})$ dans la formule (2) n'a pas de racine rationnelle. Ainsi, le polynôme $p(x)$ décrit un revêtement de la droite projective $\mathbb{P}^1$ ramifié en quatre points distincts (les 3 racines distinctes de $\Delta(T,S_0)$ et le point à l'infini). La monodromie autour de ces quatre points est une reflection. Ainsi, l'extension L est une extension cyclique de degré 5 de K qui est non ramifiée.

THÉORÈME 2. *Lorsqu'on spécialise S en $S_0 \neq -3$, la courbe elliptique E_{S_0} est munie d'une isogénie rationnelle définie sur $\mathbb{Q}$ de degré 5, c'est-à-dire que E_{S_0} admet un sous-groupe de torsion invariant par l'action de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Preuve. L'extension L est cyclique de degré 5 de K non ramifiée. Le corps K est le corps de fonctions de la courbe elliptique E_{S_0} définie par $Y^2 = \Delta(T, S_0)$; alors l'injection $K \hookrightarrow L$ de K (contenant $\mathbb{Q}(T)$) dans L induit le morphisme $\Phi : C \to E_{S_0}$ qui est de degré 5 et non ramifié. Ainsi, en utilisant la formule de Hurwitz on obtient que C est une courbe elliptique et Φ est une isogénie de courbes elliptiques $C \to E_{S_0}$ de degré 5.

La courbe C (dont l'équation nous a été calculée par O. Lecacheux) est donnée par

$$C : \quad V^2S_0^2 + VS_0U + VUS_0^2 - VS_0^2 + U^3 - S_0U^2 = 0.$$

La courbe modulaire $X_0(5)$ a un modèle sur $\mathbb{Z}$ donné par la fonction modulaire $a(z) = (\eta(z)/\eta(5z))^6$ où $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$, et nous avons le morphisme

$$j : X_0(5) \to X_0(1), \qquad (E, C) \mapsto (E),$$

qui à tout point (E, C) de $X_0(5)$ (C est un sous-groupe de 5-torsion de E invariant par l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) associe le point (E) de $X_0(1)$ paramétré par l'invariant modulaire

$$j(a) = \frac{(a^2 + 10a + 5)^3}{a}. \tag{3}$$

On vient de voir au théorème 2 que lorsqu'on spécialise S en $S_0 \in \mathbb{Q}$ avec $S_0 \neq -3$, la courbe elliptique E_{S_0} est munie d'une isogénie rationnelle de degré 5. Soit $\mathcal{F}$ la famille de courbes elliptiques E_S lorsque S parcourt $\mathbb{P}^1(\mathbb{Q})$. Question : Quelle relation y a-t-il entre la famille $\mathcal{F}$ des courbes E_S, lorsque S parcourt $\mathbb{P}^1(\mathbb{Q})$, et la courbe modulaire $X_0(5)$? Pour répondre à cette question, il est intéressant d'exprimer S en termes de la fonction modulaire $a(z) = (\eta(z)/\eta(5z))^6$ de niveau 5 (ou bien a en fonction de S).

THÉORÈME 3. *La fonction a s'exprime comme une fonction rationnelle de S de degré 2, et on a le morphisme i de degré 2 défini par* :

$$i : \mathbb{P}^1(\mathbb{Q}) \to X_0(5)(\mathbb{Q}), \qquad S \mapsto i(S) = 125\frac{S+3}{S^2 - 5S - 25}.$$

Preuve. D'après ce qui précède, pour $S = S_0 \neq -3$, E_{S_0} est munie d'une isogénie rationnelle de degré 5 ; donc (E_{S_0}, C) (C est le sous-groupe rationnel, i.e. le noyau de l'isogénie) peut être représenté par un point de $X_0(5)$. Si j est le morphisme

$$j : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q}), \qquad S \mapsto j(E_S),$$

alors ce morphisme j qui est de degré 12 se factorise comme suit :

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{Q}) & \xrightarrow{2} & X_0(5) \\ {\scriptstyle 12}\downarrow & \swarrow{\scriptstyle 6} & \\ \mathbb{P}^1(\mathbb{Q}) & & \end{array}$$

Il suffit d'égaler l'élément $j(E_S)$ donné dans la formule (2) avec l'élément $j(a)$ donné par la formule (3) et de déduire que

$$a = 125\,\frac{S+3}{S^2-5S-25}.$$

COROLLAIRE 1. *Il existe un morphisme de degré* 2 *entre* $\mathcal{F}$ *et* $X_0(5)$.

On peut spécialiser S en plusieurs valeurs telles que les courbes elliptiques obtenues n'admettent aucun point de torsion sur $\mathbb{Q}$ autre que le point à l'infini.

REMARQUE 1. La courbe

$$E'_u : \quad y^2 + uxy + (u-1)y = x^3 + (u-1)x^2$$

est une courbe elliptique contenant le point $(0,0)$ qui est d'ordre 5 ; en fait lorsque u décrit un corps de nombres F, la famille $\{E'_u\}$ est la famille universelle des courbes elliptiques définies sur F munies d'un point d'ordre 5 défini sur F, i.e. pour toute courbe elliptique E définie sur F contenant un point P d'ordre 5 défini sur F, il existe un $u_0 \in F$ unique et un isomorphisme entre E'_{u_0} et E qui envoie le point $(0,0)$ sur le point P. Voir [2].

THÉORÈME 4. *Lorsqu'on spécialise* S *dans le corps* $\mathbb{Q}(\zeta_5)$, *les courbes elliptiques* E_S *sous leurs formes de Weierstrass*

$$\begin{aligned} y^2 = x^3 &- 27(16S^4 + 3840S^3 + 41600S^2 + 144000S + 160000)x \\ &- 54(-64S^6 + 32256S^5 + 1132800S^4 + 10656000S^3 \\ &+ 44160000S^2 + 86400000S + 65600000) \end{aligned}$$

admettent le point $P = (x_S, y_S)$ *comme point d'ordre* 5 *défini sur* $\mathbb{Q}(\zeta_5)$, *où*

$$x_S = \frac{-12(-2900 + 1300\sqrt{5} - 1080S + 480\sqrt{5}S - 59S^2 + 25\sqrt{5}S^2)}{11\sqrt{5} - 25},$$

$$y_S = \frac{216(-35 + 15\sqrt{5} - 11S + 5\sqrt{5}S)(2S - 5 + 5\sqrt{5})^2(22\sqrt{5} - 50)^{1/2}}{(11\sqrt{5} - 25)^2}.$$

Preuve. Pour $u = (-40 + 20\sqrt{5} - 9S + 5\sqrt{5}S)/(2S - 5 + 5\sqrt{5})$, la courbe E'_u est isomorphe à E_S. Cet isomorphisme envoie le point $(0,0)$ d'ordre 5 de la courbe E'_u sur le point $P = (x_S, y_S)$. Le point $P = (x_S, y_S)$ est défini sur $\mathbb{Q}(\sqrt{22\sqrt{5} - 50})$. Le corps $\mathbb{Q}(\sqrt{22\sqrt{5} - 50})$ est cyclique de degré 4 sur $\mathbb{Q}$ de conducteur égal à 5. Ainsi on a $\mathbb{Q}(\sqrt{22\sqrt{5} - 50}) = \mathbb{Q}(\zeta_5)$.

THÉORÈME 5. *Pour tout $u_0 \in \mathbb{Q}(\zeta_5)$, il existe un S_0 unique dans $\mathbb{Q}(\zeta_5)$ et un isomorphisme*

$$f : E'_{u_0} \to E_{S_0}$$

défini sur $\mathbb{Q}(\zeta_5)$, qui envoie le point $(0,0)$ sur le point $P = (x_S, y_S)$ défini précédemment.

COROLLAIRE 2. *La famille $\mathcal{F}$ des courbes elliptiques E_S lorsque S parcourt $\mathbb{Q}(\zeta_5)$ est paramétrée par les points rationnels de $X_1(5)(\mathbb{Q}(\zeta_5))$.*

Remerciements. Je tiens à remercier C. Levesque pour ses conseils et les encouragements qu'il m'a prodigués le long de ce travail. Je tiens aussi à remercier vivement H. Darmon pour m'avoir permis d'utiliser [1] et pour les discussions fructueuses que j'ai eues avec lui. Je remercie aussi C. Greither pour les discussions que j'ai eues avec lui.

Références

[1] H. Darmon, Notes non publiées.
[2] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

Department of Mathematics and Computer Science
University of Lethbridge
4401 University Drive
Lethbridge, Alberta
Canada T1K 3M4
E-mail: kihel@cs.uleth.ca

Reçu le 27.4.2000
et révisé le 13.9.2001 (3814)