ANNALES DE L'INSTITUT FOURIER

ODILE LECACHEUX

Unités d'une famille de corps liés à la courbe $X_1(25)$

Annales de l'institut Fourier, tome 40, nº 2 (1990), p. 237-253
<http://www.numdam.org/item?id=AIF_1990__40_2_237_0>

© Annales de l'institut Fourier, 1990, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (http://annalif.ujf-grenoble.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Inst. Fourier, Grenoble
40, 2 (1990), 237-254

UNITÉS D'UNE FAMILLE DE CORPS LIÉS A LA COURBE $X_1(25)$

par Odile LECACHEUX

Introduction.

On appelle généralement « simplest cubic fields » [12] les extensions cycliques de degré trois engendrées par l'une des racines de

$$X^3 - tX^2 - (t+3)X - 1, \qquad t \in \mathbb{Z}.$$

Un analogue en degré quatre est donné dans (3) par les extensions cycliques engendrées par une racine de

$$X^4 - tX^3 - 6X^2 + tX + 1, \qquad t \in \mathbb{Z}.$$

E. Lehmer donne dans [6] un exemple d'une famille de corps cycliques de degré cinq.

Le principal intérêt de ces corps est que, sous certaines conditions, il est possible de déterminer un système fondamental d'unités et d'évaluer leurs nombres de classes. Ils fournissent des exemples où le nombre de classe de $\mathbb{Q}(\zeta_p)^+$ est supérieur à p [11], [10].

Dans un article précédent nous avons utilisé une courbe modulaire pour construire une famille de corps cycliques de degré 6 [8].

Nous appliquerons ici ces mêmes idées, en utilisant la courbe modulaire $X_1(25)$; ce qui nous permettra de construire une famille de corps de degré dix, contenant la famille étudiée par E. Lehmer, R. Schoof et L. C. Washington [6], [10].

Nous étudierons alors le groupe des unités de ces corps. Sous certaines conditions nous trouvons un système fondamental d'unités.

Mots-clés : Unités modulaires - Groupe d'unités - Extension abélienne - Géométrie des nombres.

Classification A.M.S. : 11G16 - 11R27 - 11R20 - 11H06.

Dans un cas particulier nous expliquerons le lien entre ces unités et les périodes de Gauss de ces extensions abéliennes. Enfin nous retrouvons la famille de corps de degré cinq abéliens sur $\mathbb{Q}(\sqrt{5})$, liée à l'involution w_{25}. On peut trouver des unités dans ces corps.

Nous remarquons que les unités et la taille des régulateurs sont en relation avec le fait que les pointes des courbes modulaires engendrent des groupes d'ordre fini dans leurs jacobiennes.

Rappels sur les courbes $X_1(25)$ et $X_0(25)$.

Kubert a étudié ces deux courbes modulaires en ce qui concerne leurs pointes et leurs automorphismes. Rappelons les différentes propriétés nécessaires à la compréhension des calculs.

Les groupes

$$\Gamma_0(25) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})/c \equiv 0(25)\right\}$$

$$\Gamma_1(25) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})/c \equiv 0, a \equiv 1, d \equiv 1(25)\right\}$$

opèrent sur le demi-plan de Poincaré. Par passage au quotient et compactification on obtient les courbes $X_0(25)$ et $X_1(25)$.

La courbe $X_1(25)$ est de genre 12, la courbe $X_0(25)$ est de genre 0. Le groupe $(\mathbb{Z}/25\mathbb{Z})^*/\pm 1$, d'ordre 10, est isomorphe au groupe de Galois du revêtement $X_1(25) \to X_0(25)$.

On choisira comme générateur de ce groupe l'automorphisme T correspondant à la matrice $\begin{pmatrix} -12 & -1 \\ 25 & 2 \end{pmatrix}$.

Les pointes rationnelles de $X_1(25)$ sont représentées par les couples ci-dessous :

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 2 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 3 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 4 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 6 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 7 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 8 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 9 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 11 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

L'action de T^5 est donnée par les flèches ci-dessus.

Les pointes non rationnelles forment trois collections de conjuguées : les pointes $\binom{1}{5}$ $\binom{2}{5}$ $\binom{3}{5}$ $\binom{4}{5}$, les pointes $\binom{1}{10}$ $\binom{2}{10}$ $\binom{3}{10}$ $\binom{4}{10}$ et les images des pointes rationnelles par l'involution w_{25} :

$$\binom{i}{25} = w_{25}\binom{0}{i}.$$

Nous notons $a_1\, a_2\, a_3 \ldots a_{12}\ \alpha \to \beta \to$ le diviseur $\Sigma a_i\binom{0}{i} + \alpha\Sigma\binom{i}{5} + \beta\Sigma\binom{i}{10}$.

On supprimera $\alpha \to \beta \to$ si α ou β sont nuls.

Deux sous-groupes sont compris entre $\Gamma_1(25)$ et $\Gamma_0(25)$. L'un est formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où $a = \pm 1, \mp 7 \bmod 5$. Il correspond à la courbe B de genre quatre quotient de $X_1(25)$ par l'automorphisme T^2. L'autre est le groupe $\Gamma_0(25) \cap \Gamma_1(25)$, la courbe correspondante C est de genre 0.

Équation de la courbe *B*.

Dans la proposition IV 4.5, p. 227 de [4], Kubert introduit les formes $\phi_{i,j}$, les quotients de ces formes donnent des fonctions modulaires sur $X_1(25)$.

Rappelons qu'en fait

$$\phi_{i,j}/\phi_{i,k} = (\mathfrak{P}(i/25;\tau,1) - \mathfrak{P}(j/25;\tau,1))/(\mathfrak{P}(i/25;\tau,1) - \mathfrak{P}(k/25;\tau,1)),$$

où $\mathfrak{P}$ est la fonction de Weierstrass.

Les développements en q, de ces fonctions permettent de calculer les valeurs, zéros et pôles en la pointe $\binom{1}{25}$.

Remarquons d'autre part que $(\phi_{i,j}/\phi_{r,s})\,|\,T = (\phi_{2i,2j})/(\phi_{2r,2s})$. Notons y la fonction modulaire $(\phi_{1,12}/\phi_{1,3}).(\phi_{7,9}/\phi_{7,4})$. Son diviseur est concentré aux pointes rationnelles et s'écrit sous la forme :

$$3 \quad -2 \quad -2 \quad -2 \quad 0 \quad 3 \quad 0 \quad 1 \quad -2 \quad 1.$$

En utilisant la définition de y on remarque que $y|T^5$ est égal à y. La fonction $y|T^2$ a pour diviseur :

$$-2 \quad 0 \quad 1 \quad 1 \quad 3 \quad -2 \quad 3 \quad -2 \quad 0 \quad -2.$$

Nous utiliserons la fonction $x = y.(y|T^2)$, de diviseur :

$$1 \quad -2 \quad -1 \quad -1 \quad 3 \quad 1 \quad 3 \quad -1 \quad -2 \quad -1.$$

Le choix de x a été déterminé pour que ses pôles soient d'ordre le plus petit possible. La nullité du diviseur de la fonction $y.(y|T).(y|T^2).(y|T^3).(y|T^4)$ montre que cette fonction est constante, sa valeur à la pointe infinie permet de déterminer cette constante. Les valeurs de $y|T^i$ en cette pointe sont des unités conjuguées, cette constante vaut donc ± 1 et est égale à la norme sur $\mathbb{Q}$ de $-\sin(13\pi/25).\sin(16\pi/25).(\sin(4\pi/25))^{-1}.(\sin(3\pi/25))^{-1}$, donc égale à -1.

On en déduit que $-1/y = (x|T).(x|T^2)$.

Pour déterminer le diviseur de la fonction $x - x|T^2$ nous aurons besoin de la fonction $L = (\phi_{12,9}.\phi_{6,8})/(\phi_{12,8}.\phi_{6,9})$ de diviseur :

$$1 \quad 2 \quad 0 \quad 0 \quad -1 \quad 1 \quad -1 \quad 2 \quad 2 \quad 2 \quad -1\rightarrow \quad -1\rightarrow.$$

Les fonctions $(\phi_{1,12}/\phi_{1,3}) - 1$ et $(\phi_{7,9}/\phi_{7,4}) - 1$ s'annulent aux 8 pointes non rationnelles $\begin{pmatrix} i \\ 5 \end{pmatrix}$ et $\begin{pmatrix} i \\ 10 \end{pmatrix}$.

Les fonctions $y|T^i - 1$ et $x|T^i - 1$ ont donc aussi comme zéros ces pointes. Par conséquent, la fonction $x - x|T^2$ s'annule en ces pointes.

La comparaison des diviseurs de x et de $x|T^2$ permet d'écrire le diviseur de $x - x|T^2$ sous la forme suivante :

$$-1 \quad -2 \quad -a \quad -a \quad 1 \quad -1 \quad 1 \quad -2 \quad -2 \quad -2 \quad b\rightarrow c\rightarrow + (d)$$

où a, b, c sont des entiers plus grands que 1 et (d) un diviseur positif. De plus les entiers a, b, c sont liés par la relation $-8 + 4.(b+c) - 2a \leqslant 0$.

Les seules possibilités sont $a = 1$, $b = c = 1$, ou $a = 0$, $b = c = 1$ et $(d) = 0$.

La première possibilité est exclue car la fonction $L.(x-x|T^2)$, stable par T^5, aurait un diviseur sur B ayant un seul pôle simple, ce qui est impossible car B est de genre 4.

En comparant les diviseurs des fonctions $x - x|T^2$, $x|T-x|T^3$ et x, nous obtenons la relation suivante :

$$x - x|T^2 = k.(x|T-x|T^3).x.$$

La constante k est rationnelle, car les fonctions x et $x|T^2$ sont rationnelles ; à la pointe infinie elles prennent des valeurs entières.

De l'égalité $N_{\mathbb{Q}}\left((x-x|T^2)\begin{pmatrix}1\\0\end{pmatrix}\right) = k^5 N_{\mathbb{Q}}\left((x|T-x|T^3)\begin{pmatrix}1\\0\end{pmatrix}\right).N_{\mathbb{Q}}(x)$,

on en déduit que $k = 1$. En utilisant l'automorphisme T, nous obtenons les cinq relations :

$$\begin{aligned}
(x-x|T^2) &= x.(x|T-x|T^3)\\
(x|T-x|T^3) &= x|T.(x|T^2-x|T^4)\\
(x|T^2-x|T^4) &= x|T^2.(x|T^3-x)\\
(x|T^3-x) &= x|T^3.(x|T^4-x|T)\\
(x|T^4-x|T) &= x|T^4.(x-x|T^2).
\end{aligned}$$

De plus $x.(x|T).(x|T^2).(x|T^3).(x|T^4) = 1$.

Pour garder la symétrie nous introduirons une fonction n, stable par T et ayant des pôles simples aux 10 pointes rationnelles. Ce choix est possible car $X_0(25)$ est de genre 0. Nous choisirons comme fonction n la fonction $-5(\eta(25\tau)/\eta(\tau) = -5(\Delta(25\tau)/\Delta(\tau))^{1/24}$. Cette fonction s'annule sur les pointes $\begin{pmatrix}i\\25\end{pmatrix}$. Son développement à la pointe $\begin{pmatrix}1\\25\end{pmatrix}$ est de la forme : $-5q + \ldots$.

Si on considère les diviseurs des fonctions $x|T^i$ et $1/(x|T^i)$ on constate que les trois fonctions

$$S = \sum_{i=0}^{4} x|T^i,\ Q = \sum_{i=0}^{4} 1/(x|T^i) \quad \text{et} \quad R = \sum_{i=0}^{4} (x|T^i).(x|T^{i+1})$$

sont des polynômes en n de degrés respectivement 2, 3 et 3. Il existe donc des coefficients a, b, c, d tels que $S + aQ + bR = cn + d$. Pour déterminer ces coefficients le plus simple est de déterminer, à l'aide des

cinq relations ci-dessus un développement à la pointe $\begin{pmatrix}0\\1\end{pmatrix}$ par rapport à x, paramètre local. Ceci donne :

$$\begin{aligned}
x\,|\,T &= 1/x^2 + 2 - x - 2x^2 + o(x^2)\\
x\,|\,T^2 &= -\,1/x - x + x^2 + o(x^2)\\
x\,|\,T^3 &= x^3 - x^4 - 3x^5 + o(x^5)\\
x\,|\,T^4 &= -\,1/x - 1 - x + x^2 + o(x^3).
\end{aligned}$$

Puis on obtient

$$\begin{aligned}
S &= 1/x^2 - 2/x + 1 + o(1),\\
Q &= -\,1/x^3 - 2/x^2 + 1 + 3x + o(x),\\
R &= 1/x^3 + 1/x^2 + 5/x - 5x + o(1).
\end{aligned}$$

On a donc $R + Q - S = 5/x + o(1)$.

Un développement à l'ordre 1 en q permet de conclure et donne les formules :

$$R + Q - S = 5 + 5q + o(q), \qquad \text{soit } R + Q - S = 5(1-n).$$

On calcule alors un développement en $1/n$ des cinq fonctions $x\,|\,T^i$. Le résultat est le suivant :

$$\begin{aligned}
x &= 1/n - 1/n^2 - 1/n^3 - 2/n^4 - 4/n^5 - 2/n^6 + 14/n^7 + 44/n^8 + 55/n^9 - 1/n^{10}\\
&\qquad - 96/n^{11} + o(1/n^{11})\\
x\,|\,T &= n^2 - 2n + 3 - 1/n - 1/n^2 + 2/n^3 + 8/n^4 + 8/n^5 - 15/n^6 - 59/n^7 - 63/n^8\\
&\qquad + o(1/n^9)\\
x\,|\,T^2 &= n - 1 + 1/n + 1/n^2 - 1/n^4 + 2/n^5 + 12/n^6 + 18/n^7 - 12/n^8 - 94/n^9\\
&\qquad + o(1/n^9)\\
x\,|\,T^3 &= -\,1/n^3 - 4/n^4 - 7/n^5 - 1/n^6 + 25/n^7 + 59/n^8 + 42/n^9 - 79/n^{10} - 194/n^{11}\\
&\qquad - 44/n^{12} + 100/n^{13} + o(1/n^{13})\\
x\,|\,T^4 &= n - 2 + 1/n + 1/n^2 - 1/n^4 + 1/n^5 + 6/n^6 + 2/n^7 - 28/n^8 - 60/n^9\\
&\qquad + o(1/n^9).
\end{aligned}$$

Les développements ont été faits avec un ordre qui sera utilisé dans la suite, pour le calcul des coefficients A_i.

Puisque le genre de B est quatre, les deux fonctions x et n engendrent le corps des fonctions de B. La fonction n étant invariante par T, x sera lié à n par un polynôme de degré 5 dont les coefficients sont des polynômes en n.

$$x^5 - Sx^4 + Px^3 - Nx^2 + Qx - 1 = 0.$$

En ajoutant les cinq relations liant les $x|T^i$ on obtient l'égalité :

$$P = \sum_{1=0}^{4} (x|T^i).(x|T^{i+1}) + \sum_{1=0}^{4} (x|T^i).(x|T^{i+3}) = 2R.$$

Un calcul analogue montre que

$$N = 2\left(\sum_{1=0}^{5} (x|T^i).(x|T^{i+1}).(x|T^{i+2}) \right) + S^2 - 5R.$$

On trouve alors $S = n^2$

$$\begin{aligned} P &= 2(n^3 - 3n^2 + 5n - 5) \\ N &= n^4 - 5n^3 + 11n^2 - 15n + 5 \\ Q &= -n^3 + 4n^2 - 10n + 10 \end{aligned}$$

$$x^5 - n^2x^4 + 2(n^3 - 3n^2 + 5n - 5)x^3 - (n^4 - 5n^3 + 11n^2 - 15n + 5)x^2 + (-n^3 + 4n^2 - 10n + 10)x - 1 = 0.$$

L'automorphisme T peut se calculer ainsi : les diviseurs des fonctions 1, x, $x|T$, nx, n, x^2, $x(x|T)$, $nx(x|T)$, y, permettent, à l'aide du théorème de Riemann-Roch de montrer l'existence d'une relation linéaire entre ces fonctions. Les coefficients de cette relation sont calculés au moyen des développements ci-dessus.

Ce qui donne :

$$2 - 2x(x|T) - x^2 + x|T - n + nx + nx(x|T) = 0.$$

Équation de la courbe $X_1(25)$ et de la courbe C.

La courbe $X_1(25)$ est un revêtement de degré deux de B. On notera u la fonction $(\phi_{10,5})/(\phi_{10,1})$ de diviseur

$$4 \quad 3 \quad 2 \quad 1 \quad -1 \quad 0 \quad 0 \quad -4 \quad -5 \quad 0.$$

Le diviseur de la fonction $u - 1 = \phi_{1,5}/\phi_{10,1}$ sera donc égal à

$$0 \quad 0 \quad 0 \quad 0 \quad -1 \quad 2 \quad 3 \quad -4 \quad -5 \quad 5.$$

Les formules sur les diviseurs donnent les égalités suivantes :

$$(u-1).(u|T^5-1) = kx/(x|T^2) \quad \text{et} \quad u.(u|T^5) = k'(x|T^3)/(x|T^4).$$

Les constantes k et k' peuvent être déterminées en considérant, par exemple la pointe $\begin{pmatrix}0\\3\end{pmatrix}$. La fonction $(u-1).(u|T^5-1)-1$ est nulle en cette pointe tandis que la fonction $(kx-x|T^2)/x|T^2$ n'est nulle que si k est égal à un. Un calcul à la pointe $\begin{pmatrix}1\\0\end{pmatrix}$ donne, de même, k' égal à -1.

On obtient alors le système suivant :

$$\begin{array}{llll}
(u-1) & .(u|T^5-1) = x/(x|T^2) & u.u|T^5 & = -(x|T^3)/(x|T^4) \\
(u|T-1) & .(u|T^6-1) = (x|T)/(x|T^3) & u|T.u|T^6 & = -(x|T^4)/x \\
(u|T^2-1) & .(u|T^7-1) = (x|T^2)/(x|T^4) & u|T^2.u|T & = -x/(x|T) \\
(u|T^3-1) & .(u|T^8-1) = (x|T^3)/x & u|T^3.u|T^8 & = -(x|T)/(x|T^2) \\
(u|T^4-1) & .(u|T^9-1) = (x|T^4)/(x|T) & u|T^4.u|T^9 & = -(x|T^2)/(x|T^3).
\end{array}$$

Si μ désigne la racine de l'unité égale à $\exp(2i\pi/5)$ et ℓ la fonction u $(u|T^2).(u|T^4).(u|T^6).(u|T^8)$ alors le développement de ℓ en q donne

$$\ell = \ell_0 . \prod_{n=1}^{\infty} ((1-\mu^3 q^n)(1-\mu^{-3}q^n)(1-\mu q^n)^{-1}(1-\mu^{-1}q^n)^{-1})^5.$$

La constante ℓ_0 est égale à $(1+\sqrt{5})^5 2^{-5}$.

Le choix de ℓ montre que $\ell|T = -1/\ell$. On en déduit que $\ell - 1/\ell$ est une fonction de $X_0(25)$, donc un polynôme en n. Les équations ci-dessus donnent les développements en n des $u|T^i$ et donc la valeur de $\ell - 1/\ell$. On a :

$$u = +1/n^4 + 6/n^5 + 17/n^6 + 22/n^7 - 20/n^8 - 153/n^9 - 312/n^{10} + o(1/n^{10})$$

$$u|T = +1/n^3 + 3/n^4 + 1/n^5 - 16/n^6 - 46/n^7 - 29/n^8 + 156/n^9 + 489/n^{10} + o(1/n^{10})$$

$$u|T^2 = -1/n - 1/n^2 + 2/n^4 + 5/n^5 + 11/n^6 + 20/n^7 + 8/n^8 - 93/n^9 - 319/n^{10} + o(1/n^{10})$$

$$u\,|\,T^3 = 1 - 1/n^3 - 3/n^4 - 2/n^5 + 11/n^6 + 37/n^7 + 36/n^8 - 85/n^9 - 352/n^{10} + o(1/n^{10})$$

$$u\,|\,T^4 = n^4 - 5n^3 + 14n^2 - 21n + 16 + 1/n - 4/n^3 - 8/n^4 - 2/n^5 + 15/n^6 + o(1/n^6)$$

$$u\,|\,T^5 = 1 + 1/n^2 + 2/n^3 + 2/n^4 + 1/n^5 + 2/n^6 + 9/n^7 + 16/n^8 - 6/n^9 - 95/n^{10} + o(1/n^{10})$$

$$u\,|\,T^6 = n^5 - 6n^4 + 20n^3 - 39n^2 + 47n - 25 + 1/n + 2/n^2 + 5/n^3 + 6/n^4 - 10/n^5 + o(1/n^5)$$

$$u\,|\,T^7 = -1/n^2 - 2/n^3 - 2/n^4 - 2/n^5 - 7/n^6 - 19/n^7 - 17/n^8 + 48/n^9 + 183/n^{10} + o(1/n^{10})$$

$$u\,|\,T^8 = -n + 1 - 1/n - 1/n^2 - 1/n^3 - 1/n^4 + 2/n^5 + 14/n^6 + 29/n^7 + 4/n^8 - 108/n^9 + o(1/n^9)$$

$$u\,|\,T^9 = 1 + 1/n^5 + 5/n^6 + 9/n^7 - 6/n^8 - 63/n^9 - 111/n^{10} + o(1/n^{10}).$$

On obtient :

$$\ell^2 + \ell.(n^5 - 5n^4 + 15n^3 - 25n^2 + 25n - 11) - 1 = \ell^2 + \ell.(D.n - 11) - 1 = 0$$

où D est égal à $n^4 - 5n^3 + 15n^2 - 25n + 25$.

Le discriminant de ce polynôme en ℓ se met sous la forme :

$$\{(n-1)^4 + 3(n-1)^2 + 1\}^2.d = D^2n^2 - 22Dn + 125$$

où d est égal à $(n-1)^2 + 4$.

Le diviseur de la fonction ℓ est :

$$-5 \quad 5 \quad 5 \quad -5 \quad -5 \quad 5 \quad -5 \quad -5 \quad 5 \quad 5.$$

Le genre de la courbe C permet d'affirmer qu'il existe une fonction m de $X_1(25)$ de puissance cinquième égale à ℓ.

On en déduit aussi que m et n sont liés par la relation suivante :

$$m^2 + (n-1)m - 1 = 0.$$

Ceci définit la courbe C.

A partir des développements ci-dessus nous obtenons une équation de degré dix en u, liant u et n.

$$u^{10} + A_9u^9 + A_8u^8 + A_7u^7 + A_6u^6 + A_5u^5 + A_4u^4 + A_3u^3 + A_2u^2 + A_1u - 1 = 0.$$

Les A_1 sont des polynômes en n dont le degré est déterminé par l'étude des diviseurs des $u|T^i$. Par exemple A_7 est de degré 10 car il contient le terme $(u|T^4).(u|T^6).(u|T^8).(u|T^3+u|T^5+u|T^9)$, ceci nécessite un développement des $u|T^i$ pour $i \neq 4, 6, 8$ à l'ordre 10, tandis que l'ordre respectivement 6, 5, 9 suffit pour $u|T^4$, $u|T^6$, $u|T^8$.

$$A_1 = n^4 - 5n^3 + 15n^2 - 25n + 30$$

$$A_2 = -n^7 + 10n^6 - 51n^5 + 163n^4 - 355n^3 + 520n^2 - 475n + 195$$

$$A_3 = -n^9 + 10n^8 - 51n^7 + 160n^6 - 321n^5 + 351n^4 + 30n^3 - 785n^2 + 1200n - 735$$

$$A_4 = -n^{10} + 15n^9 - 108n^8 + 496n^7 - 1600n^6 + 3772n^5 - 6525n^4 + 8080n^3 - 6650n^2 + 3050n - 360$$

$$A_5 = 3n^{10} - 40n^9 + 274n^8 - 1227n^7 + 3940n^6 - 9405n^5 + 16835n^4 - 22225n^3 + 20650n^2 - 12125n + 3386$$

$$A_6 = -3n^{10} + 40n^9 - 275n^8 + 1239n^7 - 4015n^6 + 9705n^5 - 17673n^4 + 23890n^3 - 22970n^2 + 14200n - 4340$$

$$A_7 = n^{10} - 15n^9 + 110n^8 - 520n^7 + 1750n^6 - 4372n^5 + 8201n^4 - 11410n^3 + 11290n^2 - 7200n + 2265$$

$$A_8 = n^9 - 11n^8 + 64n^7 - 245n^6 + 673n^5 - 1358n^4 + 2010n^3 - 2095^2 + 1400n - 445$$

$$A_9 = -n^5 + 5n^4 - 15n^3 + 25n^2 - 25n + 5.$$

Soit en exprimant les coefficients au moyen de D et d:

$$A_1 = 5 + D$$

$$A_2 = -5 + D[d(3-n) - 7]$$

$$A_3 = -10 + D[4d(n-3) + 31] - D^2 n$$

$$A_4 = 15 + D[9d(-n+3) + 6n - 75] + D^2(-d + 3n + 2)$$

$$A_5 = 11 + D[13d(n-3) + 105 - 18n] + D^2(3d - 4n - 6)$$

$$A_6 = 15 + D[11d(3-n) + 16n - 88] + D^2(-3d + 5 + 4n)$$

$$A_7 = -10 + D[5d(d-3) + 41 - 2n] + D^2(n - 3n)$$

$$A_8 = 5 + D[d(-n+3) - 8 - n] + D^2(n-1)$$

$$A_9 = +5 - Dn.$$

Compte tenu de la forme du discriminant de l'équation de degré deux il paraît judicieux de poser $k = 1 - n$. Les coefficients se simplifient et donnent :

$$A_9 = k^5 + 5k^4 + 5k - 6$$
$$A_8 = -k^9 - 2k^8 - 12k^7 - 21k^6 - 57k^5 - 72k^4 - 116k^3 - 86k^2 - 72k - 6$$
$$A_7 = k^{10} + 5k^9 + 20k^8 + 60k^7 + 140k^6 + 270k^5 + 411k^4 + 506k^3 + 461k^2 + 291k + 100$$
$$A_6 = -3k^{10} - 10k^9 - 50k^8 - 119k^7 - 312k^6 - 518k^5 - 848k^4 - 913k^3 - 889k^2 - 476k - 202$$
$$A_5 = 3k^{10} + 10k^9 + 49k^8 + 115k^7 + 293k^6 + 472k^5 + 735k^4 + 736k^3 + 635k^2 + 272k + 66$$
$$A_4 = -k^{10} - 5k^9 - 18k^8 - 52k^7 - 102k^6 - 178k^5 - 185k^4 - 152k^3 + 47k^2 + 117k + 169$$
$$A_3 = k^9 + k^8 + 7k^7 - k^6 - 2k^5 - 65k^4 - 115k^3 - 226k^2 - 193k - 142$$
$$A_2 = k^7 + 3k^6 + 12k^5 + 23k^4 + 48k^3 + 52k^2 + 50k + 6$$
$$A_1 = k^4 + k^3 + 6k^2 + 6k + 16.$$

Enfin remarquons que la fonction ℓ est une fonction sur $X_1(5)$ égale à $(\mathfrak{P}'(1/5;\tau,1)/\mathfrak{P}'(2/5;\tau,1)$ et que les fonctions m et u sont liées par la relation suivante :

$$u^5 + (m^5 - 3)u^4 + (-m^9 - 2m^8 - 3m^7 - 5m^6 - 6m^5 - 2m^4 + m^3 - m^2 + 3)u^3 + (m^{10} + 2m^9 + 4m^8 + 6m^7 + 10m^6 + 9m^5 + 4m^4 - 2m^3 + 2m^2 - 1)u^2 + (-m^9 - 2m^8 - 3m^7 - 5m^6 - 5m^5 - 2m^4 + m^3 - m^2)u + m^5 = 0.$$

Le discriminant relatif de $\mathbb{Q}(u)$ sur $\mathbb{Q}(m)$ est égal à d^4 où $d = m^4 - 2m^3 + 4m^2 - 3m + 1 = ((m-1)^5 + m^5)/(2m-1)$ et u, m, et d sont liés par la relation :

$$u^5 + [d(m+2) + 5(-m^2 + m - 1)]u^4 + [d^2(-m-6) + d(-15m^3 + 15m^2 - 18m + 9) + 10(-m^2 + m)]u^3 + [d^2(m^2 + 6m + 16) + d(20m^3 - 40m^2 + 49m - 7) + 10(-2m^2 + 2m - 1)]u^2$$
$$[d^2(-m-6) + d(-15m^3 + 15m^2 - 17m + 11) + 5(-3m^2 + 3m - 1)]u + m^5 = 0.$$

Pour terminer donnons la valeur de l'invariant modulaire j en fonction de k :

$$j - 1728 = (k^2 + 4).$$
$$(1 + 3k^2 + k^4)^2(76 - 90k + 25k^2 - 90k^3 + 50k^4 - 18k^5 + 35k^6 + 10k^8 + k^{10})^2/D(k-1).$$

On peut faire la remarque suivante : comme pour l'équation de $X_1(25)$, les coefficients intervenant dans la relation entre j et k sont plus petits, en module, que ceux qui interviennent dans la relation entre j et n.

Corps abéliens de degré 10.

Si n est un entier différent de 1, $\mathbb{Q}(u)$ est une extension abélienne de degré 10 de $\mathbb{Q}$. Nous étudierons le groupe des unités de cette extension dans le cas où D est un nombre premier, et d est sans facteurs carrés. Le discriminant de $\mathbb{Q}(u)$ est alors $D^8 d^5$. Nous noterons respectivement $\mathfrak{U}_{10}$, $\mathfrak{U}_5$, $\mathfrak{U}_2$ les groupes des unités de $\mathbb{Q}(u)$, $\mathbb{Q}(x)$, $\mathbb{Q}(m)$; $U_{a,b\ldots}$ désignera un sous-groupe de $\mathfrak{U}_{10}$ engendré par $a, b\ldots$ et leurs conjugués. Enfin $N_{i,j}$ représente la norme de l'extension de degré i sur l'extension de degré j, et nous noterons U_R le groupe des unités relatives $(N_{10,5}(U_R) = N_{10,2}(U_R) = \pm 1)$. Nous pouvons constater que $N_{10,5}(U_u)$ est d'indice cinq dans $\mathfrak{U}_5$, que $N_{10,5}(\mathfrak{U}_{10}) = \mathfrak{U}_5$ et que $N_{10,2}(U_u)$ est d'indice cinq dans $\mathfrak{U}_2$.

Nous noterons s l'unité relative $u.(u|T).(u|T^5)^{-1}.(u|T^6)^{-1}$.

PROPOSITION 1. — *Le groupe $\mathfrak{U}_2.\mathfrak{U}_5.U_R$ est d'indice 2^4 ou $2^4.5$ dans $\mathfrak{U}_{10}$. Si de plus $\{1-n^2.(D-1)/5\}^{(D-1)/5} \not\equiv 1 \bmod D$, cet indice est égal à 2^4 et il n'y a pas d'unité de Minkowski. Le groupe U_s est contenu dans U_R. Ces deux groupes sont égaux ou bien l'indice de U_s dans U_R est cinq ou $\geqslant 11$.*

En effet, l'application $N_{10,5}$ étant surjective l'indice du groupe $\mathfrak{U}_2.\mathfrak{U}_5.U_R$ dans $\mathfrak{U}_{10}$ ne peut être 1. Il ne peut prendre que les valeurs 2^4 ou $2^4.5$. Cette dernière valeur n'est prise que si la norme $N_{10,2}$ est surjective, c'est-à-dire s'il existe a tel que $m = N_{10,2}(a)$ [7]. Si σ désigne un élément du groupe de Galois de $\mathbb{Q}(u)/\mathbb{Q}$ correspondant à T, alors σ^2 agit trivialement modulo D et donc m est alors, dans ce cas, une puissance cinquième modulo D. Par ailleurs on constate que x modulo D est une racine cinquième de l'unité et est égal à $n^2/5$. Remarquons aussi que D divise $n^{10} - 5^5$. Modulo D, le polynôme irréductible de u sur $\mathbb{Q}$, est égal à $(u^2+u-1)^5$. Dans le corps $\mathbb{Z}/D\mathbb{Z}$, m est égal à $-(n^2/5)u$ et $-1/m$ à $-1-n^2/5$. Il en résulte que m est une puissance cinquième si $(-1/m)^{(D-1)/5} \equiv 1 \bmod D$, ce qui donne la condition de l'énoncé. Les

groupes U_R et U_s ont une structure de $\mathbb{Z}[\mu]$ module libre en posant $\mu|e = \sigma^2(e)$. Il en résulte que $U_R = \mathbb{Z}[\mu].\tau$ et $U_s = \mathbb{Z}[\mu].s$. L'indice de ces sous-groupes est une norme de $\mathbb{Z}[\mu]$ donc égal à cinq ou $\geqslant 11$, à moins qu'il ne soit égal à un.

THÉORÈME 1. — *Il existe une constante c telle que si $|n| > c$ le groupe $U_{u,m,x}$ est d'indice un ou cinq dans le groupe $\mathfrak{U}_{10}$.*

Pour démontrer ce théorème nous utiliserons une inégalité liant régulateur et discriminant. Nous noterons respectivement R_{10} et R_5 les régulateurs des corps $\mathbb{Q}(u)$ et $\mathbb{Q}(x)$. Nous avons la minoration suivante [1] :

$$QR_{10}/R_5 \geqslant 1/C_2[\log (N_{5,1}(\delta)/C_3]^5$$

où C_2, C_3, sont des constantes qu'on peut choisir égales respectivement à $100\sqrt{10}$ et à 1024, δ est le discriminant relatif de $\mathbb{Q}(u)$ sur $\mathbb{Q}(x)$, enfin Q est l'ordre du groupe de torsion de $\mathfrak{U}_{10}/\mathfrak{U}_5$. Les corps étant réels, Q ne peut être qu'une puissance de deux. D'autre part 2 n'est pas ramifié dans $\mathbb{Q}(u)$ et donc $Q = 1$.

Pour estimer les régulateurs nous utiliserons le fait que toutes les fonctions $u, x, m, x|T, \ldots$ ont leur support concentré aux pointes rationnelles et que ces pointes engendrent un groupe d'ordre fini dans la jacobienne de $X_1(25)$. L'ordre de ce groupe est égal à $71.5.641$ ([5], Th. 3.4, p. 158). En utilisant le développement des fonctions $u, x, \ldots$ en fonction de n, on obtiendra un équivalent à $\log |u|$ de la forme $i \log |n|$ où i est l'ordre du zéro ou du pôle de u en P_1. Le groupe de Galois de l'extension $\mathbb{Q}(u)$ sur $\mathbb{Q}$ correspond aux automorphismes T^i qui permutent les pointes.

Le régulateur d'un système de 9 unités sera donc équivalent à $\mathscr{D}.\log^9|n|$ où $\mathscr{D}$ est le déterminant de la matrice 9.9 extraite du tableau formé par les diviseurs. Si on note $D(u,x,\ldots)$ le déterminant construit avec les diviseurs des fonctions $u, x, \ldots$, les calculs donnent :

$$D(u,u|T,u|T^2, \text{et conjugués}) = 71.641.5^3.$$
$$D(u,u|T,u|T^2,u|T^3,m,x,x|T,x|T^2,x|T^3) = 5.71.641.$$
$$D(x,x|T,x|T^2,x|T^3,m,s,s|T,s|T^2,s|T^3) = 2^4.5^5.71.641.$$

Enfin si $t_{u,x,\ldots}$ désigne l'indice de $U_{u,x,\ldots}$ dans $\mathfrak{U}_{10}$, alors R_{10} sera équivalent à $D(u,x,\ldots).\log^9|n|/t_{u,x,\ldots}$. D'autre part R_5 est équivalent à

$71.\log^4|n|$, et $\log(N_{5,1}(\delta))$ est équivalent à $10.\log|n|$. Compte tenu de l'inégalité on en déduit que l'indice de $U_{u,x,m}$ dans $\mathfrak{U}_{10}$ est inférieur à 10.

En utilisant la proposition précédente, il en résulte que l'indice $U_{u,x,m}$ dans $\mathfrak{U}_{10}$ est une norme de $\mathbb{Z}[\mu]$ donc soit égal à un, soit égal à cinq.

La constante c ne paraît pas facile à déterminer exactement : la majoration de l'indice par 10 étant trop voisine de 11, il faut alors évaluer les régulateurs de façon très précise.

Cas particulier où $n = 1$.

Si $n = 1$, les corps engendrés par x et u coïncident. La fonction m prend les valeurs $+1$ et -1 ainsi que la fonction ℓ. On en déduit que la courbe elliptique correspondante a un point d'ordre cinq défini sur $\mathbb{Q}$. Compte tenu de la définition de la fonction ℓ, l'équation de la courbe elliptique correspondante est $y^2 + (1+1/\ell)xy + y/\ell = x^3 + x^2/\ell$ soit si $\ell = -1$, $y^2 - y = x^3 - x^2$.

Cette équation correspond à la courbe $X_1(11)$. En effet cette courbe est de genre 1, ses pointes rationnelles engendrent un groupe d'ordre 5 et les pointes non rationnelles, définies sur le sous-corps réel des racines onzième de l'unité engendrent un groupe d'ordre 25. Il suffit pour le montrer de remarquer que le quotient de $X_1(11)$ par le sous-groupe d'ordre cinq donne la courbe $X_0(11)$, les pointes non rationnelles de $X_1(11)$ ont pour image la pointe à l'infini qui est d'ordre cinq sur $X_0(11)$.

Pour cet exemple, nous pouvons expliquer pourquoi les valeurs de la fonction modulaire x de $X_1(25)$ sont liées aux périodes de Gauss [5] et [8]. Si p_i et q_i sont les dix pointes de $X_1(11)$, $p_i = \begin{pmatrix} 0 \\ i \end{pmatrix}$ et $q_i = \begin{pmatrix} i \\ 0 \end{pmatrix}$ nous choisirons comme fonction x le quotient $(\mathfrak{P}(1/11) - \mathfrak{P}(3/11))/(\mathfrak{P}(3/11) - \mathfrak{P}(5/11))$ et comme fonction y le quotient $(\mathfrak{P}(5/11) - \mathfrak{P}(1/11))/(\mathfrak{P}(5/11) - \mathfrak{P}(4/11))$. Ces fonctions ont comme diviseurs respectivement $-2p_1 + p_3 + p_4$ et $-3p_1 + 2p_3 + p_5$. De même, les diviseurs de $x - 1$ et de $y - 1$ sont respectivement $-2p_1 + p_2 + p_5$ et $-3p_1 + p_2 + 2p_4$. La comparaison des diviseurs de ces fonctions et

leurs valeurs à la pointe q_1, permet de retrouver l'équation de $X_1(11)$ et de déterminer les pointes non rationnelles en faisant un q développement de x et y. On obtient l'équation $y^2 - y = x^2 - x^2$. Les abscisses des multiples de q_1 sont :

$$\begin{aligned}
x(q_1) &= 2+\theta-5\theta^2-\theta^3+2\theta^4 & x(2q_1) &= 1+2\theta-\theta^3\\
x(4q_1) &= -\theta+2\theta^3+\theta^4 & x(8q_1) &= -2\theta+\theta^2+\theta^3\\
x(16q_1) &= 3+14\theta+8\theta^2-5\theta^3-3\theta^4 & x(7q_1) &= 3+3\theta-\theta^2-\theta^3\\
x(14q_1) &= -2-6\theta+14\theta^2+\theta^3-4\theta^4 & x(3q_1) &= -1-\theta+4\theta^2-\theta^4\\
x(6q_1) &= 15-8\theta-17\theta^2+3\theta^3+4\theta^4 & x(12q_1) &= 4-2\theta-4\theta^2+\theta^3+\theta^4
\end{aligned}$$

où $\theta = \exp(2i\pi/11) + \exp(-2i\pi/11)$ est l'une des périodes de Gauss.

La fonction x sur $X_1(25)$ prend la valeur $3\theta - \theta^3 = (\exp(6i\pi/11) + \exp(-6i\pi/11))$ au point de $X_1(25)$ correspondant à $n = 1$ c'est-à-dire au couple $(X_1(11), q_1)$.

Involution et extensions de degré cinq.

PROPOSITION 2. — *Le groupe* $\Gamma_0(25) \cap \Gamma_1(5)$ *est normal dans* $\Gamma_0(5)$, *l'involution* w_{25} *est aussi dans le normalisateur de ce groupe. L'automorphisme* U *de* C *correspondant à l'application* $\tau| \to \tau - 1/5$ *est d'ordre cinq et défini sur* $\mathbb{Q}(\sqrt{5})$, *il transforme la fonction* m *en* $\{-\mu m + (\mu+1/\mu)\}/\{m(\mu+1/\mu)+1/\mu\}$.

L'automorphisme U correspond au produit des trois matrices $\begin{pmatrix} 0 & -1 \\ 25 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 5 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1/25 \\ 1 & 0 \end{pmatrix}$. Les deux fonctions $m + (\mu^2+1/\mu^2)$ et $m - 1/(\mu^2+1/\mu^2)$ s'annulent à la pointe infinie et à son image par T. En comparant leurs diviseurs au diviseur de $m|w_{25}$, on en déduit que $m|w_{25} = (-(\mu^2+1/\mu^2)m+1)/(m+\mu^2+1/\mu^2)$.

Le diviseur de m est invariant par la matrice $\begin{pmatrix} 1 & 0 \\ 5 & 1 \end{pmatrix}$. Cette matrice agira sur m par la multiplication par une puissance de μ. On détermine cette puissance en considérant l'image de la pointe $\begin{pmatrix} 0 \\ 2 \end{pmatrix}$ par U et la relation $m\left(U\begin{pmatrix} 0 \\ 2 \end{pmatrix}\right) = \mu^2 + 1$.

THÉORÈME 2. — *Il existe une fonction* w *modulaire sur* $\Gamma_1(5) \cap \Gamma_0(25)$ *dont l'image par l'automorphisme* U *est* $w|U = 1/(s+\mu^2+1/\mu^2)$.

La fonction $a = \sum_{1=0}^{5} (w \mid U^i)$ *engendre le corps des fonctions de la courbe* $C/\langle U^i \rangle$, *les fonctions* w *et* a *sont liées par la relation suivante :*

$$w^5 + aw^4 - (a(1+\sqrt{5})-10)w^3 + (1+\sqrt{5})(a+5)w^2$$
$$-(a+5/2+\sqrt{5}/2)w + 1 = 0.$$

Démonstration. — Il suffit de poser $w = (m-\mu^2-1)/m(\mu^4-\mu^3)$.

COROLLAIRE — *Si* a *prend des valeurs dans* $\mathbb{Z}$, *l'équation ci-dessus définit une famille de corps abéliens et de degré cinq sur* $\mathbb{Q}(\sqrt{5})$. *Les quatre conjugués de* w *sont donnés par l'action de la matrice* $\begin{pmatrix} 0 & -1 \\ 1 & \mu^2 + 1/\mu^2 \end{pmatrix}$ *et de ses puissances. On obtient quatre unités conjuguées de ces corps.*

Remarquons que le choix de w permet de construire des unités car le support du diviseur de w est contenu dans l'ensemble des pôles de la fonction a. Nous retrouvons ainsi l'exemple de [9].

BIBLIOGRAPHIE

[1] A.-M. BERGÉ, J. MARTINET, Sur les minorations géométriques des régulateurs, Séminaire de Théorie des Nombres (1987-1988), Birkhauser.

[2] H. DARMON, Note on a polynomial of Emma Lehmer (1989), Preprint.

[3] M.-N. GRAS, Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$, Publ. Math. Besançon, fasc. 2 (1977-1978), 1-26 et 1-53.

[4] D. S. KUBERT, Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc., (3), 33 (1976), 193-237.

[5] D. S. KUBERT, S. LANG, Modular Units Springer-Verlag, Comprehensive Studies in Mathematics, 244.

[6] E. LEHMER, Connections between gaussian periods and cyclic units, Math of Computation, (50), 182 (1988), 535-541.

[7] H. W. LEOPOLDT, Über Einheittengruppe und klassen zahl reeller abelscher Zahlerkörper, Abh. Deutsch. Akad. Berlin. Math. Bat. Kl., N° 2 (1953).

[8] O. LECACHEUX, Unités d'une famille de corps de degré 6 liés à la courbe modulaire $X_1(13)$, J. Number Theory, 31 (1989), 54-63.

[9] C. LEVESQUE, Second Canadian Number Theory Association Meeting Août (1989), exposé.

[10] R. SCHOOF et L. C. WASHINGTON, Quintic polynomials and real cyclotomic fields with large class number, Math of Computation, (50), 182 (1988), 541-555.

[11] E. SEAH, L. C. WASHINGTON, H. C. WILLIAMS, The calculation of a large cubic class number field with an application to real cyclotomic field, Math. Comp., 41 (1983), 303-305.

[12] D. SHANKS, The simplest cubic fields. Math, Comp., 28 (1974), 1137-1152.

Manuscrit reçu le 6 mars 1990,
révisé le 25 avril 1990.

Odile LECACHEUX,
Université de Paris VI
UER 47-Mathématiques
Tour 45-46, 5e étage
4, place Jussieu
75252 Paris Cedex 05.