UNIVERSITAT DE BARCELONA

FACULTAT DE MATEMÀTIQUES

[Groupe des représentations de M12

$\tilde{M}_{12}$ COMME GROUPE DE GALOIS SUR ϕ

by

P. BAYER, P. LLORENTE, N. VILA

PRE–PRINT N.º 36

ENERO 1986

$\tilde{M}_{12}$ comme groupe de Galois sur $\mathbb{Q}$

P. Bayer, P. Llorente, N. Vila

Introduction

Soit $\tilde{M}_{12}$ l'unique extension non triviale du groupe de Mathieu M_{12}, de noyeau $Z/2Z$. D'après la réalisation de M_{12} comme groupe de Galois sur $\mathbb{Q}[T]$ donnée par Matzat dans [2] , on peut considérer le problème de plongement lié à la réalisation de $\tilde{M}_{12}$ comme groupe de Galois. En utilisant la formule de Serre sur la trace [5] , on prouve qu'il y a des spécialisations de T pour lesquelles ce problème de plongement sur $\mathbb{Q}$ a une réponse affirmative. Ceci donne que $\tilde{M}_{12}$ et, d'ailleurs, toute extension centrale du groupe M_{12}, se réalise comme groupe de Galois sur le corps des rationnels.

1. Problème de plongement associé à $\tilde{M}_{12}$

Soit $f(T,X) = \sum_{i=0}^{12} s_{12-i} X^i$ le polynôme irreductible sur $\mathbb{Q}[T]$ donné par

$s_0 = 1$
$s_1 = 2^2 5^2$
$s_2 = 2\ 3^4\ 5^2$
$s_3 = 2^2\ 3^3\ 5^2\ 31$
$s_4 = 3^4\ 5^2\ 439$
$s_5 = 2^3\ 3^6\ 5^4$
$s_6 = -\ 2^2\ 3^6\ 5^3\ 29$
$s_7 = -\ 2^3\ 3^7\ 5^3\ 7^2$
$s_8 = 3^9\ 5^3\ 41$
$s_9 = 2^2\ 3^9\ 5^4\ 23$
$s_{10} = -\ 5^4\ (2\ 3^9\ 13 + 5^6\ T)$
$s_{11} = 2^2\ 3^{12}\ 5^4$
$s_{12} = 3^{12}\ 5^4$.

D'après Matzat [2] , on sait que le groupe de Galois de ce polynôme sur $\mathbb{Q}(T)$, $G_{\mathbb{Q}(T)}(f(T,X))$, est isomorphe au groupe de Mathieu M_{12}. En spécialisant T à valeurs entières $t \equiv 1 \pmod{66}$, on a aussi que le groupe de Galois $G_{\mathbb{Q}}(f(t,X))$ est isomorphe à M_{12} (cf. [2]).

Soit $x = x_T$ une racine de $f(T,X)$ dans une clôture algébrique $\overline{\mathbb{Q}(T)}$ de $\mathbb{Q}(T)$. Soit $E = \mathbb{Q}(T,x)$, et soit N la clôture galoisienne de E dans $\overline{\mathbb{Q}(T)}$.

L'action de M_{12} sur les racines de $f(T,X)$ nous donne une représentation de permutation de degré 12 , $\rho : M_{12} \longrightarrow A_{12}$, étant A_{12} le groupe alterné.

Les groupes A_{12} et M_{12} ont $\mathbb{Z}/2\mathbb{Z}$ comme groupe des multiplicateurs de Schur. On note a_{12}, resp. m_{12}, les éléments non nuls de $H^2(A_{12}, \mathbb{Z}/2\mathbb{Z})$, resp. de $H^2(M_{12}, \mathbb{Z}/2\mathbb{Z})$; et $\tilde{A}_{12}$, resp. $\tilde{M}_{12}$, les extensions centrales correspondantes:

$$1 \to \mathbb{Z}/2\mathbb{Z} \longrightarrow \tilde{A}_{12} \xrightarrow{\varphi} A_{12} \longrightarrow 1$$

$$1 \to \mathbb{Z}/2\mathbb{Z} \longrightarrow \tilde{M}_{12} \longrightarrow M_{12} \longrightarrow 1 \ .$$

Proposition 1. Soit res : $H^2(A_{12}, Z/2Z) \longrightarrow H^2(M_{12}, Z/2Z)$ l'homomorphisme de restriction induit par ρ. On a $\mathrm{res}(a_{12}) = m_{12}$.

Démonstration. L'extension $N/\mathbb{Q}(T)$ a deux points de ramification η et ∞ (cf. [2]). Soit $\tau \in G(N/\mathbb{Q}(T))$ un générateur d'un groupe d'inertie d'un diviseur premier de ∞ dans N. On a que $\rho(\tau^5)$ est un produit de six transpositions disjointes. Tout élément $b \in \tilde{A}_{12}$ tel que $\varphi(b) = \rho(\tau^5)$ a ordre quatre, car on peut voir que b^2 est l'élément non trivial du noyeau de φ. Ceci montre que $\mathrm{res}(a_{12})$ ne peut pas être trivial.

Soit $S = \left\{ t \in Z \mid t \equiv 1 \pmod{66} \right\}$. Pour chaque $t \in S$, soient $E_t = \mathbb{Q}(x_t)$ et N_t la clotûre galoisienne de E_t dans $\bar{\mathbb{Q}}$. Nous considérons les problèmes de plongement donnés par:

$$\begin{array}{ccccccccc} & & & & G_{\mathbb{Q}(T)} & & & & \\ & & & & \downarrow \pi & & & & \\ 1 \to Z/2Z & \to & \tilde{M}_{12} & \to & M_{12} & \to & 1, & & \end{array} \qquad \begin{array}{ccccccc} & & & & G_{\mathbb{Q}} & & \\ & & & & \downarrow \pi_t & & \\ 1 \to Z/2Z & \to & \tilde{M}_{12} & \to & M_{12} & \to & 1, \end{array}$$

où $G_{\mathbb{Q}(T)}$, $G_{\mathbb{Q}}$ désignent les groupes de Galois absolus correspondants, et π, π_t les projections associées aux réalisations de M_{12} définies par N et N_t.

L'obstruction à chacun de ces deux problèmes de plongement est égale à inf (m_{12}), resp. $\inf_t(m_{12})$, où

$$\inf : H^2(M_{12}, Z/2Z) \longrightarrow H^2(G_{\mathbb{Q}(T)}, Z/2Z),$$

$$\inf_t : H^2(M_{12}, Z/2Z) \longrightarrow H^2(G_{\mathbb{Q}}, Z/2Z)$$

sont les homomorphismes d'inflation induits par π et π_t, respectivement.

On va voir d'abord que le premier problème de plongement n'a pas

de solution.

Proposition 2. $\inf(m_{12}) \neq 0$.

Démonstration. Soit $r_1 = r_1(t)$ le nombre de racines réelles de $f(t,X)$, $t \in S$. Soit $\gamma \in M_{12} \simeq G(N_t/\mathbb{Q})$ le générateur, induit par la conjugaison complexe, d'un groupe de Galois local à l'infini. L'obstruction locale à l'infini, $\inf_t(m_{12})_\infty$, est nulle si et seulement si il y a un élément d'ordre deux dans l'anti-image de $\rho(\gamma)$ par φ ; c'est à dire, si et seulement si $r_1 \equiv 4 \pmod 8$. On peut constater que $r_1(t) = 4$ si $t \geq -197$, et que $r_1(t) = 0$ si $t < -197$. Donc $\inf(m_{12})$ ne peut pas être trivial.

Néanmoins on peut se demander si le problème de plongement sur $\mathbb{Q}$ a des solutions pour certaines valeurs de $t \geq -197$. Pour le savoir, on va utiliser la formule de Serre sur la trace (cf. [5]) qui, dans notre cas, nous dit:

Théorème (Serre). *Soit* $w(t) = w(\mathrm{Tr}_{E_t/\mathbb{Q}}(X^2))$ *l'invariant de Witt de la forme quadratique* $\mathrm{Tr}_{E_t/\mathbb{Q}}(X^2)$, *alors on a* $\inf_t(m_{12}) = w(t)$.

2. Calcul des facteurs invariants de $\mathrm{Tr}(X^2)$

Soit $B = (b_{ij}) \in \mathcal{M}_{12}(\mathbb{Q}[T])$, où $b_{ij} = b_{ij}(T) = \mathrm{Tr}_{E/\mathbb{Q}(T)}(x^{i+j})$, la matrice de la forme bilinéaire $\mathrm{Tr}_{E/\mathbb{Q}(T)}(XY)$ relative à la base $1, x, \ldots, x^{11}$. D'après les formules de Newton:

$$\mathrm{Tr}(1) = 12$$

$$\mathrm{Tr}(x^i) = \begin{cases} -\sum_{j=1}^{i-1} \mathrm{Tr}(x^{i-j})s_j - i\,s_i & \text{si } 0 \leq i \leq 12 \\ -\sum_{j=1}^{12} \mathrm{Tr}(x^{i-j})s_j & \text{si } 12 \leq i \leq 22, \end{cases}$$

on obtient les termes de la matrice B.

En faisant par exemple $t = 1$, quelques termes de la matrice spécialisée $B_{(1)}$ ont déjà environ une trentaine de chiffres. Étant donné que pour déterminer $w(t)$ il faut diagonaliser cette matrice, on va d'abord étudier son discriminant et ses facteurs invariants, afin de débarrasser les calculs.

Proposition 3. Soit $\mathcal{O}_E$ la fermeture intégrale de $\mathbb{Q}[T]$ dans E. Soient $\mathcal{I} = \mathcal{I}(\mathcal{O}_E/\mathbb{Q}[T])$ l'ideal discriminant, et $d(T)$ le discriminant du polynôme $f(T,X)$. On a:

i) $\mathcal{I} = (d_1(T)^6)$, où $d_1(T) = 5^{15}\, T^2 - 2^{22}\, 3^{18}$,

ii) $d(T) = 2^{12}\, 3^{12}\, 5^{44}\, d_1(T)^6$,

iii) $\mathcal{O}_E = \mathbb{Q}[T,x]$.

Démonstration . Soit $\mathcal{P}$ l'unique ideal de $\mathbb{Q}[T]$ ramifié dans E. Soit $L = E(\sqrt{5})$. D'après Matzat on sait que la décomposition de $\mathcal{P}$ en ideals premiers dans L est donnée par $\mathcal{P} = \mathcal{P}_1^4\, \mathcal{R}_1\, \mathcal{P}_2^4 \mathcal{R}_2$, avec $\deg(\mathcal{P}_i) = 2$ et $\deg(\mathcal{R}_i) = 4$ pour $i = 1, 2$. Étant L un corps de genre zéro, ou peut choisir des générateurs $q_i(X)$, $r_i(X)$ des ideaux $\mathcal{P}_i$, $\mathcal{R}_i$, respectivement, de sorte que

$$g(T,X) = \frac{1}{2}\,(q_1(X)^4\, r_1(X) + q_2(X)^4\, r_2(X)\,) - TX^2 \quad ,$$

où $g(T,X) = 5^{-12}\, f(T, 5X)$.

La connaissance explicite de ces polynômes permet le calcul de i).

Notons $x_1 = 5^{-1}\, x$ une racine de g. On a

$$d(g(T,X)) = N_{E/\mathbb{Q}(T)}\ (g'(T,x_1)) = 2^{12}\, 3^{-12}\, 5^{20} N_{E/Q(T)}(q_1(x_1)q_2(x_1))^3 \ .$$

Le polynôme $h(X) = q_1(X)\, q_2(X)$ est unitaire, à coefficients rationnels, et de degré 4. Soient ξ_i les racines de $h(X)$ dans $\bar{\mathbb{Q}}$, alors

$N(h(x_1)) = \prod_{i=1}^{4} g(T, \xi_i)$. Étant le coefficient de T^4 égal à $3^8\, 5^{-6}$ on obtient ii), car $d(T) = 5^{132}\, d(g(T,X))$.

Maintenant, iii) est clair.

Pour déterminer les facteurs invariants de la matrice B nous utiliserons le

Lemma 4. Soit $\mathcal{O}$ un anneau principal et K son corps des fractions. Soit E/K une extension séparable de degré n, et $\mathcal{O}_E$ la fermeture intégrale de $\mathcal{O}$ dans E. Soient α_i, $1 \leq i \leq n$, les facteurs invariants de la matrice $B = (\mathrm{Tr}_{E/K}(x^{i+j}))$, étant $x \in \mathcal{O}_E$ un générateur de l'extension E/K. On a:

i) α_n est égal à l'annulateur de $\mathcal{O}$-module $\Omega(\mathcal{O}[x]/\mathcal{O})$ des $\mathcal{O}$-différentielles de l'anneau $\mathcal{O}[x]$.

ii) Soit $\mathfrak{d} = \mathfrak{D}(\mathcal{O}_E/\mathcal{O})$ l'idéal discriminant et $\mathrm{rad}\, \mathfrak{d} = \mathfrak{p}_1 \ldots \mathfrak{p}_m$. Dans le cas modérément ramifié et monogène, c'est à dire si $\mathcal{O}_E = \mathcal{O}[x]$, on a

$$\alpha_i = \mathfrak{p}_1^{\varepsilon_1} \ldots \mathfrak{p}_m^{\varepsilon_m},\ 1 \leq i \leq n,\ \text{où}\ \varepsilon_j = 1\ \text{si}\ v_{\mathfrak{p}_j}(\mathfrak{d}) > n - i\ \text{et}\ \varepsilon_j = 0\ \text{sinon.}$$

Démonstration. i) Soit $f(X) \in \mathcal{O}[X]$ le polynôme minimal de x. Pour simplifier, désignons par $\mathcal{O}_f$ l'anneau $\mathcal{O}[x]$. Considérons la codifférente de $\mathcal{O}_f$ sur $\mathcal{O}$ donnée par

$$\mathcal{O}_f^* = \left\{ \omega \in \mathcal{L}(E|K) \quad | \quad \omega(\mathcal{O}_f) \subset \mathcal{O} \right\} .$$

La matrice B s'interprète alors comme la matrice associée à l'application linéaire $\mathcal{O}_f \hookrightarrow \mathcal{O}_f^*$ induite par la trace, donc α_n est l'annulateur du $\mathcal{O}$-module $\mathcal{O}_f^*/\mathcal{O}_f$. Compte tenue de la proposition 11, § 6, Ch. III de [4], on a les isomorphismes de $\mathcal{O}$-modules suivants

$$\mathcal{O}_f^* / \mathcal{O}_f \simeq \mathcal{O}'[X]/(f, f') \simeq \Omega(\mathcal{O}_f/\mathcal{O}) ,$$

d'où l'affirmation i).

ii) Dans le cas monogène, on sait que la différente $\mathfrak{d} = \mathfrak{d}(\mathcal{O}_E/\mathcal{O})$ est égale à l'idéal principal engendré par f'(x). Ceci permet d'écrire l'isomorphisme de $\mathcal{O}$-modules

$$\mathcal{O}_f^* / \mathcal{O}_f \simeq \mathcal{O}_E/\mathfrak{d} ,$$

d'où le résultat.

Corollaire 5. Les facteurs invariants α_i sur $\mathbb{Q}[T]$ de la matrice $B = (Tr_{E/\mathbb{Q}(T)}(x^{i+j}))$ sont égaux à

$$\alpha_i = \begin{cases} 1 & \text{si} \quad 1 \leq i \leq 6 \\ d_1(T) & \text{si} \quad 7 \leq i \leq 12 , \end{cases}$$

où $d_1(T) = 5^{15} T^2 - 2^{22} 3^{18}$ est donné comme dans la proposition 3.

Pour chaque entier $t \in S$, il est clair que le déterminant de la matrice spécialisée $B_{(t)} = (Tr_{E_t/\mathbb{Q}}(x_t^{i+j}))$ est égal à

$$d(t) = 2^{12} 3^{12} 5^{44} d_1(t)^6 .$$

On va étudier les facteurs invariants de cette matrice dans la proposition suivante.

Proposition 6. Les facteurs invariants $\alpha_{i,t}$ sur $\mathbb{Z}$ de la matrice $B_{(t)}$ sont égaux à:

$$\alpha_{1,t} = 2 \qquad \alpha_{7,t} = 2 \quad 5^4 \quad d_1(t)$$

$$\alpha_{2,t} = 2 \quad 5^2 \qquad \alpha_{8,t} = 2 \quad 5^4 \quad d_1(t)$$

$$\alpha_{3,t} = 2 \quad 5^2 \qquad \alpha_{9,t} = 2 \quad 5^5 \quad d_1(t)$$

$$\alpha_{4,t} = 2 \quad 5^2 \qquad \alpha_{10,t} = 2 \quad 5^6 \quad d_1(t)$$

$$\alpha_{5,t} = 2 \quad 5^3 \qquad \alpha_{11,t} = 2 \quad 5^6 \quad d_1(t)$$

$$\alpha_{6,t} = 2 \quad 5^4 \qquad \alpha_{12,t} = 2 \quad 3^{12} \quad 5^6 \quad d_1(t) \ .$$

Démonstration. On désigne par $\alpha_{i,t,p}$ les facteurs invariants sur $\mathbb{Z}_p$ de la matrice $B_{(t)}$. Soient $B_i^{\nu}(T)$ les mineurs d'ordre ν de la matrice B. Dans le cas p = 2, il faut seulement observer que $\alpha_{1,t,2} = 2$, pour tout t.

A l'aide de l'ordinateur, on a calculé les facteurs invariants de $B_{(1)}$ pour p = 3, et on a obtenu que $\alpha_{11,1,3} = 1$. Ceci nous dit qu'il existe un mineur $B_{i_o}^{11}(T)$ tel que $B_{i_o}^{11}(1) \not\equiv 0 \pmod 3$, donc $\alpha_{11,t,3} = 1$ pour tout $t \in S$.

Le résultat dans le cas p = 5 a été obtenu en estimant la valoration minimale des mineurs $\nu \times \nu$ de la matrice $B_{(t)}$, pour chaque ν .

Soit p un premier différent de 2, 3, 5. D'après le corollaire 5 on sait que $\alpha_6(B) = 1$; c'est à dire, il existent des polynômes $\lambda_i(T) \in \mathbb{Z}[T]$ tels que

$$\sum \lambda_i(T)\, B_i^6(T) = c \ ,$$

où $c \in \mathbb{Z}$. En calculant le premier mineur principal d'ordre 6 de la matrice B on obtient $B_1^6(T) = -\, 2^{31}\, 3^{15}\, 5^{20}\, T$. En conséquence,

$$pgcd\ \{B_i^6(0)\}_{i\geq 1} = pgcd\ \{B_i^6(0)\}_{i>1} = 2^6\ 5^{13}\ .$$

Soient $\lambda_i \in \mathbb{Z}$, $i \geq 2$, tels que $\sum \lambda_i\ B_i^6(0) = 2^6\ 5^{13}$. Alors on voit qu'il existe un polynôme $\lambda_1(T) \in \mathbb{Z}[T]$ tel que

$$\lambda_1(T)\ B_1^6(T) + 2^{31}\ 3^{15}\ 5^{20} \sum_{i>1} \lambda_i\ B_i^6(T) = 2^{37}\ 3^{15}\ 5^{33}\ .$$

Ceci entraîne que $\alpha_{6,t,p} = 1$, donc $d_1(t)$ divise $\alpha_{12,t,p}$ dans $\mathbb{Z}_p$. D'autre part, $d_1(t)^5$ divise chaque mineur $B_i^{11}(T)$ dans $\mathbb{Z}_p[T]$, car $p \neq 5$, et aussi d'après le corollaire 5. En conséquence, $d_1(t)^5$ divise le produit $\alpha_{1,t,p} \cdot \ldots \cdot \alpha_{11,t,p}$ pour tout $t \in \mathbb{Z}_p$. Donc $d_1(t)$ et $\alpha_{i,t,p}$ doivent être associés dans $\mathbb{Z}_p$ pour chaque i telle que $7 \leq i \leq 12$.

3. Calcul de l'invariant de Witt de $Tr_{E_t/\mathbb{Q}}(X^2)$

Pour calculer l'invariant de Witt de la forme quadratique $Tr_{E_t/\mathbb{Q}}(X^2)$), il faut d'abord diagonaliser la matrice $B_{(t)}$ pour tout p divisant d(t). Par applications successives de matrices du type

$$\begin{pmatrix} 1 & \frac{-b_{1,2}}{b_{1,1}} & \cdots & \frac{-b_{1,k}}{b_{1,1}} \\ 0 & 1 & 0 \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & & 0\ 1 \end{pmatrix}$$

où $12 \geq k \geq 1$ et $p \nmid b_{1,1}$, on arrive à diagonaliser $B_{(t)}$ sur $\mathbb{Z}_p$. En fait, on peut travailler mod p^s, avec s petit, grâce au résultat

classique suivant (cf. [3]):

Proposition 7. Soient Q_1 et Q_2 deux formes quadratiques non singulières, à n variables, avec matrices associées B_1, $B_2 \in \mathcal{M}_n(\mathbb{Z}_p)$. Soient $\alpha_j(B_i)$, $1 \leq j \leq n$, ses facteurs invariants sur $\mathbb{Z}_p$. Si $B_1 \equiv B_2 \pmod{p^s}$, $s > \sup_{i=1,2} \{ v_p(4\, \alpha_n(B_i)) \}$, alors on a que Q_1 et Q_2 sont $\mathbb{Z}_p$-équivalents.

Démonstration. Vu que $\alpha_1(B_1) = \alpha_1(B_2)$, on peut supposer que $\alpha_1(B_i) = 0$. Si $p \neq 2$, ou bien si $p = 2$ et dans la diagonale de B_1 il y a une unité 2-adique, alors on peut trouver une décomposition des formes Q_i du type

$$Q_i \overset{\mathbb{Z}_p}{\sim} \langle u_i \rangle \perp Q'_i \quad , \; i = 1,2,$$

où $u_i \in \mathbb{Z}_p^*$, Q'_i sont des formes quadratiques non singulières, à n-1 variables, et satisfaisant $u_1 \equiv u_2 \pmod{p^s}$, $B'_1 \equiv B'_2 \pmod{p^s}$, où B'_i dénote la matrice de Q'_i. Comme, d'autre part, $\alpha_n(B_i) = \alpha_{n-1}(B'_i)$ et $\langle u_1 \rangle \overset{\mathbb{Z}_p}{\sim} \langle u_2 \rangle$, la démonstration finit par induction sur n.

Si $p = 2$ et tous les termes de la diagonale de B_1 sont pairs, alors on peut trouver une décomposition du type

$$Q_i \overset{\mathbb{Z}_2}{\sim} F_i \perp Q'_i \quad , \quad i = 1,2,$$

où F_i est une forme quadratique à deux variables sur $\mathbb{Z}_2$, improprement primitive, et satisfaisant $F_1 \equiv F_2 \pmod{2^s}$, $B'_1 \equiv B'_2 \pmod{2^s}$. Ceci implique que $F_1 \overset{\mathbb{Z}_2}{\sim} F_2$ (cf. [1], ch. 8) et, en conséquence, la démonstration finit aussi par induction car, comme dans le cas précédent, $\alpha_n(B_i) = \alpha_{n-2}(B'_i)$.

On note $w(t)_p$ la p-composante locale de l'invariant de Witt de la forme quadratique $Tr_{E_t/\mathbb{Q}}(X^2)$.

Proposition 8 . Pour chaque spécialisation $t \in S$, on a :

i) $w(t)_2 = (-1)^{\frac{t-1}{2}}$,

ii) $w(t)_3 = 1$,

iii) $w(t)_5 = 1$,

iv) $w(t)_p = \left(\frac{-6t}{p} \right)^{v_p(d_1(t))}$, si $p \neq 2, 3, 5$,

v) $w(t)_\infty = 1$ si et seulement si $t \geq -197$.

Démonstration. Au moyen d'une diagonalisation module p^s , $s > v_p(4\alpha_n(B_t))$, on obtient le résultat pour $p = 2$ et 5; le cas $p = 3$ est trivial.

Soit $p \neq 2, 3, 5$. Si $v_p(d_1(t))$ est pair, alors la proposition 6 suffit pour voir que $w(t)_p = 1$.

Si $v_p(d_1(t))$ est impair, on remarque d'abord que $p \nmid B_1^6(t)$. Donc, compte tenu de la proposition 6, il existe una diagonalisation de $B_{(t)}$,

$$B_{(t)} \overset{\mathbb{Q}_p}{\sim} \langle u_1 \rangle \perp \ldots \perp \langle u_6 \rangle \perp \langle pu_7 \rangle \perp \ldots \perp \langle pu_{12} \rangle \quad ,$$

telle que $u_i \in \mathbb{Z}_p^*$, $1 \leq i \leq 12$, et $u_1 \cdot \ldots \cdot u_6 = B_1^6(t)$. D'où

$$w(t)_p = \left(\frac{-u_7 \cdot \ldots \cdot u_{12}}{p} \right) = \left(\frac{-u_1 \cdot \ldots \cdot u_6}{p} \right) = \left(\frac{-B_1^6(t)}{p} \right) = \left(\frac{-6t}{p} \right) \quad .$$

Corollaire 9. Pour chaque entier $t \in S$ tel que:

$t \geqslant -197$, $t \equiv 1 \pmod 4$, et $d_1(t)$ soit premier, on a que $w(t) = 1$.

On vérifie que si $t = 66k + 1$ et $k = 2, 4, 42, 44, 56, 62, 74, 80$, alors $d_1(t)$ est, en effet, un nombre premier, d'où l'on obtient finalement le

Théorème 10. $\widetilde{M}_{12}$ se réalise comme groupe de Galois sur $\mathbb{Q}$.

Remarque. Etant donné que $\widetilde{M}_{12}$ est le groupe des représentations de M_{12}, on a, plus géneralement, que toute extension centrale de M_{12} se réalise comme groupe de Galois sur $\mathbb{Q}$.

La table suivante, élaborée par J. Quer, donne les valeurs de $t = 66k + 1$, $-2 \leqslant k \leqslant 98$, pour lesquelles $w(t)$ est aussi trivial.

TABLE

k	t	$d_1(t)$	factorisation de $d_1(t)$
-2	-131	-1101247148491531	46487700979 * 23689
2	133	-1085133867241531	
4	265	518137617133469	
12	793	17565989179633469	516054795371 * 34039
26	1717	88343577070258469	1814446324021 * 269 * 181
42	2773	233040842695258469	
44	2905	255913645429633469	
50	3301	330912913007758469	434839570312429 * 761
52	3433	358039621992133469	2402950483168681 * 149
54	3565	386229807539008469	3550484611 * 108782279
56	3697	415483469648303469	
60	3961	477181223554633469	25114801239717551 * 19
62	4093	509625315351508469	
74	4885	726622873945258469	
80	5281	849478586835883469	
82	5413	892557444257758469	947140186039 * 942371
92	6073	1123903879804633469	4364014303871 * 257539

Bibliographie

[1] Cassels, J. W. S. : Rational Quadratic Forms. Acad. Press, 1978.

[2] Matzat, B.M. et Zeh, A.: Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbb{Q}$. J. Number Theory, à paraître.

[3] Minkowski, H.: Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten (1884). Gesammelte Abhandlungen, p. 3-144. Chelsea, 1967.

[4] Serre, J.-P.: Corps Locaux, 3 ème édition. Hermann, 1968.

[5] Serre, J.-P.: L'invariant de Witt de la forme $Tr(x^2)$. Comment. Math. Helvetici 59 (1984) 651-676.

Facultat de Matemàtiques

Universitat de Barcelona

Gran Via de les Corts Catalanes, 585

08007 Barcelona. ESPANYA.

Dipòsit Legal B.: 2.102-1986
BARCELONA—1986