ISRAEL JOURNAL OF MATHEMATICS 107 (1998), 333–341

EXTENSIONS Q-RÉGULIÈRES DE $\mathbf{Q}(t)$ DE GROUPE DE GALOIS $6.A_6$ ET $6.A_7$

PAR

J-F. MESTRE

UFR de Mathématiques, Université de Paris VII
2 place Jussieu, 75251 Paris Cedex 05, France
e-mail: mestre@mathp7.jussieu.fr

ABSTRACT

We prove that $6\mathbf{A}_6$ and $6\mathbf{A}_7$ are Galois groups of regular extensions of $\mathbf{Q}(t)$, therefore of infinitely many extensions of $\mathbf{Q}$.

1. Introduction

Soit n un entier ≥ 4. Si n est différent de 6 et de 7, le multiplicateur de Schur du groupe alterné A_n est égal à $\mathbf{Z}/2\mathbf{Z}$, et nous avons montré dans [3] que le groupe $\tilde{A_n}$, unique extension centrale de A_n par $\mathbf{Z}/2\mathbf{Z}$, est groupe de Galois d'une extension $\mathbf{Q}$-régulière de $\mathbf{Q}(t)$ (et donc d'une infinité d'extensions de $\mathbf{Q}$ deux à deux linéairement disjointes).

Dans le cas où $n = 6$ ou 7, le multiplicateur de Schur de A_n est égal à $\mathbf{Z}/6\mathbf{Z}$. Conformément aux notations de l'Atlas ([2]), on désigne alors par $6.A_n$ ($n = 6$ ou 7), l'unique extension centrale de A_n par $\mathbf{Z}/6\mathbf{Z}$ égale à son groupe de commutateurs.

Nous prouvons ici le théorème suivant:

THÉORÈME: *Les groupes $6.A_6$ et $6.A_7$ sont groupes de Galois d'extensions $\mathbf{Q}$-régulières de $\mathbf{Q}(t)$.*

Via le théorème d'irréductibilité de Hilbert, on en déduit aussitôt:

Received October 16, 1996

COROLLAIRE: *Il existe une infinité d'extensions de* $\mathbf{Q}$, *deux à deux linéairement disjointes, dont le groupe de Galois est* $6.A_6$ *(resp.* $6.A_7$*).*

Le théorème résulte de l'existence, démontrée dans la section suivante, d'une extension K de $\mathbf{Q}(t)$ de degré n ($n = 6$ ou 7), dont la clôture galoisienne M est $\mathbf{Q}$-régulière et a comme groupe de Galois G (où $G = A_6$ ou A_7), et telle que les deux conditions suivantes soient réalisées:

(i) En toute place v de $\mathbf{Q}(t)$ où M est ramifiée, le degré de v est premier à 3, le groupe d'inertie I_v est d'ordre impair et le groupe de décomposition D_v est d'ordre non divisible par 9.

(ii) Pour $t = 0$, l'extension K se spécialise en une algèbre étale E telle que l'invariant de Witt de la forme trace q_E définie par $x \mapsto \mathrm{Tr}_{E/\mathbf{Q}}(x^2)$ soit nul.

En effet, soit α l'élément de $H^2(G, \mathbf{Z}/6\mathbf{Z})$ correspondant à l'extension $6.G$, et soit $\rho : \mathrm{Gal}(\overline{\mathbf{Q}(t)}/\mathbf{Q}(t)) \to G$ le morphisme correspondant à l'extension $M/\mathbf{Q}(t)$; il existe une extension L de M telle que $L/\mathbf{Q}(t)$ soit galoisienne de groupe de Galois $6.G$ si et seulement si l'élément $\beta = \rho^*(\alpha)$ de $H^2(\mathrm{Gal}(\overline{\mathbf{Q}(t)}/\mathbf{Q}(t)), \mathbf{Z}/6\mathbf{Z})$ est nul, c'est-à-dire si et seulement si les éléments correspondants $\beta_2 \in H^2(\mathrm{Gal}(\overline{\mathbf{Q}(t)}/\mathbf{Q}(t)), \mathbf{Z}/2\mathbf{Z})$ et $\beta_3 \in H^2(\mathrm{Gal}(\overline{\mathbf{Q}(t)}/\mathbf{Q}(t)), \mathbf{Z}/3\mathbf{Z})$ sont nuls.

Pour tout point fermé x de la droite projective, de corps résiduel $\mathbf{Q}(x)$, notons $r_x(\beta_2)$ le **résidu** de β_2, qui est un élément de $H^1(\mathbf{Q}(x), \mathbf{Z}/2\mathbf{Z})$. (Pour la définition du résidu, nous renvoyons à Arason [1] et à Serre, [6], pp. 121–122.)

Comme β_2 provient de l'extension $M/\mathbf{Q}(t)$, dont les groupes d'inertie sont d'ordre premier à 2, on a $r_x(\beta_2) = 0$. (Cf. Serre, *loc. cit.*, p. 121.)

Cela entraîne (*loc. cit.*, p. 122, (4.2)) que β_2 est constant, i.e. est un élément de $H^2(\mathbf{Q}, \mathbf{Z}/2\mathbf{Z})$. Or, d'après [4], β_2 est égal à l'invariant de Witt de la forme quadratique q_K; le point (ii) montre donc que $\beta_2 = 0$.

Pour montrer que $\beta_3 = 0$, on remarque que, pour tout sous-groupe H de G d'ordre non divisible par 9, la restriction de α à $H^2(H, \mathbf{Z}/3\mathbf{Z})$ est nulle (on peut le voir par exemple en remarquant que $6.G$ n'a pas d'élément d'ordre 9). Par suite, d'après (i), en toute place v où $K/\mathbf{Q}(t)$ est ramifiée, l'obstruction est nulle (et en particulier le résidu est nul). Par le même argument que ci-dessus, cela prouve que β_3 est constant. Si v est une place ramifiée, la spécialisation de β_3 en v est nulle, donc (le degré de v étant premier à 3), $\beta_3 = 0$.

Enfin, les extensions de groupe de Galois $6.A_n$ ($n = 6$ ou 7) ainsi obtenues sont $\mathbf{Q}$-régulières, car leurs sous-extensions galoisiennes distinctes de $\mathbf{Q}(t)$ contiennent M, qui est régulière par hypothèse.

2. Le cas de $6.A_6$

Considérons les polynômes

$$P = X\left(X^2 - 8X + 6\right)\left(X^2 + 8X + 6\right)$$

et

$$Q = 625X^6 + 15750X^4 - 51300X^2 + 6696.$$

Les polynômes P et Q sont premiers entre eux, le discriminant de P est un carré, et l'on a l'identité

$$Q'P - QP' = (X^2 - 186)(5X^2 + 6)^4.$$

(La construction des polynômes P et Q est expliquée dans la section 4.)

Soient s une indéterminée, et $K_0 = \mathbf{Q}(s)$; le discriminant de l'élément $Q - sP$ de $K_0[X]$ est égal à

$$U(s) = 2^{28}3^6 5^2 (s^2 - s_1^2)(s^2 - s_2^2)^4,$$

où l'on a posé $s_1 = \sqrt{44804543042/25}$ et $s_2 = \sqrt{-675000}$.

Le corps de décomposition M_0 de $Q - sP$ sur K_0 est ramifié en les racines $\{\pm s_1, \pm s_2\}$ de U; en $s = \pm s_1$, $Q - sP$ a une racine d'ordre 2, à savoir $\pm\sqrt{186}$, et en $s = \pm s_2$, $Q - sP$ a une racine d'ordre 5, à savoir $\pm\sqrt{-6/5}$; par suite, le groupe d'inertie de M_0 est cyclique d'ordre 2 au-dessus de $\pm s_1$ et cyclique d'ordre 5 au-dessus de $\pm s_2$.

De plus, le groupe de Galois de l'extension correspondante de $\mathbf{C}(s)$ est transitif (car $Q - sP$ est irréductible dans $K_0[X]$), et engendré par des cycles d'ordre 2 et 5. D'après [5], p. 40, c'est donc le groupe symétrique S_6. Par suite, le groupe de Galois de M_0 sur $\mathbf{Q}(s)$ est aussi égal à S_6.

Soit u l'une des racines carrées de $s^2 - s_1^2$; posons $t = 5(s + u)/4908$ (ce qui revient à paramétrer la conique $u^2 = s^2 - s_1^2$ par $s = f(t) = 2454(t^2 + 186)/5t$ et $u = 2454(t^2 - 186)/5t$). On a $\mathbf{Q}(t) = \mathbf{Q}(u, s)$.

L'extension $M = M_0 \otimes_{K_0} \mathbf{Q}(t)$ de $\mathbf{Q}(t)$ est non ramifiée en les points t images réciproques par f de $\pm s_1$ (on peut par exemple invoquer le lemme d'Abhyankar), et ramifiée en les quatre valeurs de t images réciproques de $\pm s_2$, le groupe d'inertie étant cyclique d'ordre 5. En ces valeurs, le groupe de décomposition est un sous-groupe de S_5, et son ordre n'est donc pas divisible par 9.

Le point (i) de la section précédente est donc vérifié. Il nous reste à vérifier que le point (ii) l'est aussi.

Pour $t = 0$ (donc $s = \infty$), la spécialisation de $Q - sP$ est le polynôme $P = X(X^2 - 8X + 6)(X^2 + 8X + 6)$; on vérifie (voir la section 5) que l'invariant de Witt correspondant est nul.

Les points (i) et (ii) sont donc vérifiés. Par construction, le groupe de Galois de $M/\mathbf{Q}(t)$ est le groupe alterné $\mathbf{A}_6$, et l'on a le même résultat sur $\mathbf{C}$, donc l'extension $M/\mathbf{Q}(t)$ est $\mathbf{Q}$-régulière.

D'où le théorème pour le groupe $6.A_6$.

3. Le cas de $6.A_7$

Considérons les polynômes

$$P(X) = X(49X^6 - 882X^4 + 1365X^2 - 100)$$

et

$$Q(X) = 32585X^4 - 9702X^2 + 141.$$

Ils sont premiers entre eux, le discriminant de P est un carré, et l'on a l'identité

$$P'Q - PQ' = 15(7X^2 + 1)^4(133X^2 - 940).$$

(La construction des polynômes P et Q est expliquée dans la section 4.)

Soient s une indéterminée, et $K_0 = \mathbf{Q}(s)$; le discriminant de $P - sQ$ par rapport à X est de la forme $U(s) = A(s^2 - s_1^2)(s_2 - s_2^2)^4$, A non nul et $s_1 \neq s_2$. (Plus précisément, on a $A = -2^{12}3^65^57^{13}19^543^247.107^2$,

$$s_1 = \sqrt{727652224800000/845015060359038779}$$

et $s_2 = \sqrt{-1/343}$.)

Le corps de décomposition M_0 de $P - sQ$ sur K_0 est ramifié en l'infini et en les racines $\{\pm s_1, \pm s_2\}$ de U; le groupe d'inertie est cyclique d'ordre 3 en l'infini, cyclique d'ordre 2 au-dessus de $\pm s_1$ et cyclique d'ordre 5 au-dessus de $\pm s_2$.

De plus, le groupe de Galois de l'extension correspondante de $\mathbf{C}(s)$ est transitif (car $P - sQ$ est irréductible dans $K_0[X]$), et engendré par des cycles d'ordre 2, 3 et 5. D'après [5], p. 40, c'est donc le groupe symétrique S_7. Par suite, le groupe de Galois de M_0 sur $\mathbf{Q}(s)$ est aussi égal à S_7.

Faisons à présent le changement de base défini par $u^2 = -5.7.19.47(s^2 - s_1^2)$; les points d'abscisse $s = 0$ de cette conique sont rationnels, donc elle est isomorphe à la droite projective; paramétrons-la par exemple par

$$s = f(t) = \frac{120636000}{11626727} \frac{t}{t^2 + 31255}.$$

L'extension $M = M_0 \otimes \mathbf{Q}(t)$ de $\mathbf{Q}(t)$ est non ramifiée en les points t images réciproques par f de $\pm s_1$; elle est ramifiée en les deux points images réciproques de l'infini, le groupe d'inertie étant cyclique d'ordre 3 (et le groupe de décomposition est un sous-groupe du produit direct du groupe symétrique S_3 par le groupe diédral D_4, et est donc d'ordre non divisible par 9), et ramifiée en les quatre valeurs de t images réciproques de $\pm s_2$, le groupe d'inertie étant cyclique d'ordre 5 (et le groupe de décomposition étant un sous-groupe de $S_5 \times S_2$, donc d'ordre non divisible par 9).

Le point (i) de la section précédente est donc vérifié. Pour $t = 0$ (donc $s = 0$), le polynôme $P - f(t)Q$ se spécialise en le polynôme P. On vérifie que l'invariant de Witt de l'algèbre étale définie par P est nul (voir la section 5 pour la démonstration), d'où le point (ii).

Par construction, le groupe de Galois de $M/\mathbf{Q}(t)$ est le groupe alterné A_7. De plus, M étant une extension non constante de $\mathbf{Q}(t)$, elle est $\mathbf{Q}$-régulière. D'où le théorème pour le groupe $6.A_7$.

4. Construction des polynômes P et Q

Comme on l'a vu dans les deux sections précédentes, la démonstration du théorème utilise l'existence de polynômes P et Q premiers entre eux, tels qu'il existe des polynômes R et S, premiers entre eux, vérifiant la relation $P'Q - PQ' = R^4 S$.

Nous montrons dans cette section comment construire de tels couples de polynômes P et Q.

LEMME: *Soit k un corps de caractéristique nulle, et soient P et T deux éléments de $k[X]$ premiers entre eux, P sans racine multiple. Il existe un polynôme $Q \in k[X]$ tel que $PQ' - P'Q = T$ si et seulement si $P'T' - P''T \equiv 0 \mod P$.*

En effet, l'existence de Q tel que $PQ' - P'Q = T$ équivaut à dire que les primitives de T/P^2 sont des fractions rationnelles, c'est-à-dire que les résidus de T/P^2 en les racines de P sont nuls; or, si a est une racine de P, le résidu de T/P^2 en a est égal à $(P'(a)T'(a) - P''(a)T(a))/P'(a)^3$; donc les résidus de T/P^2 sont nuls si et seulement si $P'T' - P''T \equiv 0 \mod P$, d'où le lemme. (Le fait que Q soit un élément de $k[X]$ provient du fait que Q est obtenu en résolvant un système d'équations linéaires à coefficients dans k.)

Remarque: Lorsque Q existe, il est premier à P (car P est premier à T), et son degré est égal à $\deg(T) + 1 - \deg(P)$.

Nous nous intéressons ici au cas où T est de la forme $(X^2+a)^4(X^2+b)$; dans la section 2, le polynôme P est de degré 5 (et le polynôme Q est donc de degré 6), et dans la section 3, le polynôme P est de degré 7 (et le polynôme Q est donc de degré 4). Dans les deux cas, pour simplifier les calculs, on a supposé P impair.

4.1 LE CAS OÙ P EST DE DEGRÉ 5. On cherche ici un polynôme $P = X(X^4+a_2X^2+a_0)$ et un polynôme

$$T = (X^2+a)^4(X^2+b)$$

tels que $P''T - P'T' \equiv 0 \mod P$, P étant séparable et premier à T.

Comme $P''T - P'T'$ est égal à

$$2X(X^2+a)^3((10X^2+3a_2)(X^2+a)(X^2+b)-(5X^4+3a_2X^2+a_0)(5X^2+4b+a)),$$

et que T est premier à P, cela revient donc à résoudre l'équation

$$\begin{aligned}(10X^2+3a_2)(X^2+a)(X^2+b) - (5X^4+3a_2X^2+a_0)(5X^2+4b+a)\\ \equiv 0 \mod(X^4+a_2X^2+a_0),\end{aligned}$$

c'est-à-dire, après calcul,

$$\left(-5\,aa_2+10\,a_0+ba_2+10\,ab-3\,a_2^2\right)X^2-6\,aa_0+3\,aba_2+6\,ba_0-3\,a_0\,a_2=0.$$

On élimine alors b entre les deux coefficients de ce polynôme, et l'on trouve la relation $(a_2^2-4a_0)(5a_0+3aa_2+5a^2)=0$, soit, P étant séparable, $a_0 = -a(a+3a_2/5)$, d'où

$$b = \frac{(2a+a_2)(5a+3a_2)}{a_2+10a}.$$

À des facteurs carrés près, le discriminant de P est égal à $-5a(5a+3a_2)$; c'est donc un carré si et seulement si $a_2 = -\frac{5}{3}a(1+u^2)$, avec $u \in \mathbf{Q}$.

Il reste à prouver que le point (ii) de l'introduction est vérifié. Pour cela, si k est un corps et $P \in k[X]$ un polynôme séparable, notons q_P la forme quadratique q_E, où E est l'extension $k[X]/(P)$ de k.

Le calcul de l'invariant de Witt de q_P est particulièrement simple (voir la section 5) lorsque P se scinde en deux facteurs $S(X)S(-X)$, où $S(X) = X^2 + AX + B$ est du second degré; un calcul facile montre qu'il en est ainsi si

$$B = au \quad \text{et} \quad a = \frac{3\,A^2}{5\,u^2+6\,u+5}.$$

Le changement de variable $X \mapsto AX/(5u^2 + 6u + 5)$ permet d'éliminer le paramètre A; on trouve alors $P = S(X)S(-X)$, avec

$$S(X) = X^2 + (5u^2 + 6u + 5)(X + 3u).$$

La proposition de la section 5 montre que l'invariant de Witt correspondant est égal à $w = ((5u^2 + 6u + 5)(5u^2 - 6u + 5), -1)$. On remarque alors que $5u^2+6u+5-(u-1)^2 = 4(u+1)^2$, donc $(5u^2+6u+5, -1) = 0 = (5u^2-6u+5, -1)$, et $w = 0$.

Les polynômes donnés au début de la section 2 ont été obtenus en prenant $u = 5$, et en faisant le changement de variable $X \mapsto 20X$, qui simplifie l'écriture de P.

4.2 LE CAS OÙ P EST DE DEGRÉ 7. On cherche ici un polynôme $P = X(X^6 + a_4X^4 + a_2X^2 + a_0)$ et un polynôme $T = (X^2 + a)^4(X^2 + b)$ tels que $P''T - P'T' \equiv 0 \bmod P$, P étant supposé séparable et premier à T.

Comme ci-dessus, le polynôme $P''T - P'T'$ est de la forme $X(X^2 + a)^3R(X)$, où R est un polynôme pair; le reste de R modulo $X^6 + a_4X^4 + a_2X^2 + a_0$ est un polynôme pair de degré 4 dont les coefficients de degré respectivement 0, 2 et 4 sont

$$15a_0a - 3a_0b - 3a_2ab - a_0a_4,$$
$$-10a_4ab - 9a_0 + 2a_2b - a_2a_4 + 14a_2a,$$
$$-2a_2 + 3a_4b + 9a_4a - 21ab - a_4^2.$$

On tire a_2 et a_0 des deux dernières expressions, puis on substitue dans la première, et l'on trouve

$$(21ab - 3a_4b + a_4^2 + 210a^2 - 29a_4a)(6b^2 - a_4b - a4^2 - 21ab + 9a_4a) = 0.$$

Le second terme de ce produit conduit à un polynôme P non séparable; par contre, le premier terme donne

$$b = \frac{a_4^2 - 29a_4a + 210a^2}{3a_4 - 21a},$$

d'où $a_0 = -5a^2(14a - a_4)$ et $a_2 = 5a(21a - 2a_4)$.

À des facteurs carrés près, le discriminant de P est égal à $5(14a - a_4)$; c'est donc un carré dès que $a_4 = 14a - 5u^2$. En posant $a = u^2/v$ et en faisant le changement de variable $X \mapsto uX/v$, on trouve finalement

$$P(X) = X(X^6 - v(5v - 14)X^4 + 5v^2(10v - 7)X^2 - 25v^4).$$

D'après la proposition de la section 5, l'invariant de Witt de la forme q_P est égal à $w = (\delta, -2\alpha c) + (a, -\alpha) + (-c, 2\alpha)$, avec $a = v(5v - 14)$, $c = 25v^4$ et $\alpha = 10\,v^4\left(125\,v^3 - 1750\,v^2 + 2765\,v - 1176\right)$ et

$$\delta = 400\,v^6\,(v-1)\left(125\,v^3 - 1675\,v^2 + 1715\,v - 1029\right).$$

Pour $v = 28$, on obtient $w = (1117, -5.821) + (2, -2.5.821) + (-1, 5.821) = 0$. On trouve ainsi le polynôme P de la section 3 (une fois fait le changement de variable $X \mapsto 14X$, qui simplifie l'écriture de P); le polynôme Q correspondant est alors calculé par résolution d'un système d'équations linéaires.

5. Calcul de certains invariants de Witt

PROPOSITION: *Soit k un corps de caractéristique $\neq 2$.*

(1) *Soit $P = (X^2+aX+b)(X^2+cX+d)$, $a, b, c, d \in k$, P séparable. L'invariant de Witt de la forme trace q_P est égal à $(2(a^2-4b), 2(c^2-4d))$. En particulier, si $a^2 - 4b$ et $c^2 - 4d$ sont égaux modulo $(k^*)^2)$, cet invariant est égal à $(a^2 - 4b, -1)$.*

(2) *Soit $P(X) = X^6 - aX^4 + bX^2 - c$, $a, b, c \in k$, P séparable. L'invariant de Witt de la forme trace q_P est égal à*

$$(\delta, -2\alpha c) + (a, -\alpha) + (-c, 2\alpha),$$

où δ est le discriminant du polynôme $X^3 - aX^2 + bX - c$ et où $\alpha = a^2b + 3ac - 4b^2$.

Soit $P(X) = (X^2+aX+b)(X^2+cX+d)$; l'algèbre $A = k[X]/(P)$ est isomorphe à $k[X]/(X^2 + aX + b) \times k[X]/(X^2 + cX + d)$, et la forme q_P est la somme des formes traces de chacun de ces deux facteurs. Or la forme q_E de l'extension $E = k[X]/(X^2 + aX + b)$ de k est isomorphe à $\langle 2, 2(a^2 - 4b)\rangle$; donc la forme q_A est isomorphe à

$$\langle 2, 2(a^2 - 4b), 2, 2(c^2 - 4d)\rangle = \langle 2, 2, a^2 - 4b, c^2 - 4d\rangle.$$

Comme $\langle 2, 2\rangle$ est isomorphe à $\langle 1, 1\rangle$, la forme q_A est isomorphe à $\langle 1, 1, 2(a^2 - 4b), 2(c^2 - 4d)\rangle$, dont l'invariant de Witt est $(2(a^2 - 4b), 2(c^2 - 4d))$. Supposons qu'il existe $u \in k^*$ tel que $c^2 - 4d = u^2(a^2 - 4b)$; l'invariant de Witt est alors égal à $(2(a^2 - 4b), 2(a^2 - 4b)) = (2(a^2 - 4b), -1) = (a^2 - 4b, -1)$, d'où le point (1) de la proposition.

Soit à présent $Q(X) = X^3 - aX^2 + bX - c$, et $P(X) = Q(X^2)$. Soit B la k-algèbre $k[X]/(P)$; notons z l'image de X dans B; B contient la sous-algèbre

C engendrée par $1, z^2, z^4$, qui est isomorphe à $k[X]/(Q)$, et dont l'orthogonal $C^\perp$ (relativement à la forme q_P) est l'espace de dimension 3 ayant pour base $\{z, z^3, z^5\}$. On sait (voir [4], p. 656) que la forme q_C est isomorphe à la forme $\langle 1, 2, 2\delta\rangle$, δ étant le discriminant de Q. Par suite, la restriction de q_P à C, qui est égale à $2q_P$, est isomorphe à $2\langle 1, 2, 2\delta\rangle = \langle 2, 1, \delta\rangle$.

La matrice de la restriction de q_P à $C^\perp$, dans la base $\{z, z^3, z^5\}$, a comme matrice $2\begin{pmatrix} s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \\ s_3 & s_4 & s_5 \end{pmatrix}$, où les s_i sont les sommes de Newton $\sum_{j=1}^3 x_j^i$ du polynôme Q (les x_j étant les racines de Q dans une clôture algébrique de k); on a $s_1 = a$, $s_2 = a^2 - 2b$ et $s_3 = a^3 - 3ab + 3c$. Le discriminant de P est égal à $c\delta^2$, comme on le voit par la formule de transitivité des discriminants relatifs. Par ailleurs, ce discriminant est égal au produit du déterminant d_3 de la matrice ci-dessous et du discriminant de la forme q_P restreinte à C, soit 2δ. On en déduit que $d_3 = c\delta$.

Les deux autres déterminants mineurs principaux de cette matrice valent respectivement $d_1 = 2a$ et $d_2 = 4\alpha$, où $\alpha = a^2b + 3ac - 4b^2$. La forme quadratique est donc équivalente à $\langle d_1, d_1d_2, d_2d_3\rangle$, soit $\langle 2a, 2\alpha, 2c\alpha\delta\rangle$. Par suite, la forme quadratique q_P est isomorphe à la forme $\langle 1, 2, \delta, 2a, 2a\delta, 2c\alpha\delta\rangle$.

Après un calcul facile, on trouve que l'invariant de Witt de cette forme est $(\delta, -2\alpha c) + (a, -\alpha) + (-c, 2\alpha)$, d'où la proposition.

References

[1] J. K. Arason, *Cohomologische Invarianten Quadratischer Formen*, Journal of Algebra **36** (1975), 448–491.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Clarendon Press, Oxford, 1985.

[3] J.-F. Mestre, *Extensions régulières de* $\mathbf{Q}(t)$ *de groupe de Galois* $\tilde{A}_n$, Journal of Algebra **131** (1990), 483–495.

[4] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Commentarii Mathematici Helvetici **59** (1984), 651–676.

[5] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Jones and Bartlett, London, 1992.

[6] J.-P. Serre, *Cohomologie galoisienne des extensions transcendantes pures*, in *Cohomologie Galoisienne*, 5-ième édition, révisée et complétée, Lecture Notes in Mathematics **5**, Springer-Verlag, Berlin, 1994.