ACTA ARITHMETICA
LXII.1 (1992)

Sur les extensions de groupe de Galois $\widetilde{A}_4$

par

C. Bachoc et S.-H. Kwon (Talence)

0. Introduction. Soit K/k_0 une extension séparable de degré n, et soit N/k_0 sa clôture galoisienne (dans une clôture séparable k_0^s de k_0). Le groupe de Galois G de N/k_0 se plonge dans le groupe symétrique S_n, de façon canonique à automorphisme intérieur près. Nous nous limiterons aux extensions paires, c'est-à-dire pour lesquelles l'image de G est contenue dans A_n. On sait depuis Schur que, pour $n \geq 4$, $H^2(A_n, \{\pm 1\})$ est d'ordre 2, et définit donc une extension de G, unique à isomorphisme près, que nous notons $\widetilde{G}$. Nous nous intéressons dans cet article au cas où G est isomorphe à A_4. L'unique extension non triviale de A_4 par $\{\pm 1\}$ a une réalisation dans le groupe des quaternions usuels de norme 1 : $\{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$. L'autre groupe pair en degré 4 est le groupe bicyclique de type $(2,2)$; c'est le 2-sous-groupe de Sylow de A_4, et son extension correspondante est le groupe quaternionien H_2.

Lorsque k_0 n'est pas de caractéristique 2, ce qui est le cas dans nos applications, un théorème de Serre ([S1]) permet de lier la possibilité de plonger N/k_0 dans une extension $\widetilde{N}/k_0$ de groupe de Galois $\widetilde{G}$ à un calcul d'invariant de Witt de la forme $\mathrm{Tr}_{K/k_0}(x^2)$. En outre, dans le cas A_4, $\widetilde{N}$ est la clôture galoisienne d'une extension $\widetilde{K}/k_0$ de degré 8 contenant K/k_0.

Dans cette note, nous considérons le cas où $k_0 = \mathbb{Q}$. Nous calculons des polynômes définissant les corps de groupe de Galois $\widetilde{A}_4$ réalisant les plongements des corps de groupe de Galois A_4 extraits de la table [BPS] de corps de degré 4 et totalement réels; pour cela nous utilisons un critère de plongement arithmétique valable pour $k_0 = \mathbb{Q}$ (proposition 1.3), et l'existence d'un "plongement pur" (théorème 2.2), c'est-à-dire non ramifié en dehors des idéaux premiers déjà ramifiés dans K.

Le théorème 2.5 montre l'existence d'une classe au sens restreint d'ordre 2 pour toute extension de $\mathbb{Q}$ de groupe de Galois A_4 totalement réelle. Cette propriété remarquable est aussi vérifiée par toute extension bicyclique de $\mathbb{Q}$ plongeable dans une extension quaternionienne.

Le paragraphe 3 donne les résultats numériques, et en particulier les discriminants minimaux pour les deux signatures possibles (proposition 3.2). Ces calculs numériques ont été faits dans le système PARI, mis au point par C. Batut, D. Bernardi, H. Cohen, M. Olivier.

Cet article est extrait des chapitre 3 des thèses de chacun des auteurs (Bordeaux, 1989).

Remerciements. Les auteurs remercient Jacques Martinet pour les avoir guidées dans ce travail, Jean-Pierre Serre pour leur avoir communiquées le résultat sur l'existence d'un plongement non ramifié du lemme 2.4, et Henri Cohen pour son aide dans l'utilisation du système PARI.

1. Problème de plongement. Reprenons les notations de l'introduction. Dans le cas où $K = k_0(\sqrt{x_1}, \sqrt{x_2})$ est une extension bicyclique de k_0, le théorème de Serre ([S1], Th. 1) donne le critère de plongement suivant, déjà démontré par Witt dans [W]. On note (x, y) le symbole de Hilbert.

1.1. Proposition ([S1]). *K/k_0 est plongeable dans une extension quaternionienne si et seulement si*

$$(-1, x_1)(-1, x_2)(x_1, x_2) = 1.$$

En effet, il suffit de remarquer que l'invariant de Witt de la forme $\mathrm{Tr}_{K/k_0}(x^2)$, calculé dans la base $\{1, \sqrt{x_1}, \sqrt{x_2}, \sqrt{x_1x_2}\}$, est égal à l'expression de gauche. ∎

Ce critère se généralise aux extensions de groupe de Galois A_4. Soit K/k_0 une telle extension, et soit N sa clôture galoisienne. Soit S le 2-sous-groupe de Sylow de G, et posons $k = N^S$ et $N = k(\sqrt{x_1}, \sqrt{x_2})$. Alors, comme $[G : S]$ est impair, l'homomorphisme de restriction Res : $H^2(G, \{\pm 1\}) \to H^2(S, \{\pm 1\})$ est injectif.

Soit s l'élément de $H^2(S, \{\pm 1\})$ correspondant à l'extension de S par le groupe des quaternions. Soit $x = \mathrm{Cor}\,(s)$ la Corestriction de s; x correspond à l'extension non triviale de G que l'on note $\widetilde{G}$.

1.2. Proposition. *Sous les hypothèses précédentes, N/k_0 est plongeable dans une extension de groupe de Galois $\widetilde{G}$ si et seulement si*

$$(-1, x_1)(-1, x_2)(x_1, x_2) = 1.$$

Démonstration. Soit G_{k_0} le groupe de Galois absolu de k_0, et soit $\pi : G_{k_0} \to G$ l'homomorphisme surjectif définissant N.

Alors N/k_0 est plongeable si et seulement si il existe un relèvement

$\widetilde{\pi} : G_{k_0} \to \widetilde{G}$ de π rendant commutatif le diagramme suivant :

$$\begin{array}{ccccccc} 1 & \to & \{\pm 1\} & \to & \widetilde{G} & \to & G \to 1 \\ & & & & {\scriptstyle\tilde{\pi}}\nwarrow & \uparrow & {\scriptstyle\pi} \\ & & & & & G_{k_0} & \end{array}$$

Un tel relèvement est nécessairement surjectif, car la suite exacte n'est pas scindée.

L'homomorphisme π induit un élément $\pi^* x$ de $H^2(G_{k_0}, \{\pm 1\})$. L'existence de $\widetilde{\pi}$ est équivalente à la condition $\pi^* x = 1$.

La commutativité du diagramme suivant :

$$\begin{array}{ccc} H^2(G, \{\pm 1\}) & \xrightarrow{\text{Res}} & H^2(S, \{\pm 1\}) \\ {\scriptstyle\pi^*}\downarrow & & {\scriptstyle(\pi|_{G_k})^*}\uparrow \\ H^2(G_{k_0}, \{\pm 1\}) & \xrightarrow{\text{Res}} & H^2(G_k, \{\pm 1\}) \end{array}$$

et l'injectivité des restrictions montrent que

$$\pi^* x = 1 \Leftrightarrow (\pi|_{G_k})^* s = 1,$$

c'est-à-dire : N/k_0 est plongeable dans une extension de groupe de Galois $\widetilde{G}$ si et seulement si N/k est plongeable dans une extension quaternionienne. On peut donc appliquer la proposition 1.1. ∎

Dans le cas où $k_0 = \mathbb{Q}$, le critère de la proposition 1.2 se traduit par des conditions arithmétiques. On retrouve les conditions de plongement démontrées dans [K], et généralisées dans [B] au cas d'un groupe G isomorphe à $\mathrm{PSL}(2, l)$.

Notation : L'indice figurant dans un idéal premier désigne son degré résiduel.

1.3. Proposition. *Soit K un corps quartique sur $\mathbb{Q}$ dont le groupe de Galois de la clôture galoisienne est isomorphe à A_4. Alors K est plongeable dans une extension de groupe de Galois $\widetilde{A}_4$ si et seulement si* :

(i) *K est totalement réel*,

(ii) *pour tout nombre premier impair p divisant le discriminant d_K de K*,

$$pO_K = \mathfrak{p}_2^2 \Rightarrow p \equiv 3 \bmod 4 \quad \text{et} \quad pO_K = (\mathfrak{p}_1 \mathfrak{p}_1')^2 \Rightarrow p \equiv 1 \bmod 4.$$

Nous utiliserons plus particulièrement dans le paragraphe 3 le corollaire suivant :

1.4. Corollaire. *Si K est totalement réel et si $d_K d_k^{-1} = 1$ ou est une puissance d'un nombre premier, alors K est plongeable.*

Démonstration du Corollaire. La condition de la proposition 1.2 se localise aux places v de k. Elle est trivialement vérifiée si v est non ramifiée dans N. Sous les hypothèses du corollaire, elle est donc vérifiée partout sauf peut-être aux places au-dessus d'un seul nombre premier p; la formule du produit pour le symbole de Hilbert montre qu'elle l'est partout. ∎

1.5. Remarque. Il n'y a que deux signatures possibles pour $\widetilde{K}$. En effet, on a vu que, si K est plongeable, alors il est totalement réel. Si $\widetilde{K} = K(\sqrt{\gamma})$ est une réalisation du plongement, alors pour tout σ appartenant à G, $\gamma^\sigma\gamma^{-1}$ est un carré dans N, donc γ est soit totalement positif soit totalement négatif et $\widetilde{K}$ et soit totalement réel soit totalement imaginaire.

1.6. Application numérique. La table de [BPS] des corps réels de degré 4 et de discriminant inférieur à 10^6 fournit une description des 31 premiers corps réels de degré 4 et de groupe de Galois isomorphe à A_4. Ils vérifient tous les hypothèses du point (ii) de la proposition 1.3 sauf deux d'entre eux, pour lesquels

$$d_K = 520^2 = (2^3 \cdot 13 \cdot 5)^2, \qquad d_k = 13^2, \qquad (5) = \mathfrak{p}_2^2,$$
$$d_K = 728^2 = (2^3 \cdot 7 \cdot 13)^2, \qquad d_k = 7^2, \qquad (13) = \mathfrak{p}_2^2.$$

D'après la proposition 1.3, ils sont donc tous plongeables sauf les deux corps dont le discriminant est 520^2 et 728^2.

2. Plongement et ramification. Le corps de base est $k_0 = \mathbb{Q}$. Si K est un corps de degré 4 sur $\mathbb{Q}$ de type A_4 et plongeable dans une extension de type $\widetilde{A}_4$, on cherche à réaliser le plongement en minimisant le nombre de places ramifiées.

Nous aurons besoin du résultat suivant, dû à T. Crespo, qui décrit toutes les réalisations du plongement à partir de l'une d'entre elles :

2.1. Proposition ([C1]). *Si $K(\sqrt{\gamma})$ est une réalisation du plongement, alors les autres sont les $K(\sqrt{m\gamma})$ avec $m \in \mathbb{Z} - \{0\}$.*

Le théorème suivant décrit la ramification dans le (ou les) plongements de plus petit discriminant :

2.2. Théorème. *On suppose K plongeable.*

1) *Si $\widetilde{K}$ est une réalisation du plongement, alors tout idéal premier de K au-dessus d'un nombre premier de $\mathbb{Q}$ ramifié dans N/k est ramifié dans $\widetilde{K}$.*

2) *Il existe une réalisation $\widetilde{K}$ du plongement telle que $\widetilde{K}/K$ soit non ramifiée en dehors des idéaux premiers de K qui sont ramifiés dans N/k. On appellera un tel corps un "$\widetilde{A}_4$ pur".*

2.3. Remarque. Si $\widetilde{K} = K(\sqrt{\gamma})$ est un $\widetilde{A}_4$ pur, alors $\widetilde{K}$ est éventuellement ramifié à l'infini. Changer γ en $-\gamma$ chasse la ramification à l'infini, mais enintroduit éventuellement en 2.

Démonstration. 1) Soient L_1, L_2, L_3 les trois extensions intermédiaires de N/k. Si $\widetilde{K} = K(\sqrt{\gamma})$ est une réalisation du plongement, posons $\widetilde{N} = N(\sqrt{\gamma})$. Alors le groupe de Galois de N sur k est le groupe quaternionien d'ordre 8, donc les extensions $\widetilde{N}/L_i$ sont cycliques. Si $\mathfrak{P}$ est un idéal premier de N ramifié sur k, il est ramifié sur au moins un des L_i, donc dans $\widetilde{N}$.

2) Partons d'une réalisation $\widetilde{K} = K(\sqrt{\gamma})$ du plongement. Soit S l'ensemble des nombres premiers p de $\mathbb{Z}$ au-dessous d'un idéal premier de K ramifié dans $\widetilde{K}$.

Si p appartenant à S est ramifié dans k, alors p est impair, donc modéré dans $\widetilde{K}/K$, et par la théorie de Kummer le changement de γ en $p\gamma$ élimine la ramification en p (il faut remarquer que l'indice de ramification d'un idéal de K au-dessus de p est impair et que la valuation de γ en deux idéaux au-dessus de p a même parité). On se ramène donc à une réalisation du plongement pour laquelle les éléments de S sont non ramifiés dans k.

Si p appartenant à S est non ramifié dans N, alors le lemme suivant permet de conclure. Il nous a été communiqué par J.-P. Serre et nous reproduisons sa démonstration :

2.4. Lemme ([S4]). *Soit $1 \to C \to \widetilde{G} \to G \to 1$ une extension centrale de groupes finis, et soit $G_{\mathbb{Q}}$ le groupe de Galois absolu de $\mathbb{Q}$. Soit $\pi : G_{\mathbb{Q}} \to G$ un homomorphisme continu, et soit S l'ensemble des p où π est ramifié. Supposons que π soit relevable en $\widetilde{\pi} : G_{\mathbb{Q}} \to \widetilde{G}$. Alors on peut choisir un tel relèvement qui soit non ramifié en dehors de S.*

Démonstration. Soit $\widetilde{\pi}_1$ un choix quelconque d'un relèvement de π, et soit S_1 l'ensemble des p où $\widetilde{\pi}_1$ est ramifié. Soit p appartenant à $S_1 \setminus S$. Il suffit de montrer que l'on peut construire un relèvement $\widetilde{\pi}_2$ de π ayant pour ensemble de ramification $S_1 \setminus \{p\}$.

Soit I_p (respectivement D_p) le groupe d'inertie (respectivement de décomposition) de p dans $G_{\mathbb{Q}}$ (défini à conjugaison près). L'homomorphisme $\widetilde{\pi}_1$ applique I_p dans C; de plus $\widetilde{\pi}_1(D_p)/\widetilde{\pi}_1(I_p)$ est cyclique, donc $\widetilde{\pi}_1(D_p)$ est abélien. Par la théorie locale du corps de classes, on peut donc voir $\widetilde{\pi}_1|D_p$ comme un homomorphisme $g_p : \mathbb{Q}_p^* \to \widetilde{G}$, homomorphisme dont la restriction à $\mathbb{Z}_p^*$ a une image dans C. Soit $e_p : \mathbb{Z}_p^* \to C$ l'homomorphisme ainsi obtenu. En utilisant maintenant le fait que $G_{\mathbb{Q}}^{\mathrm{ab}}$ s'identifie au produit des groupes d'inertie locaux $\mathbb{Z}_p^*$, on voit qu'il existe un homomorphisme $e : G_{\mathbb{Q}} \to C$ et un seul qui est non ramifié en dehors de p, et dont la restriction à $\mathbb{Z}_p^*$ vu comme groupe d'inertie en p est égale à e_p. On pose $\widetilde{\pi}_2 = e^{-1}\widetilde{\pi}_1$.

C'est bien un relèvement de π qui a pour ensemble de ramification $S_1 \setminus \{p\}$. ∎

Le théorème suivant montre encore une analogie entre le cas des extensions bicycliques plongeables dans des quaternioniennes et celui des extensions de type A_4 dans des $\widetilde{A}_4$. En effet, J. Martinet a remarqué que, lorsque le plongement dans une extension quaternionienne est possible, alors le nombre de classes au sens restreint de l'extension bicyclique est pair (indication : les corps bicycliques dont le nombre de classes au sens restreint est impair sont les corps $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ où p_1 et p_2 sont des nombres premiers congrus à 1 modulo 4 (ou $p_2 = 2$) et tels que $\left(\frac{p_1}{p_2}\right) = -1$. On vérifie que l'invariant de Witt de la forme $\mathrm{Tr}(x^2)$ est alors l'algèbre de quaternions sur $\mathbb{Q}$ ramifiée en p_1 et en p_2).

2.5. Théorème. *Si K est de degré 4 sur $\mathbb{Q}$, de groupe de Galois A_4 et totalement réel, alors le nombre de classes au sens restreint h_K^+ de K est pair.*

Démonstration. Si l'extension N/k est non ramifiée, alors, d'après le corollaire 1.4, K est plongeable, et, d'après le théorème 2.2, il existe un "$\widetilde{A}_4$ pur", c'est-à-dire une extension quadratique de K, de groupe de Galois $\widetilde{A}_4$ sur $\mathbb{Q}$, et non ramifiée sur K sauf peut-être à l'infini. Le nombre de classes au sens restreint de K est donc pair.

Si l'extension N/k est ramifiée au-dessus du nombre premier p de $\mathbb{Z}$, alors il existe un idéal I de K tel que $pO_K = I^2$ (cf. [K1], [K2]). Alors, soit I est d'ordre 2 dans le groupe des classes de K, et donc h_K est pair, soit il est principal; dans ce cas, si θ_p est un générateur de I alors $\theta_p^2/p = \varepsilon_p$ est une unité totalement positive et non carrée dans K. ∎

2.6. Remarque. Les unités ε_p obtenues de cette façon sont indépendantes dans le $\mathbb{F}_2$-espace vectoriel E_K^+/E_K^2 (c'est le quotient du groupe des unités totalement positives par les carrés d'unités), car K ne contient pas d'extension quadratique de $\mathbb{Q}$. En particulier, si h_K est impair, alors h_K^+/h_K est supérieur ou égal à 2^r, où r est le nombre de nombres premiers de $\mathbb{Z}$ ramifiés dans N/k. De plus, si ε_p est une unité obtenue de cette façon, alors $K(\sqrt{\varepsilon_p}) = K(\sqrt{p})$; le groupe de Galois sur $\mathbb{Q}$ de $K(\sqrt{\varepsilon_p})$ est donc isomorphe à $A_4 \times \mathbb{Z}/2\mathbb{Z}$.

3. Résultats numériques. On applique ici les résultats des paragraphes précédents aux 31 corps de type A_4 extraits des tables [BPS] de corps réels, de degré 4 sur $\mathbb{Q}$, de discriminant inférieur à 10^6.

Elles donnent pour chaque corps K de discriminant d_K, un polynôme définissant l'extension, une base de l'anneau des entiers, une base $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ du groupe des unités et la valeur du nombre de classes h_K de K. On note h_K^+ le nombre de classes au sens restreint de K.

En particulier, on trouve les discriminants minimaux de corps de type $\widetilde{A}_4$ totalement réel (277^4) et totalement imaginaire (163^4).

Les trois cas de la proposition suivante recouvrent les 31 corps sauf les deux corps non plongeables (de discriminants 520^2 et 728^2) et quatre autres corps (de discriminants 688^2, 703^2, 711^2, 995^2).

3.1. PROPOSITION. 1) *Si* $d_K = d_k$, $h_K \equiv 1 \bmod 2$, $h_K^+ \equiv 2 \bmod 4$, *alors* k *est plongeable et le "*$\widetilde{A}_4$ *pur" est* $\widetilde{K} = K(\sqrt{-\varepsilon})$, *où* ε *est l'unique* (*modulo les carrés*) *unité totalement positive.*

2) *Si* $d_K = d_k$, $h_K = h_K^+ \equiv 2 \bmod 4$, *alors, si* I *est un idéal de* K *non principal de carré principal,* I^2 *est engendré par un unique* (*modulo les carrés*) *élément totalement positif* γ, *et le "*$\widetilde{A}_4$ *pur" est* $K(\sqrt{\gamma})$.

3) *Si* K/k *est ramifiée en un seul nombre premier* p *de* $\mathbb{Z}$, *si* $h_K \equiv 1 \bmod 2$ *et* $h_K^+ \equiv 2 \bmod 4$, *alors : il existe un idéal* I *de* K *tel que* $(p) = I^2$ (*ou, si* $p = 2$ *et si* 2 *a* 4 *pour indice de ramification dans* K, $(2) = I^4$); *cet idéal est principal et si* γ *et* $\varepsilon\gamma$ *sont les deux générateurs totalement positifs de* I *modulo les carrés d'unités, alors les quatre corps* $K(\sqrt{\gamma})$, $K(\sqrt{-\gamma})$, $K(\sqrt{\varepsilon\gamma})$, $K(\sqrt{-\varepsilon\gamma})$ *sont des* $\widetilde{A}_4$, *et ils ont même ramification sur* K, *sauf éventuellement en* 2 (*et à l'infini*). *Ceux pour lesquels la ramification en* 2 *est minimale sont des "*$\widetilde{A}_4$ *purs".*

Démonstration. 1) K est plongeable d'après la proposition 1.3, et il existe une réalisation $\widetilde{K}$ du plongement non ramifiée sur K d'après le théorème 2.2. Comme h_K est impair et $h_K^+/h_K = 2$, $\widetilde{K} = K(\sqrt{-\varepsilon})$ ($K(\sqrt{\varepsilon})$ est ramifiée en 2 puisque h_K est impair).

2) K est plongeable d'après la proposition 1.3, et il existe une réalisation $\widetilde{K}$ du plongement non ramifiée sur K d'après le théorème 2.2. Comme $h_K^+/h_K = 1$, $\widetilde{K} = K(\sqrt{\alpha})$ avec $(\alpha) = J^2$, et J est un idéal de K non principal. Donc α est totalement positif et n'importe quel idéal non principal de carré principal convient.

3) K est plongeable d'après la proposition 1.3, et il existe une réalisation du plongement $\widetilde{K} = K(\sqrt{\alpha})$ ramifiée en p, et non ramifiée en dehors de p d'après le théorème 2.2. Comme h_K est impair, on peut prendre pour α un générateur de I (si $p = 2$, α ne peut pas être une unité car la seule unité totalement positive ε donne un $A_4 \times \mathbb{Z}/2\mathbb{Z}$, voir Remarque 1.5). Donc I a un générateur γ totalement positif, et α est, modulo K^{*2}, l'un des quatre éléments : $\pm\gamma$, $\pm\varepsilon\gamma$. Les quatre extensions quadratiques de K correspondantes sont des $\widetilde{A}_4$ car $K(\sqrt{\varepsilon})$ est un $A_4 \times \mathbb{Z}/2\mathbb{Z}$.

Si $p \neq 2$, il y a parmi ces quatre corps exactement deux corps non ramifiés en 2; ce sont donc deux "$\widetilde{A}_4$ purs"; si $p \equiv 1 \bmod 4$, ils ont même signature, et si $p \equiv -1 \bmod 4$, l'un est réel et l'autre est totalement imaginaire.

Si $p = 2$, les quatre corps ont le même discriminant, qui est $d_K^2 \cdot 2^{10}$. ∎

La proposition précédente permet de calculer le discriminant et un polynôme minimal d'un plongement pur de 25 des 29 corps plongeables de la table. A titre d'exemple, nous avons effectué les calculs pour les neuf corps K de discriminant inférieur ou égal à 511^2; on trouve au moins une fois chaque cas de la proposition. Les quatre cas "exceptionnels" sont traités plus loin.

Les résultats sont regroupés dans le tableau numérique de la fin du paragraphe. En particulier nous avons démontré :

3.2. Proposition. 1) *Le plus petit discriminant pour un corps totalement imaginaire de degré* 8 *de groupe de Galois* $\widetilde{A}_4$ *est* 163^4. *Il est atteint par le corps défini par le polynôme* $X^8+14X^6+23X^4+9X^2+1$, *et uniquement par celui-ci à conjugaison près.*

2) *Le plus petit discriminant pour un corps totalement réel de degrée* 8 *de groupe de Galois* $\widetilde{A}_4$ *est* 277^4. *Il est atteint par le corps défini par le polynôme* $X^8-22X^6+123X^4-150X^2+49$, *et uniquement par celui-ci à conjugaison près.*

Dans les quatre cas échappant à la proposition 3.1, les résultats des paragraphes précédents ne suffisent pas à déterminer un plongement effectif : ils laissent encore plusieurs possibilités pour $K(\sqrt{\gamma})$. Pour déterminer celles réalisant le plongement, on peut utiliser la résolvante Φ de degré 12 définie dans [H-K, Théorème 5.2]. Regardons par exemple le cas des deux corps de discriminant respectif 703^2 et 711^2. Pour ces deux corps, $d_K = d_k$, donc il existe une réalisation du plongement non ramifiée sur K. Dans les deux cas, $h_K = 2$ et $h_K^+ = 4$. Elle peut donc être *a priori* de la forme $K(\sqrt{\varepsilon})$ avec ε unité de K, ou de la forme $K(\sqrt{\gamma})$ avec $(\gamma) = I^2$ et I est un idéal non principal de K.

Le corps K de discriminant 703^2 est défini par le polynôme $X^4-2X^3-19X^2+19X+19$. Une unité totalement positive est $\varepsilon = -4/9\theta^3+1/9\theta^2+80/9\theta+64/9$.

La résolvante définie dans [H-K] montre que $K(\sqrt{\varepsilon})$ a pour groupe de Galois $\widetilde{A}_4$. C'est donc le plongement "pur"; son discriminant est 703^4 et il est défini par le polynôme $X^8-22X^6+47X^4-23X^2+1$.

Un calcul semblable pour le corps de discriminant 711^2 conduit au polynôme $X^8-17X^6+60X^4-29X^2+1$.

Les deux autres cas sont traités de la même façon; les résultats figurent dans le tableau suivant.

La troisième colonne donne le discriminant et un polynôme définissant un plongement $\widetilde{K}$ de K de plus petit discriminant. La notation (Re) (respectivement (Im)) signifie que ce plongement est totalement réel (respectivement totalement imaginaire). Les corps de discriminant 183^2, 248^2, 407^2, 473^2, 511^2 on aussi un plongement totalement imaginaire de même discriminant.

$d_K = 163^2,\ \ d_k = 163^2$	$h_K = 1$	$d_{\widetilde{K}} = 163^4$ (Im)
$X^4 - 2X^3 - 7X^2 + 3X + 8$	$h_K^+ = 2$	$X^8 + 14X^6 + 23X^4 + 9X^2 + 1$
$d_K = 183^2 = (61 \cdot 3)^2,\ \ d_k = 61^2$	$h_K = 1$	$d_{\widetilde{K}} = 3^6 \cdot 61^4$ (Re)
$X^4 - 7X^2 - 3X + 1$	$h_K^+ = 2$	$X^8 - 54X^6 + 891X^4 - 4131X^2 + 729$
$d_K = 248^2 = 31^2 \cdot 2^6,\ \ d_k = 31^2$	$h_K = 1$	$d_{\widetilde{K}} = 2^{22} \cdot 31^4$ (Re)
$X^4 - 2X^3 - 7X^2 + 6X + 11$	$h_K^+ = 2$	$X^8 - 12X^6 + 42X^4 - 40X^2 + 4$
$d_K = 277^2,\ \ d_k = 277^2$	$h_K = 2$	$d_{\widetilde{K}} = 277^4$ (Re)
$X^4 - X^3 - 16X^2 + 3X + 1$	$h_K^+ = 2$	$X^8 - 22X^6 + 123X^4 - 150X^2 + 49$
$d_K = 349^2,\ \ d_k = 349^2$	$h_K = 1$	$d_{\widetilde{K}} = 349^4$ (Im)
$X^4 - X^3 - 10X^2 + 3X + 20$	$h_K^+ = 2$	$X^8 + 121X^6 + 87X^4 + 18X^2 + 1$
$d_K = 397^2,\ \ d_k = 397^2$	$h_K = 1$	$d_{\widetilde{K}} = 397^4$ (Im)
$X^4 - 13X^2 - 2X + 19$	$h_K^+ = 2$	$X^8 + 108X^6 + 422X^4 + 236X^2 + 1$
$d_K = 407^2 = (11 \cdot 37)^2,\ \ d_k = 37^2$	$h_K = 1$	$d_{\widetilde{K}} = 11^6 \cdot 37^4$ (Re)
$X^4 - 2X^3 - 9X^2 - X + 3$	$h_K^+ = 2$	$X^8 - 539X^6 + 6347X^4 - 18150X^2 + 121$
$d_K = 473^2 = (11 \cdot 43)^2,\ \ d_k = 43^2$	$h_K = 1$	$d_{\widetilde{K}} = 11^6 \cdot 43^4$ (Re)
$X^4 - X^3 - 16X^2 - 7X + 27$	$h_K^+ = 2$	$X^8 - 594X^6 + 1815X^4 - 1210X^2 + 121$
$d_K = 511^2 = (7 \cdot 73)^2,\ \ d_k = 73^2$	$h_K = 1$	$d_{\widetilde{K}} = 7^6 \cdot 73^4$ (Re)
$X^4 - X^3 - 9X^2 + 2X + 11$	$h_K^+ = 2$	$X^8 - 35X^6 + 371X^4 - 1078X^2 + 49$
$d_K = 688^2 = 43^2 \cdot 2^8,\ \ d_k = 43^2$	$h_K = 2$	$d_{\widetilde{K}} = 2^{24} \cdot 43^4$ (Re)
$X^4 - 10X^2 - 4X + 6$	$h_K^+ = 4$	$X^8 - 24X^6 + 92X^4 - 80X^2 + 4$
$d_K = 703^2 = (19 \cdot 37)^2,\ \ d_k = 703^2$	$h_K = 2$	$d_{\widetilde{K}} = 703^4$ (Re)
$X^4 - 2X^3 - 19X^2 + 19X + 19$	$h_K^+ = 4$	$X^8 - 22X^6 + 47X^4 - 23X^2 + 1$
$d_K = 711^2 = 3^4 \cdot 79^2,\ \ d_k = 711^2$	$h_K = 2$	$d_{\widetilde{K}} = 711^4$ (Re)
$X^4 - X^3 - 24X^2 + X + 11$	$h_K^+ = 4$	$X^8 - 17X^6 + 60X^4 - 29X^2 + 1$
$d_K = 995^2 = (5 \cdot 199)^2,\ \ d_k = 199^2$	$h_K = 2$	$d_{\widetilde{K}} = 5^6 \cdot 199^4$ (Re)
$X^4 - X^3 - 32X^2 + 23X + 224$	$h_K^+ = 4$	$X^8 - 2865X^6 + 15530X^4 - 2725X^2 + 100$

Bibliographie

[B] S. Böge, *Witt-Invariante und ein gewisses Einbettungsproblem*, J. Reine Angew. Math. 410 (1990), 153–159.

[BPS] J. Buchman, M. Pohst and J. v. Schmettow, *On the computation of unit groups and class groups of totally real quartic fields*, Math. Comp. 52 (185) (1989), 161–174.

[BMcK] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra 11 (8) (1983), 863–911.

[C1] T. Crespo, *Explicit construction of $\widetilde{A}_n$ type fields*, J. Algebra 127 (1989), 452–461.

[C2] —, *Embedding problems with ramification conditions*, J. Number Theory, to appear.

[H-K] F.-P. Heider and P. Kolvenbach, *The construction of* $\mathrm{Sl}(2,3)$*-polynomials*, J. Number Theory 19 (1984), 392–411.

[K] P. Kolvenbach, *Zur algebraischen und arithmetischen Theorie der* $\mathrm{Sl}(2,3)$*-Erweiterungen*, Dissertation, Köln 1982.

[K1] S.-H. Kwon, *Extensions à groupe de Galois A_4*, Thèse, Univ. Bordeaux I, 1984.

[K2] —, *Corps de nombres de degré* 4 *de type alterné*, C. R. Acad. Sci. Paris 299 (2) (1984), 41–43.

[M] J. Martinet, *Discriminants and permutation groups*, dans : Number Theory, R. Mollin (éd.), Walter de Gruyter, Berlin 1990, 359–385.

[Sc] I. Schur, *Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen*, J. Crelle 139 (1911), 155–250 (= Ges. Abh. I, 346–441).

[S1] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (1984), 651–676 (= Oeuvres, Vol. III, 675–700).

[S3] —, *Corps locaux*, 3e éd., Hermann, Paris 1980.

[S4] —, Lettre à J. Martinet du 15/11/89.

[Sp] T. A. Springer, *Sur les formes quadratiques d'indice zéro*, C. R. Acad. Sci. Paris 244 (1952), 1517–1519.

[W] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Reine Angew. Math. 174 (1936), 237–245.

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ DE BORDEAUX I
351 COURS DE LA LIBÉRATION
F-33400 TALENCE CEDEX, FRANCE

Reçu le 11.2.1991 (2121)