ACTA ARITHMETICA
LXXXVI.3 (1998)

Constructions de polynômes génériques à groupe de Galois résoluble

par

Odile Lecacheux (Paris)

1. Introduction. On sait que les seuls sous-groupes résolubles transitifs du groupe symétrique $\mathbf{S}_5$ sont isomorphes au groupe de Frobenius $\mathbf{F}_{20}$, au groupe diédral D_5 et au groupe cyclique C_5. Nous montrerons comment construire des extensions de degré 5 à groupe de Galois résoluble à l'aide de courbes elliptiques. Dans un premier paragraphe nous utiliserons une courbe elliptique ayant un point de 5-torsion rationnel pour les groupes D_5 et C_5. Puis, dans le paragraphe suivant, nous utiliserons une courbe elliptique ayant un sous-groupe rationnel d'ordre 5 pour construire des extensions à groupe de Galois $\mathbf{F}_{20}$. Reprenant alors un résultat de A. Brumer nous obtenons un polynôme générique pour $\mathbf{F}_{20}$.

1.1. *Groupe de Frobenius.* Rappelons qu'un *groupe de Frobenius* G de degré premier $p \geq 5$ est un sous-groupe transitif de S_p tel que tout élément de G différent de l'identité a au plus un point fixe et qu'il existe un élément ayant un point fixe. Un tel groupe peut s'identifier à un sous-groupe du groupe des transformations affines du corps premier $\mathbb{F}_p$, c'est-à-dire du groupe $A_{\text{ff}}(\mathbb{F}_p) = \{x \mapsto ax + b : a \in \mathbb{F}_p^*,\ b \in \mathbb{F}_p\}$. Il peut aussi s'identifier au produit semi-direct de $\mathbb{F}_p$ par l'unique sous-groupe H d'ordre l divisant $p-1$ de $\mathbb{F}_p^*$. Si $l = 1$ on obtient le groupe cyclique C_p, si $l = 2$ on obtient le groupe diédral D_p. Dans notre cas si $p = 5$, le troisième cas possible correspond à $l = p - 1$ et nous noterons $\mathbf{F}_{20}$ ce groupe qui est aussi égal à $A_{\text{ff}}(\mathbb{F}_5)$.

Nous utiliserons dans la suite les représentations de ces groupes à l'aide des permutations $\sigma = (1, 4, 5, 2)$, de carré $\sigma^2 = (1, 5)(2, 4)$ et $\tau = (1, 2, 3, 4, 5)$. Les deux permutations σ et τ engendrent un groupe isomorphe à $\mathbf{F}_{20}$. Les permutations σ^2 et τ engendrent un groupe isomorphe à D_5.

1991 *Mathematics Subject Classification*: Primary 12F10, 12F05; Secondary 11G05, 14K02.

Key words and phrases: polynômes, théorie de Galois, courbes elliptiques.

1.2. *Polynômes génériques.* Soit G un groupe fini et k un corps de caractéristique nulle.

Définition 1.1. Un polynôme $P(X, n_1, \ldots, n_r) \in k[X, n_1, \ldots, n_r]$ est un *polynôme générique* sur k pour G si

1. comme polynôme en X sur le corps $k(n_1, \ldots, n_r)$, un corps de décomposition de P a un groupe de Galois isomorphe à G,

2. pour tout corps K contenant k et toute extension L/K galoisienne de groupe G, le corps L est le corps de décomposition du polynôme obtenu en spécialisant $P(X, n_1, \ldots, n_r)$ en des valeurs $n_i \in K$.

1.3. *Courbes elliptiques et extensions.* On considère une courbe elliptique E, définie sur k, munie d'une isogénie k-rationnelle ϕ d'ordre p premier, de noyau engendré par A. On notera E' la courbe quotient $E/\langle A\rangle$. Soit

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

une équation de Weierstrass de E' et $P' = (x', y')$ un point de E' dont l'abscisse x' est dans k. Soit P tel que $\phi(P) = P'$ et soit $k(x)$ l'extension engendrée par l'abscisse x de P dans un modèle de Weierstrass de E. Soit $\mathcal{G}$ le groupe de Galois de la clôture galoisienne, sur k, du corps de définition de P et $\mathcal{G} \to Gl_2(\mathbb{F}_p)$ la représentation de $\mathcal{G}$ définie par $\sigma \mapsto \left(\begin{smallmatrix} \pm 1 & 0 \\ b & a \end{smallmatrix}\right)$ où $P^\sigma = \pm P + bA$ et $A^\sigma = aA$. De plus, puisque x est une fonction paire sur E, le groupe de Galois de la clôture galoisienne de $k(x)$ sur k s'identifie à un sous-groupe du quotient de $Gl_2(\mathbb{F}_p)$ par le sous-groupe $\pm I_2$.

Cette construction et le théorème d'irréductibilité de Hilbert permettent de démontrer, si $p = 5$, les résultats suivants :

1. Si A est défini sur k, le groupe de Galois de la clôture galoisienne de $k(x)$ est, pour une infinité de x, le groupe D_5.

2. Si A est défini sur une extension cyclique de degré 4 le groupe de Galois de la clôture galoisienne de $k(x)$ est, pour une infinité de x, le groupe $\mathbf{F}_{20}$. De même, si θ est une fonction paire sur E le groupe de Galois de la clôture galoisienne de $k(\theta(P))$ est $\mathbf{F}_{20}$.

2. Groupe cyclique et diédral. Dans ce paragraphe nous expliciterons la construction à l'aide des équations des courbes elliptiques, montrerons qu'on retrouve le polynôme générique donné par A. Brumer et donnerons des exemples.

2.0.1. *Notations.* Soient E une courbe elliptique définie sur un corps k de caractéristique nulle et A un point de 5-torsion k-rationnel. On notera $A_i = iA$ les multiples de A.

Il existe une unique fonction X sur E telle que $X(A_4) = X(A_1) = 1$, $X(A_2) = X(A_3) = \infty$, $X(A_0) = 0$. Il en résulte alors que

$$\mathrm{div}(X) = 2A_0 - A_2 - A_3, \qquad \mathrm{div}(X-1) = A_1 + A_4 - A_2 - A_3.$$

Si M désigne un point générique de E, on notera Φ l'automorphisme du corps des fonctions de E défini par $f(M) \mapsto f(M+A)$, on notera aussi f_i la $i$ème itérée de f par Φ.

2.0.2. *Equations de E.* Il est alors facile de calculer les diviseurs de X_i et $X_i - 1$; plus précisément, on a

$$\mathrm{div}(X_i) = 2A_{5-i} - A_{2-i} - A_{3-i}, \qquad \mathrm{div}(X_i - 1) = A_{1-i} + A_{4-i} - A_{2-i} - A_{3-i}$$

pour $0 \le i \le 4$.

De l'égalité des diviseurs des fonctions X_i, on déduit les relations suivantes :

$$X_i X_{i+2} = k'(1 - X_{i+1}).$$

En considérant les diviseurs des fonctions X_i, il résulte que le corps des fonctions de E est engendré par X_i et X_{i+1}. Posons $Y = X_1$ et déterminons une relation entre X et Y. Cette relation peut être obtenue en considérant la fonction $\prod_{i=0}^{4} X_i$. Son diviseur est nul : c'est donc une constante que nous noterons $-t$. Exprimons les différentes fonctions X_i à l'aide de X et Y. L'automorphisme Φ étant d'ordre 5, il en résulte que $k' = 1$ et on constate que $\Phi(Y) = (1-Y)/X$. On obtient alors une équation de E, notée E_t,

$$-tXY = (Y-1)(X-1)(X+Y-1).$$

Le changement de variable

$$X = t/x, \qquad Y = 1 - tx/y$$

donne le modèle de Weierstrass E_t habituellement utilisé (cf. Kubert [4])

$$y^2 + (1-t)xy - ty = x^3 - tx^2.$$

Inversement, si on considère la famille de cubiques E_t et si $D = t^5(t^2 - 11t - 1) \neq 0$ on obtient une courbe elliptique de discriminant D, d'invariant

$$j = -\frac{(1 - 12t + 14t^2 + 12t^3 + t^4)}{D}.$$

Dans ce dernier modèle les points de 5-torsion ont pour coordonnées $A = (t, 0)$, $2A = (0, 0)$, $3A = (0, t)$, $4A = (t, t^2)$.

On peut alors expliciter à l'aide de l'automorphisme Φ l'équation de la courbe E'_t quotient de E_t par le groupe engendré par A. Pour cela, remarquons que les fonctions $X - 2$ et $X - Y$ ont respectivement 2 et 3 pôles simples; posons alors

$$X' = 2\prod_{i=0}^{4} \Phi^i(X-2) = 2\frac{(X-2)(X^2+2Xt-1)(2X^2-2Xt-2X+t)}{X(X-1)^2},$$

$$\begin{aligned} Y' &= 4\prod_{i=0}^{4} \Phi^i(X-Y) \\ &= -4\frac{(tX^2+(2X-1)(X-1)^2)((X+1)t-X^2(X-1))R(X,Y)}{X^2(X-1)^3} \end{aligned}$$

où $R(X,Y) = Xt + (X-1)(X+2(Y-1))$.

Une équation de Weierstrass de E'_t est alors

$$\begin{aligned} Y'^2 = X'^3 + 25(1+t^2)X'^2 + (208 + 76t + 252t^2 - 76t^3 + 208t^4)X' \\ + 4(1+t^2)(-3t+4)^2(4t+3)^2. \end{aligned} \tag{2.1}$$

L'équation aux abscisses liant X et X' est

$$\begin{aligned} X^5 + (t-3)X^4 + \left(1 - \tfrac{1}{4}X' - 2t^2 - \tfrac{7}{2}t\right)X^3 + \left(4t + 3 + 5t^2 + \tfrac{1}{2}X'\right)X^2 \\ + \left(-2t^2 - 2 - \tfrac{1}{4}X' - \tfrac{5}{2}t\right)X + t. \end{aligned} \tag{2.2}$$

2.1. *Extension générique à groupe diédral D_5*

Théorème 2.1 (A. Brumer). *Un polynôme générique à groupe de Galois D_5 sur k est*

$$X^5 + (s-3)X^4 + (u-s+3)X^3 + (s^2-s-2u-1)X^2 + uX + s. \tag{2.3}$$

Rappelons les grandes lignes de sa démonstration [2] : soient x_i les racines d'un polynôme $P(X) \in k[X]$ à groupe de Galois D_5 représenté à l'aide des permutations τ et σ. On pose

$$X = \frac{(x_4 - x_2)(x_1 - x_5)}{(x_4 - x_1)(x_2 - x_5)},$$

birapport de quatre racines. On a alors $k(x_3) = k(X)$ ou bien X est dans k. L'action de la permutation τ d'ordre 5 sur X a même formule que Φ : plus exactement, $\tau^2(X) = (1-\tau(X))/X$. L'équation aux abscisses (2.2) et le polynôme (2.3) dont les racines sont les $\tau^i(X)$ sont identiques en posant $s = t$ et $X' = -4u - 8 - 8t^2 - 10t$.

Ceci prouve le corollaire suivant :

Corollaire 2.2. *Un polynôme générique $P(X,s,u)$ pour D_5 sur un corps k est donné par l'équation aux abscisses d'une courbe elliptique E définie sur $k(s)$ munie d'un point de 5-torsion $k(s)$-rationnel.*

2.2. *Extensions de degré* 5 *à groupe cyclique* C_5

THÉORÈME 2.3. *Toute extension galoisienne* L *de* $\mathbb{Q}$ *à groupe de Galois cyclique* C_5 *est engendrée par les coordonnées d'un point* P *d'une courbe elliptique* E *définie sur* $\mathbb{Q}$ *munie d'un point* A *de* 5*-torsion* $\mathbb{Q}$*-rationnel dont l'image* P' *dans le quotient* $E/\langle A\rangle$ *est* $\mathbb{Q}$*-rationnel. Le point* P *est ou bien de* 25*-torsion, ou bien d'ordre infini.*

Preuve. Reprenons la construction et les notations du paragraphe précédent. Si l'extension $\mathbb{Q}(x_i)$ est cyclique, $(X, \tau(X)) \in E_t(\mathbb{Q}(x_3))$ et donc son image dans E_t' est dans $\mathbb{Q}$.

Si P est d'ordre fini égal à e, ses cinq conjugués sont du même ordre donc $e \neq 2, 3$. L'extension $\mathbb{Q}(x_i)$ ne contient pas de racines de l'unité $\neq \pm 1$ donc le groupe engendré par P est stable par le groupe de Galois. Le couple (E, P) correspond alors à un point rationnel de la courbe $Y_0(5e)$. La seule possibilité est $e = 5$ si le corps de base est $\mathbb{Q}$. Dans ce cas on a $5P = A$.

On sait alors que ce cas correspond à la famille de corps quintiques suivante (cf. [6]) :

$$\begin{aligned}X^5 &+ (m^5-3)X^4 + (-m^9-2m^8-3m^7-5m^6-6m^5-2m^4+m^3-m^2+3)X^3\\ &+ (m^{10}+2m^9+4m^8+6m^7+10m^6+9m^5+4m^4-2m^3+2m^2-1)X^2\\ &- m^2(m^7+2m^6+3m^5+5m^4+5m^3+2m^2-m+1)X + m^5.\end{aligned}$$

Soit avec les notations précédentes :

$$s = m^5 \quad \text{et} \quad u = -m^2(m^7+2m^6+3m^5+5m^4+5m^3+2m^2-m+1)$$

et la courbe

$$y^2 + (1-m^5)xy - m^5y = x^3 - x^2m^5.$$

2.3. *Familles de courbes elliptiques de rang* ≥ 1. Il existe des exemples de familles paramétrées d'extensions cycliques de degré 5; explicitons les familles de courbes elliptiques dont l'existence est donnée par le théorème 2.3.

2.3.1. EXEMPLE 1. E. Lehmer [7] et R. Schoof–L. Washington [8] ont étudié la famille de corps définie par les polynômes

$$\begin{aligned}X^5 - n^2X^4 + 2(n^3-3n^2+5n-5)X^3 - (n^4-5n^3+11n^2-15n+5)X^2&\\ + (-n^3+4n^2-10n+10)X - 1&\end{aligned}$$

de discriminants

$$D = (-7+10n-5n^2+n^3)^2(n^4-5n^3+15n^2-25n+25)^4.$$

Notons $d = (n^4-5n^3+15n^2-25n+25)$ et $s = -7+10n-5n^2+n^3$, les deux facteurs premiers du discriminant.

Si x est une racine on vérifie que

$$z = \frac{x^2 - nx + n - 2}{(n-2)x + 1}$$

est aussi racine, ce qui permet de déterminer l'action de τ en posant

$$\tau(x_1) = x_2 = \frac{x_1^2 - nx_1 + n - 2}{(n-2)x_1 + 1}.$$

Si

$$W = \frac{(x_4 - x_2)(x_5 - x_1)}{(x_4 - x_1)(x_5 - x_2)}$$

alors W vérifie l'équation

$$\begin{aligned} W^5 + (n^3 - 10 - 5n^2 + 10n)W^4 + (-13n^3 + 5n^4 - 5n + 15n^2 - n^5 - 10)W^3 \\ + (-160n + 95 - 8n^5 + 35n^4 + 155n^2 + n^6 - 91n^3)W^2 \\ + (-20 - n^5 - 12n^3 + 5n^4 + 10n^2 + 5n)W - 7 + 10n - 5n^2 + n^3. \end{aligned}$$

Posons

$$u = -n^5 + 5n^4 - 12n^3 + 10n^2 + 5n - 20.$$

On obtient, pour cet exemple, les valeurs de s et u polynôme générique du théorème 2.3.

Cette famille de corps est obtenue avec la famille de courbes elliptiques

$$\begin{aligned} y^2 - xy(n-2)(n^2 - 3n + 4) - (n^3 - 5n^2 + 10n - 7)y \\ = x^3 - x^2(n^3 - 5n^2 + 10n - 7) \end{aligned} \tag{2.4}$$

en prenant l'image inverse du point de coordonnées

$$\begin{aligned} x' &= -8n^6 + 84n^5 - 380n^4 + 950n^3 - 1350n^2 + 1000n - 250, \\ y' &= 4(n^4 - 5n^3 + 15n^2 - 25n + 25)^2 \end{aligned}$$

dans le modèle donné en (2.1).

La courbe (2.4) a un discriminant égal à

$$(n^2 - 5n + 5)(n^4 - 5n^3 + 15n^2 - 25n + 25)(n^3 - 5n^2 + 10n - 7)^5.$$

Notons le point rationnel Q d'ordre infini sur la courbe (2.4) :

$$Q = (x = n - 1, y = n - 2).$$

2.3.2. Exemple 2. Dans [9] et [10] G. Smith donne une méthode pour déterminer un polynôme générique pour les extensions cycliques de degré 5. Après simplification on obtient

$$P_{C_5}(X) = X^5 + cX^3 + dX^2 + eX + f$$

où

$$\begin{aligned} d_1 &= (u^2 - v^2 + uv)^2 + 5(u^2 + v^2 + 1), \\ c &= -50d_1, \quad d = 500d_1, \\ e &= 625d_1(d_1 - 4u^2 - 4v^2 - 8), \\ f &= -500d_1(d_1 + 10uv(u^2 - v^2 + uv) - 10). \end{aligned}$$

Le discriminant de P_{C_5} est égal à

$$2^{12}5^{16}A^2B^2d_1^4$$

où

$$\begin{aligned} A &= (7v - u)(u^2 + uv - v^2)^2 + 25v^2(u + v), \\ B &= (7u + v)(u^2 + uv - v^2)^2 + 25u^2(u - v). \end{aligned}$$

On pose $t = B/A$ et on considère les courbes E_t et E'_t.

La courbe E_t a un discriminant égal à

$$125d_1(u^2 + 4uv - v^2)(u^2 + uv - v^2)^2A^5/B^7$$

car

$$A^2 + 11AB - B^2 = 125d_1(u^2 + 4uv - v^2)(u^2 + uv - v^2)^2.$$

L'extension cyclique est alors le corps de définition du point P de E_t dont l'image dans E'_t (modèle (2.1)) est le point de coordonnées

$$\begin{aligned} x' = \{&2(u^2 - v^2 + uv)^6 + 5(u^2 + v^2) - 10(u + v)(u - 3v)(3u + v)(u - v) \\ &- 5(u^4 + v^4) - 25(u^2 + v^2)(2u + v)^2(u - 2v)^2\}/A^2, \\ y' = {}&2^25^3d_1^2(u^2 + uv - v^2)^5/A^3. \end{aligned}$$

3. Polynômes à groupe de Galois $\mathbf{F}_{20}$

3.1. *Isogénies.* On considère la courbe elliptique E_p d'équation

$$y^2 - \frac{d}{4}(x^2 + 1) = \frac{1}{2}L(x)L'(x)$$

où $L(x) = x^2 - px - 1$, L' la dérivée de L en x et $d = p^2 + 4$ le discriminant de L.

Soient t et $-1/t$ les deux racines de L et s tel que

$$s^2 = \frac{d}{4}(t^2 + 1) = \frac{d^{3/2}}{4}t.$$

Il est facile de voir que l'extension $\mathbb{Q}(s)/\mathbb{Q}(p)$ est cyclique, de degré 4 et qu'un générateur λ du groupe de Galois de $\mathbb{Q}(s)/\mathbb{Q}(p)$ peut être défini par $s \mapsto -s/t$. On vérifie que les points $(t, \pm s)$ et $(-1/t, \pm s/t)$ sont sur la courbe E_p et que la droite passant par les points (t, s) et $(-1/t, -s/t)$ est tangente en $A = (t, s)$ à la courbe E_p. Il est alors facile de montrer que le point A engendre un sous-groupe d'ordre 5 stable par le groupe de Galois de $\mathbb{Q}(s)/\mathbb{Q}$.

On note E'_p la courbe quotient de E_p par le groupe engendré par A.

Si $M = (x, y)$ est un point générique de E_p l'abscisse x_{M+A} de $M + A$ est

$$x_{M+A} = \frac{y^2 + (d/4)(t^2+1) - 2ys}{(x-t)^2} - x - t - \frac{1}{4}d + \frac{3}{2}p. \tag{3.1}$$

Il en résulte que

$$\sum_{i=0}^{4} x_{M+iA} = x + 2p + d^2\frac{px+2}{L^2} + d\frac{x(p+2) + (p^2-p+6)}{L}.$$

Posons $rd + 5p/2 = \sum_{i=0}^{4} x_{M+iA}$ et $l = L/d$; alors l, p, r sont liés par la relation

$$l^5 + (-r^2d + 2p + 17/4)l^4 + (3rd + p^2 + 13p/2 + 5)l^3 + (rd + 11p/2 - 8)l^2 + (p-6)l - 1.$$

3.2. *Extension générique à groupe de Galois* $\mathbf{F}_{20}$

THÉORÈME 3.1. *Soit k un corps de caractéristique nulle. Un polynôme générique $P(X, r, p)$ à groupe de Galois $\mathbf{F}_{20}$ sur k est*

$$X^5 + (-r^2d + 2p + 17/4)X^4 + (3rd + d + 13p/2 + 1)X^3 + (rd + 11p/2 - 8)X^2 + (p-6)X - 1$$

où $d = p^2 + 4$.

Preuve. Soit K un corps contenant k et $K' = K(x_3)$ une extension de degré 5 de K à groupe de Galois $\mathbf{F}_{20}$.

Nous utiliserons la représentation de $\mathbf{F}_{20}$, à l'aide des permutations, donnée dans l'introduction.

Reprenons les notations précédentes :

$$X = \frac{(x_4 - x_2)(x_1 - x_5)}{(x_4 - x_1)(x_2 - x_5)}, \quad Y = X^\tau \quad \text{et} \quad -t = \prod_{i=0}^{4} X^{\tau^i}.$$

Il est facile de vérifier que

$$X^\sigma = \frac{(x_2 - x_4)(x_5 - x_1)}{(x_2 - x_1)(x_5 - x_4)}, \quad Y^\sigma = \frac{(x_4 - x_1)(x_2 - x_3)}{(x_4 - x_3)(x_2 - x_1)}.$$

Il en résulte que

$$X^\sigma = X/(X-1), \quad Y^\sigma = (Y-1)/(X+Y-1),$$
$$t^\sigma = -1/t, \quad X'^\sigma = X'/t^2, \quad Y'^\sigma = -Y'/t^3.$$

On pose $T = X.X^\sigma$, $p = t - 1/t$, $d = p^2 + 4$ et $X' + X'^\sigma = r_1(p^2 + 4)$.

Il en résulte que r_1 et $p \in K$ et T, r_1, p sont liés par la relation

$$T^5-(-p+6)T^4+(-dr_1/2-2d-11p/2+8)T^3+(3dr_1/2+7d+13p/2+1)T^2 \\ + (r_1^2 d/4 + 2r_1 d + 4d - 2p - 17/4)T + 1.$$

Si on pose $T = -1/l$, $r_1 = 2r - 4$, on retrouve le polynôme construit avec la courbe elliptique E_p.

Ce polynôme est générique sur k : en effet, il suffit de montrer qu'il existe x_3 tel que $K' = K(x_3)$ et $T \notin K$. Si $T \in K$, alors $T = T^\tau$ et $T^5 = -1$. Si $X = Y$, alors X est racine de $X^2 + X - 1$ et on conclut avec le même argument que pour le cas diédral. Si $X \neq Y$, alors $X = Y/(Y-1)$, ce qui est incompatible avec $T^5 = -1$.

Remarque 3.1. Le corps de plus petit discriminant ([5]) à groupe de Galois $\mathbf{F}_{20}$, ayant une seule place réelle, est ainsi obtenu pour $p = 3$, $r = -1/2$ et le polynôme

$$X^5 + 7X^4 + 14X^3 + 2X^2 - 3X - 1.$$

Il est aussi obtenu avec $p = -3$, $r = -3/2$ et le polynôme

$$X^5 - 31X^4 - 64X^3 - 44X^2 - 9X - 1.$$

Remarque 3.2. Par un choix convenable de p et r on peut obtenir des polynômes à coefficients entiers et, puisque le terme constant est 1, les extensions de degré 5 sont engendrées par des unités paramétrées. Cette possibilité résulte des propriétés du diviseur de L et du type de mauvaise réduction de E_p.

Remarque 3.3. L'équation liant les abscisses des points de E_p et de E'_p donne aussi un polynôme générique pour $\mathbf{F}_{20}$; le terme constant est différent de 1 mais les coefficients sont de degré 1 en x_2.

Références

[1] A. A. Bruen, C. Jensen and N. Yui, *Polynomials with Frobenius groups of prime degree as Galois groups II*, J. Number Theory 24 (1986), 305–359.

[2] A. Brumer, preprint.

[3] D. S. Dummit, *Solving solvable quintics*, Math. Comput. 57 (1991), 387–401.

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

[5] S. Kwon et J. Martinet, *Sur les corps résolubles de degré premier*, J. Reine Angew. Math. 375–376 (1987), 12–23.

[6] O. Lecacheux, *Unités d'une famille de corps liés à la courbe* $X_1(25)$, Ann. Inst. Fourier (Grenoble) 40 (1990), 237–253.

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

[8] R. Schoof and L. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, ibid., 543–556.

[9] G. W. Smith, *Some polynomials over* $\mathbb{Q}(t)$ *and their Galois groups*, Ph.D. thesis, University of Toledo, 1993.

[10] —, *Generic cyclic polynomials of odd order*, Comm. Algebra 19 (1991), 3367–3391.

Institut de Mathématiques
Université P. et M. Curie
46-56, 5ème étage, Boîte 247
4 Place Jussieu
75252 Paris Cedex 05, France
E-mail: ol@ccr.jussieu.fr

Reçu le 20.5.1997
et révisé le 9.2.1998 (3190)