ACTA ARITHMETICA
LXIX.3 (1995)

Sur les extensions de $\mathbb{Q}$ à groupe de Galois S_4 et $\widetilde{S}_4$

par

Arnaud Jehanne (Talence)

Introduction. Soient k_0 un corps et k_0^{s} une clôture séparable de k_0. Soit K/k_0 une sous-extension de k_0^{s}/k_0 de clôture galoisienne N/k_0. Le groupe de Galois G de N/k_0 peut être vu comme groupe de permutations sur les racines d'un polynôme définissant K/k_0, isomorphe à un sous-groupe du groupe symétrique S_n. I. Schur a démontré que pour $n \geq 4$, $H^2(S_n, \{\pm 1\})$ est bicyclique d'ordre 4. Il existe donc à isomorphisme près trois extensions centrales non triviales de S_n par $\{\pm 1\}$.

Dans ce travail, nous considérons l'extension $\widetilde{S}_n$ de S_n notée II′ dans [Sc], p. 164 et décrite dans [Se1], p. 654, en nous limitant au cas $n = 4$. Dans $\widetilde{S}_n$, toute transposition de S_n est relevée en un élément d'ordre 2 et tout produit de deux transpositions à supports disjoints est relevé en un élément d'ordre 4. Ajoutons que l'on peut donner une interprétation géométrique de l'extension $\widetilde{S}_4$ de S_4, S_4 étant isomorphe à $\mathrm{PGL}_2(\mathbb{F}_3)$ et $\widetilde{S}_4$ à $\mathrm{GL}_2(\mathbb{F}_3)$. De façon générale, on définit l'extension $\widetilde{G}$ de G en plongeant G dans S_n.

L'étude décrite dans cette note s'inspire de l'article de C. Bachoc et S.-H. Kwon sur le groupe A_4 (voir [B-K]), qui admet une unique extension centrale non triviale par $\{\pm 1\}$, laquelle a une réalisation dans le groupe des quaternions usuels de norme 1 : $\{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$.

Ce travail considère le cas où $k_0 = \mathbb{Q}$ et où G est isomorphe à S_4. La première partie décrit les extensions à groupe de Galois S_4 et en étudie les ramifications. La seconde utilise un théorème de Serre ([Se1]) — qui permet de lier la possibilité de plonger N/k_0 dans une extension $\widetilde{N}/k_0$ de groupe de Galois $\widetilde{G}$ à la valeur de l'invariant de Witt de la forme quadratique $\mathrm{Tr}_{K/k_0}(x^2)$ — pour donner une condition suffisante de plongement portant sur les ramifications de nombres premiers dans l'extension $N/\mathbb{Q}$.

Dans une troisième partie, nous considérons le cas où $N/\mathbb{Q}$ est plongeable et cherchons à réaliser le plongement en minimisant le nombre de places ramifiées. La quatrième partie discute ensuite l'existence d'une classe au sens restreint d'ordre 2 dans la clôture galoisienne N de toute extension

quartique de $\mathbb{Q}$ de type S_4 dans le cas où N est plongeable dans une extension galoisienne de $\mathbb{Q}$ à groupe de Galois isomorphe à $\widetilde{S}_4$. En fait, nous démontrons l'existence d'une telle classe dans le cas où K est totalement réel, que N soit plongeable ou non (théorème IV.2), et donnons une condition suffisante d'existence dans le cas plongeable (théorème IV.3).

La dernière partie utilise le paragraphe III pour calculer des polynômes définissant les corps à groupe de Galois $\widetilde{S}_4$ qui réalisent les plongements de corps à groupe de Galois S_4 et de déterminer les discriminants minimaux des corps de degré 8 de type $\widetilde{S}_4$.

Dans le cas où $k_0 = \mathbb{Q}$ et où l'extension $\widetilde{G}$ de G (le groupe G n'étant pas nécessairement isomorphe à S_4) est non triviale (i.e. $\widetilde{G}$ n'est pas produit direct de G par un sous-groupe d'ordre 2), J. Martinet a conjecturé que le plongement $\widetilde{G} \to G$ n'est possible que lorsque le nombre de classes au sens restreint h_N^+ de N est pair. Quand G est isomorphe à S_4, le théorème IV.2 démontre cette conjecture dans le cas totalement réel, et même un résultat plus précis : le nombre de classes au sens restreint du sous-corps K' de N de degré 2 sur K est pair.

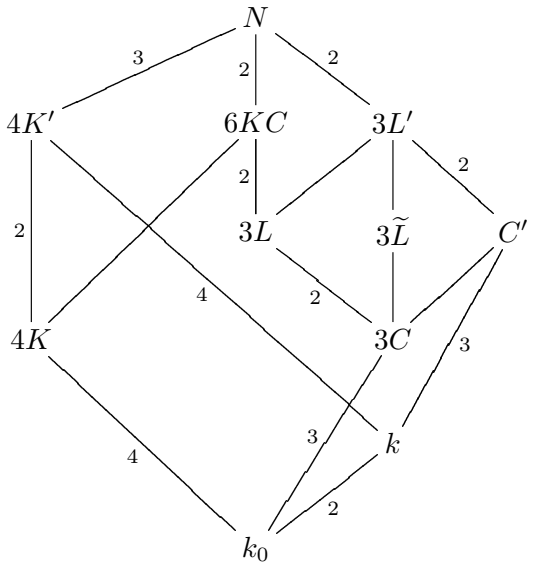
Toutefois, à la suite du théorème IV.3, nous donnons des contre-exemples à la parité de $h_{K'}^+$ dans le cas d'une signature mixte et exhibons même un exemple pour lequel h_N^+ est impair (cf. exemple 1, §IV). Le caractère semble-t-il largement aléatoire de la parité du nombre de classes dans une extension cubique donne à penser que le nombre de classes au sens restreint de N est souvent impair lorsque celui de K' l'est. Aussi, sans doute convient-il de se limiter aux corps totalement réels pour comparer la parité du nombre de classes au sens restreint et la possibilité de construire un plongement $\widetilde{G} \to G$, supposé non trivial.

Pour les exemples numériques, les calculs ont été faits à l'aide du logiciel PARI, réalisé par C. Batut, D. Bernardi, H. Cohen et M. Olivier à Bordeaux. Des tables de corps quartiques établies par J. Buchmann, D. Ford et M. Pohst (cf. [Bu-Fo] et [Bu-Fo-Po]) ont également été utilisées.

Remerciements. Je remercie Jacques Martinet pour m'avoir guidé dans ce travail, ainsi que Christine Bachoc et Francisco Diaz y Diaz pour m'avoir fait profiter de leur connaissance du sujet. Je remercie également Sigrid Böge et Philippe Cassou-Noguès pour leurs nombreuses remarques et suggestions.

I. Extensions à groupe de Galois S_4. Reprenons les notations de l'introduction avec $G \simeq S_4$ comme groupe de Galois de l'extension N/k_0. L'étude des sous-groupes de S_4 donne le diagramme de Hasse suivant :

Diagramme I.1 :



Le corps C est une extension cubique non galoisienne de k_0 de clôture galoisienne C' qui contient l'extension quadratique k de k_0 associée à K/k_0, c'est-à-dire l'extension définie par l'unique caractère d'ordre 2 de G. Soient H et g les groupes de Galois respectifs de N/K et de N/C, définis à conjugaison près dans G; H est isomorphe à S_3 et g au groupe diédral D_4 d'ordre 8. Les extensions N/L, N/C' et L'/C sont bicycliques d'ordre 4, $N/\widetilde{L}$ est cyclique d'ordre 4 et N/K est diédrale d'ordre 6. Si l'on identifie $\mathrm{Gal}(N/\mathbb{Q})$ à S_4 agissant par permutations des indices sur l'ensemble $\{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$ des racines d'un polynôme définissant K à conjugaison près, on prendra par exemple le corps K' (resp. KC, L') fixé par le sous-groupe de S_4 engendré par (123) (resp. (12), (12)(34)).

On définit une norme $\mathcal{N}_{C/k_0}$ du groupe des extensions quadratiques de C contenues dans N sur celui des extensions quadratiques de k_0 de la façon suivante : si L est une extension quadratique de C, il lui correspond un élément x de $H^1(g, \{\pm 1\})$. On notera $\mathcal{N}_{C/k_0}(L)$ l'extension quadratique de k_0 définie par $\mathrm{Cor}(x)$ où Cor est la corestriction de $H^1(g, \{\pm 1\})$ dans $H^1(G, \{\pm 1\})$ (voir [Ma], p. 365). La norme sur k_0 de l'extension C'/C est égale à k/k_0. Comme les normes des extensions $\widetilde{L}/C$ et L/C sont incluses dans N/k_0, on en déduit que l'une d'entre elles est triviale, l'autre étant égale à k/k_0.

Théorème I.2. *L'extension L/C est de norme triviale.*

P r e u v e. Soient x l'élément de $H^1(g, \{\pm 1\})$ correspondant à l'extension L/C et χ un élément de $\mathrm{Hom}(g, \{\pm 1\})$ représentant x (i.e. $\mathrm{Ker}(\chi)$ fixe L).

Tableau I.3

C	L	k	K	K'	Commentaire
$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''$	$\mathfrak{p}_1^2\mathfrak{p}_1'^2\mathfrak{p}_2''$	$\mathfrak{p}_1\mathfrak{p}_1'$	$\mathfrak{p}_2^2$	$\mathfrak{p}_2^2\mathfrak{p}_2'^2$	$G_{-1} \simeq C_2 \times C_2$ $G_{-1} \subset A_4$
$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''$	$\mathfrak{p}_1^2\mathfrak{p}_1'^2\mathfrak{p}_1''\mathfrak{p}_1'''$	$\mathfrak{p}_1\mathfrak{p}_1'$	$\mathfrak{p}_1^2\mathfrak{p}_1'^2$	$\prod_{i=1}^4 \mathfrak{p}_1^{(i)2}$	$G_{-1} = G_0 \subset A_4$ $\lvert G_0\rvert = 2$
$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''$	$\mathfrak{p}_1^2\mathfrak{p}_1'^2\mathfrak{p}_1''^2$	$\mathfrak{p}_1\mathfrak{p}_1'$	$\mathfrak{p}_1^4$	$\mathfrak{p}_1^4\mathfrak{p}_1'^4$	$G_{-1} = G_0 \subset A_4$ $G_0 \simeq C_2 \times C_2,\ p = 2$
$\mathfrak{p}_1\mathfrak{p}_2'$	$\mathfrak{p}_2^2\mathfrak{p}_1'\mathfrak{p}_1''$ ou $\mathfrak{p}_2\mathfrak{p}_2'^2$	$\mathfrak{p}_2$	$\mathfrak{p}_1^2\mathfrak{p}_1'^2$ ou $\mathfrak{p}_2^2$	$\mathfrak{p}_2^2\mathfrak{p}_2'^2$ ou $\mathfrak{p}_4^2$	$\lvert G_0\rvert = 2$ $G_0 \subset A_4$
$\mathfrak{p}_1\mathfrak{p}_2'$	$\mathfrak{p}_2^2\mathfrak{p}_1'^2$	$\mathfrak{p}_2$	$\mathfrak{p}_1^4$	$\mathfrak{p}_2^4$	$G_0 \simeq C_2 \times C_2$, $p = 2$ $G_{-1} \simeq D_4$, $G_0 \subset A_4$
$\mathfrak{p}_1\mathfrak{p}_1'^2$	$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''^4$ ou $\mathfrak{p}_2\mathfrak{p}_1'^4$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^2\mathfrak{p}_1'^2$ ou $\mathfrak{p}_2^2$	$\mathfrak{p}_1^4\mathfrak{p}_1'^4$ ou $\mathfrak{p}_2^4$	$G_0 \simeq C_2 \times C_2$ $G_0 \not\subseteq A_4$, $p = 2$
$\mathfrak{p}_1\mathfrak{p}_1'^2$	$\mathfrak{p}_1^2\mathfrak{p}_1'^4$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^4$	$\mathfrak{p}_1^4\mathfrak{p}_1'^4$ ou $\mathfrak{p}_2^4$	G_0 cyclique d'ordre 4
$\mathfrak{p}_1\mathfrak{p}_1'^2$	$\mathfrak{p}_1^2\mathfrak{p}_1'^4$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^4$	$\mathfrak{p}_1^8$	$G_0 \simeq D_4$ $p = 2$
$\mathfrak{p}_1\mathfrak{p}_1'^2$	$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''^2\mathfrak{p}_1'''^2$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''^2$	$\mathfrak{p}_1^2\mathfrak{p}_1'^2\mathfrak{p}_1''^2\mathfrak{p}_1'''^2$	$\lvert G_0\rvert = 2$ $G_0 \not\subseteq A_4$
$\mathfrak{p}_1\mathfrak{p}_1'^2$	$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_2''^2$	$\mathfrak{p}_1^2$	$\mathfrak{p}_2\mathfrak{p}_1'^2$	$\mathfrak{p}_2^2\mathfrak{p}_2'^2$	$\lvert G_0\rvert = 2$, $G_0 \not\subseteq A_4$ $G_{-1} \simeq C_2 \times C_2$
$\mathfrak{p}_1^3$	$\mathfrak{p}_1^3\mathfrak{p}_1'^3$	$\mathfrak{p}_1\mathfrak{p}_1'$ ou $\mathfrak{p}_2$	$\mathfrak{p}_1^3\mathfrak{p}_1'$	$\mathfrak{p}_1^3\mathfrak{p}_1'^3\mathfrak{p}_1''\mathfrak{p}_1'''$ ou $\mathfrak{p}_2^3\mathfrak{p}_2'$	$\lvert G_0\rvert = 3$
$\mathfrak{p}_1^3$	$\mathfrak{p}_1^3\mathfrak{p}_1'^3$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^3\mathfrak{p}_1'$	$\mathfrak{p}_1^6\mathfrak{p}_1'^2$	$\lvert G_0\rvert = 6$ $p = 3$
$\mathfrak{p}_1^3$	$\mathfrak{p}_1^6$	$\mathfrak{p}_1\mathfrak{p}_1'$ ou $\mathfrak{p}_2$	$\mathfrak{p}_1^4$	$\mathfrak{p}_1^4\mathfrak{p}_1'^4$ ou $\mathfrak{p}_2^4$	$G_0 \simeq A_4$ $p = 2$

Soit $\mathrm{Ver}_{k_0}^C$ le transfert de G^{ab} vers g^{ab}, où G^{ab} et g^{ab} sont les groupes G et g rendus abéliens. Comme $L = N^{\mathrm{Ker}(\chi)}$, $\mathcal{N}_{C/k_0}(L) = N^{\mathrm{Ker}(\chi\circ\mathrm{Ver}_{k_0}^C)}$. Par conséquent, nous sommes ramenés à montrer que $\chi \circ \mathrm{Ver}_{k_0}^C$ est trivial. Le quotient g^{ab} est représenté par l'ensemble $\{1, \tau, \sigma, \tau\sigma\}$ où τ est une transposition et σ un élément d'ordre 4 de g. Soit c un élément d'ordre 3 de G tel que $\langle c, \tau\rangle$ soit isomorphe au groupe symétrique S_3 d'ordre 6. Le quotient G^{ab} est représenté par $\{1, \tau\}$ et G/g par $S = \{1, c, c^2\}$. Quand on écrit pour $t \in S$: $t\tau = a(t,\tau) \cdot b(t,\tau)$, où $a(t,\tau) \in g$ et $b(t,\tau) \in S$, on voit que la permutation $a(t,\tau)$ est une transposition puisqu'elle est impaire et contenue dans $\langle c, \tau\rangle$. Ainsi, $\prod_{t\in S} a(t,\tau)$, qui vérifie les mêmes propriétés, est l'élément de G^{ab}

représenté par les transpositions de g. Comme $\mathrm{Gal}(N/KC)$ est engendré par une transposition, $\chi \circ \mathrm{Ver}_{k_0}^{C}$ est bien trivial. ∎

On suppose que k_0 est le corps des fractions d'un anneau de Dedekind A, à corps résiduels parfaits, relativement auquel sont définis les conducteurs. Le groupe G possède cinq caractères irréductibles. Trois d'entre eux relèvent les caractères irréductibles du groupe symétrique S_3 : le caractère trivial 1, le caractère de signature ε (dont le noyau fixe k) et un caractère φ de degré 2. Les deux autres sont des caractères fidèles de degré 3, notés χ et χ', où χ est la représentation naturelle de S_4 dans $\mathbb{R}^3$ et où $\chi' = \varepsilon\chi$ (voir par exemple [Se3]). Soit ψ le relèvement à g du caractère non trivial de $\mathrm{Gal}(L/C)$. On vérifie que χ est induit par ψ et que le caractère de permutation de G/H est égal à $1 + \chi$. Ainsi, $\mathfrak{d}_{K/k_0} = \mathfrak{d}_{C/k_0} \cdot N_{C/k_0}(\mathfrak{d}_{L/C})$. Comme $N_{C/k_0}(\mathfrak{d}_{L/C})$ est un carré, on obtient $\mathfrak{d}_{K/k_0} = \mathfrak{d}_{C/k_0} \cdot \mathfrak{g}^2 = \mathfrak{d}_{k/k_0} \cdot (\mathfrak{f} \cdot \mathfrak{g})^2$, où $\mathfrak{f}$ est l'idéal de A tel que $\mathfrak{d}_{C/k_0} = \mathfrak{d}_{k/k_0} \cdot \mathfrak{f}^2$. En particulier, la ramification dans K d'un idéal premier quelconque de k_0 se lit dans les extensions C/k_0 et L/C. Si $k_0 = \mathbb{Q}$, on a $d_K = d_k(fg)^2 = d_C g^2$, où f et g sont des entiers strictement positifs.

Posons $k_0 = \mathbb{Q}$. Soit p un nombre premier ramifié dans K et $\mathfrak{P}$ un idéal de $\mathcal{O}_N$ au-dessus de p. On note respectivement G_{-1} et G_0 le groupe de décomposition et le groupe d'inertie de $\mathfrak{P}$ dans $N/\mathbb{Q}$. Le tableau I.3 donne les décompositions possibles de p dans les corps C, L, k, K et K'. (Dans ce tableau, C_2 désigne un groupe d'ordre 2.)

II. Le problème de plongement $\widetilde{S}_4 \to S_4$. Reprenons les notations du paragraphe I. Si l'on suppose l'extension N/k_0 plongeable dans une extension $\widetilde{N}/k_0$ à groupe de Galois isomorphe à S_4, la caractérisation de $\widetilde{S}_n$ donnée dans l'introduction montre que l'extension $\widetilde{N}/K'$ est cyclique d'ordre 6. De plus, on peut décrire un 2-sous-groupe de Sylow de $\widetilde{S}_4$ à l'aide de la présentation suivante : $\langle \widetilde{\tau}, \widetilde{\sigma} : \widetilde{\tau}^2 = \widetilde{\sigma}^8 = 1;\ \widetilde{\tau}\widetilde{\sigma}\widetilde{\tau}^{-1} = \widetilde{\sigma}^3 \rangle$. Soit $\widetilde{K}'$ l'unique extension quadratique de K' contenue dans $\widetilde{N}$; on remarque que $\widetilde{K}'$ est une extension bicyclique de degré 4 de K. On note $\widetilde{K}$ et K'' les deux extensions quadratiques de K distinctes de K' contenues dans $\widetilde{K}'$. Les deux extensions $\widetilde{N}/\widetilde{K}$ et $\widetilde{N}/K''$ sont diédrales d'ordre 6. Par la suite, nous dirons que K est *plongeable* dans le cas où l'extension N/k_0 sera plongeable dans une extension $\widetilde{N}$ à groupe de Galois isomorphe à $\widetilde{S}_4$.

Comme l'extension C/k_0 est de degré impair, on montre :

PROPOSITION II.1. *L'extension N/k_0 est plongeable dans une extension de groupe de Galois $\widetilde{G}$ si et seulement si l'extension N/C est plongeable dans une extension de groupe de Galois $\widetilde{g}$, extension centrale correspondant à* $\mathrm{Res}(x)$, *où* Res *est la restriction de $H^2(G, \{\pm 1\})$ dans $H^2(g, \{\pm 1\})$ et x l'élément de $H^2(G, \{\pm 1\})$ correspondant à $\widetilde{G}$.

P r e u v e. 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. L'extension N/k_0 est plongeable si et seulement s'il existe un relèvement $\widetilde{\pi} : G_{k_0} \to \widetilde{G}$ de π rendant commutatif le diagramme suivant :

$$\begin{array}{ccccc} 1 \to \{\pm 1\} \to \widetilde{G} & \xrightarrow{q} & G & \to 1 \\ & \widetilde{\pi}\nwarrow & \uparrow \pi & \\ & & G_{k_0} & \end{array}$$

Soit π^* l'application de $H^2(G, \{\pm 1\})$ dans $H^2(G_{k_0}, \{\pm 1\})$ induite par π. L'existence de $\widetilde{\pi}$ équivaut à la condition $\pi^* x = 1$. Considérons le diagramme commutatif

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

Comme $[G : g] = [G_{k_0} : G_C] = 3$, les restrictions sont injectives et

$$\pi^* x = 1 \Leftrightarrow (\pi|_{G_C})^*(\mathrm{Res}(x)) = 1. \ \blacksquare$$

Posons maintenant $k_0 = \mathbb{Q}$ et déterminons les conditions de plongement portant sur la signature de K. Dans [Se1], J.-P. Serre démontre que K est plongeable dans un $\widetilde{K}$ si et seulement si l'une des conditions équivalentes suivantes est réalisée :

(1) $\omega_2(\mathrm{Tr}_{K/\mathbb{Q}}(x^2)) = (2, d_K)$,
(2) $\mathrm{Tr}_{K/\mathbb{Q}}(x^2) \sim X_1^2 + X_2^2 + 2X_3^2 + 2d_K X_4^2$,

où $\omega_2(\mathrm{Tr}_{K/\mathbb{Q}}(x^2))$ est l'invariant de Witt de la forme quadratique $\mathrm{Tr}_{K/\mathbb{Q}}(x^2)$ et où $(\ ,\ )$ désigne le symbole de Hilbert.

Comme $\mathrm{Tr}_{K/\mathbb{Q}}(x^2) = \sum_{i=1}^{4} \sigma_i(x^2)$ où les σ_i sont les plongements de K dans $\mathbb{C}$, on en déduit que si K est plongeable, alors sa signature est $(4, 0)$ quand d_K est positif ou $(2, 1)$ quand d_K est négatif. Pour déterminer la signature de $\widetilde{K}$ dans chacun de ces cas, donnons une condition nécessaire sur $\gamma \in K$ pour que $K(\sqrt{\gamma})$ réalise le plongement. On peut voir $\widetilde{S}_4$ comme un groupe de permutation de degré 8 impair qui agirait sur les racines d'un polynôme définissant $\widetilde{K}/\mathbb{Q}$. Ce groupe de permutation admet un unique caractère d'ordre 2 dont le noyau, quand il agit sur $\widetilde{N}$, fixe le corps k. Ainsi, $d_{\widetilde{K}} \in d_k \mathbb{Q}^{*2} = d_K \mathbb{Q}^{*2}$. Or, $d_{\widetilde{K}} \equiv N_{K/\mathbb{Q}}(\gamma) \bmod \mathbb{Q}^{*2}$, et si les γ_i où $i \in \{1, 2, 3, 4\}$ sont les conjugués de γ, le produit $\gamma_1\gamma_2\gamma_3\gamma_4$ appartient à $d_K \mathbb{Q}^{*2}$. Comme $N(\sqrt{\gamma})/\mathbb{Q}$ est galoisienne, $\gamma_i\gamma^{-1}$ est un carré de N. Si K est totalement réel, le corps N est également totalement réel et $\gamma_i\gamma^{-1}$ est totalement positif pour tout $i \in \{1, 2, 3, 4\}$. La signature de $K(\sqrt{\gamma})$ est donc $(8, 0)$ (resp. $(0, 4)$) quand γ est totalement positif (resp. quand γ est totalement négatif). Si maintenant K est de signature $(2, 1)$, on peut choisir

les σ_i tels que $\sigma_1(\gamma)$ et $\sigma_2(\gamma)$ soient réels et que $\sigma_4(\gamma) = \overline{\sigma_3(\gamma)}$. Alors, comme d_K est négatif, $\sigma_1(\gamma)\sigma_2(\gamma)$ est négatif et $K(\sqrt{\gamma})$ est de signature $(2,3)$.

On peut maintenant énoncer une condition suffisante de plongement de N dans un $\widetilde{N}$:

PROPOSITION II.2. *Si K est totalement réel ou de signature mixte, si l'extension $k/\mathbb{Q}$ n'est ramifiée qu'en un nombre premier p et si l'extension L/C est non ramifiée, alors N est plongeable.*

Cette proposition est une conséquence directe de la proposition II.1 et du lemme II.3 suivant qu'on applique à l'extension N/C (après avoir vérifié que cette extension N/C est alors ramifiée en un et un seul idéal premier de C). Ce lemme II.3 est dû à J.-P. Serre et m'a été communiqué par C. Bachoc.

LEMME II.3. *Soit $1 \to \mu \to \widetilde{\Gamma} \to \Gamma \to 1$ une extension centrale de groupes finis, où μ est un groupe fini de racines de l'unité. Soient E un corps de nombres contenant μ et G_E le groupe de Galois absolu de E. Soit $\pi : G_E \to \Gamma$ un homomorphisme continu définissant une extension galoisienne F/E. Pour toute place v de E et tout groupe G obtenu comme quotient de G_E, on note G_v le groupe de décomposition de v dans G, défini à conjugaison près.*

(1) *Une place v_0 étant donnée, supposons que pour toute place v de E distincte de v_0 l'homomorphisme $\pi|_{(G_E)_v}$ puisse être relevé en un homomorphisme*

$$\widetilde{\pi|_{(G_E)_v}} : (G_E)_v \to \widetilde{\Gamma}.$$

Alors il existe un relèvement $\widetilde{\pi} : G_E \to \widetilde{\Gamma}$ de π et donc, si la suite exacte n'est pas scindée, $\widetilde{\pi}$ est surjectif et F est plongeable dans un $\widetilde{F}$.

(2) *En particulier, si les conditions à l'infini pour que F/E soit plongeable dans une extension $\widetilde{F}/E$ à groupe de Galois isomorphe à $\widetilde{\Gamma}$ sont satisfaites et si un idéal au plus de E est ramifié dans F, alors π est relevable en un tel $\widetilde{\pi}$.*

P r e u v e. (1) Si l'on considère l'injection

$$i : H^2(G_E, \mu) \to \prod_v H^2((G_E)_v, \mu)$$

où $\mathrm{Im}(i) = \{(x_v)_v : \prod_v x_v = 1\}$ (voir par exemple [Se2], p. 171), on obtient $\pi^*_{\mathfrak{p}_0} x_{\mathfrak{p}_0} = 1$ et donc $\pi^* x = 1$, où x désigne l'élément de $H^2(\Gamma, \mu)$ définissant $\widetilde{\Gamma}$.

(2) Soit $\mathfrak{p}$ un idéal de E non ramifié dans F. Par la théorie locale du corps de classes, on peut voir $\pi|_{(G_E)_\mathfrak{p}}$ comme un homomorphisme $\pi_\mathfrak{p} : \widehat{\mathbb{Z}} \to \Gamma$ puisque $\widehat{\mathbb{Z}}$ est le groupe de Galois de l'extension maximale non ramifiée de E. Comme $\widehat{\mathbb{Z}}$ admet un générateur topologique, on peut relever $\pi_\mathfrak{p}$ en un $\widetilde{\pi}_\mathfrak{p}$

de $\widehat{\mathbb{Z}}$ dans $\widetilde{\Gamma}$. Ainsi, si $x_{\mathfrak{p}}$ est l'élément de $H^2(\Gamma,\mu)$ définissant $\widetilde{\Gamma}$, $\pi_{\mathfrak{p}}^* x_{\mathfrak{p}} = 1$. De plus, les conditions de plongement à l'infini sont vérifiées. Pour toute place infinie v de E, on a donc $\pi_v^* x_v = 1$ où $\pi_v = \pi|_{(G_E)_v}$. On peut alors conclure grâce au (1) du lemme. ∎

On peut enfin donner une condition nécessaire et suffisante de plongement portant sur la décomposition dans K des nombres premiers impairs ramifiés dans K. En effet, dans [Ba-Fr], p. 398, P. Bayer et G. Frey donnent les conditions locales de plongement en tout nombre premier p impair ramifié dans K. En utilisant la formule du produit, on en déduit :

Proposition II.4. *Supposons K totalement réel ou de signature mixte. Alors K est plongeable si et seulement si tout nombre premier p impair ramifié dans K vérifie les conditions suivantes* :

(1) $\quad p\mathcal{O}_K \neq \mathfrak{p}_1^2\mathfrak{p}_2'$,

(2) $\quad p\mathcal{O}_K = \mathfrak{p}_1^4 \Rightarrow p \equiv 1$ *ou* $3 \bmod 8$,

(3) $\quad p\mathcal{O}_K = \mathfrak{p}_2^2 \Rightarrow p \equiv 3 \bmod 4$,

(4) $\quad p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'^2 \Rightarrow \begin{cases} p \equiv 1 \bmod 4 & \text{si } (d_k,p)_p = 1, \\ p \equiv 3 \bmod 4 & \text{si } (d_k,p)_p = -1. \end{cases}$

Soit $\widetilde{N} = N(\sqrt{\gamma})$ une réalisation du plongement; alors les autres sont les $N(\sqrt{m\gamma})$ où $m \in \mathbb{Z} \setminus \{0\}$ (ce résultat transpose à S_4 le résultat de [Cr] qui envisage le cas alterné, mais qui est en fait un résultat commun à tous les problèmes de plongement à noyau $\{\pm 1\}$). Comme $\widetilde{N}$ est la clôture galoisienne sur $\mathbb{Q}$ d'une extension quadratique $\widetilde{K}$ de K, on en déduit :

Proposition II.5. *Si $K(\sqrt{\gamma})$ est une réalisation du plongement, alors les autres sont les $K(\sqrt{m\gamma})$ où $m \in \mathbb{Z} \setminus \{0\}$.*

III. Plongement et ramification. On reprend les notations des paragraphes précédents avec comme corps de base $k_0 = \mathbb{Q}$. On suppose que N est plongeable dans une extension $\widetilde{N}/\mathbb{Q}$ de type $\widetilde{S}_4$. On cherche à réaliser le plongement en minimisant le nombre de places ramifiées.

Dans la suite, nous utiliserons le résultat suivant, dû à J.-P. Serre, et dont on peut trouver la démonstration dans [B-K], p. 5 :

Lemme III.1. *Soit $1 \to A \to \widetilde{\Gamma} \to \Gamma \to 1$ une extension centrale de groupes finis et soit $G_{\mathbb{Q}}$ le groupe de Galois absolu de $\mathbb{Q}$. Soit $\pi : G_{\mathbb{Q}} \to \Gamma$ un homomorphisme continu et soit S l'ensemble des nombres premiers p où π est ramifié. Supposons que π soit relevable en $\widetilde{\pi} : G_{\mathbb{Q}} \to \widetilde{\Gamma}$. Alors on peut choisir un tel relèvement qui soit non ramifié en dehors de S.*

THÉORÈME III.2. *On suppose K plongeable. Alors* :

(1) *Pour toute réalisation du plongement $\widetilde{N}/\mathbb{Q}$, l'extension $\widetilde{N}/N$ est ramifiée en tout idéal premier ramifié dans L/C et en tout idéal premier situé au-dessus de 2 si $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_1'^2$, auquel cas $d_k \equiv 4 \bmod 8$.*

(2) *Il existe une réalisation du plongement telle que $\widetilde{N}/N$ soit non ramifiée en dehors des idéaux premiers de N qui sont ramifiés dans L/C et des idéaux premiers de N au-dessus de 2 si $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_1'^2$. On appellera un tel corps $\widetilde{N}$ un "$\widetilde{S}_4$ pur".*

La démonstration de ce théorème s'appuie sur les lemmes III.3 et III.4 suivants :

LEMME III.3. *Supposons l'extension $K/\mathbb{Q}$ plongeable. Si p est un nombre premier de $\mathbb{Q}$ tel que $p\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_1'^2$, alors $p = 2$ et $d_k \equiv 4 \bmod 8$.*

P r e u v e. On a vu au paragraphe II que $d_{\widetilde{K}} \in d_k\mathbb{Q}^{*2}$. Or la formule de transitivité du discriminant donne l'égalité

$$\mathfrak{d}_{\widetilde{K}/\mathbb{Q}} = \mathfrak{d}_{K/\mathbb{Q}}^2 \cdot N_{K/\mathbb{Q}}(\mathfrak{d}_{\widetilde{K}/K}).$$

Supposons que $p\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_1'^2$. Alors $p = 2$ d'après la proposition II.4. Si $\mathfrak{p}_1'$ ne se ramifie pas dans $\widetilde{K}$, alors $\mathfrak{p}_2$ est le seul idéal au-dessus de 2 à pouvoir éventuellement se ramifier dans $\widetilde{K}$. Ainsi, $\mathfrak{d}_{\widetilde{K}/\mathbb{Q}}$ est un carré dans le localisé en 2 de $\mathbb{Z}$ et $d_k \equiv 4 \bmod 8$. Si par contre $\mathfrak{p}_1'$ se ramifie dans $\widetilde{K}$, alors $2\mathcal{O}_{\widetilde{K}'}$ est de la forme $\prod \mathfrak{P}^{(i)4}$ et $\mathfrak{p}_2$ est totalement ramifié dans $\widetilde{K}'$. Posons $\widetilde{K} = K(\sqrt{\gamma})$. Si $v_{\mathfrak{p}_2}(\gamma) \equiv 1 \bmod 2$, d'après la proposition II.5, on a une autre réalisation du plongement en prenant $\widetilde{K} = K(\sqrt{2\gamma})$. On peut donc se ramener au cas où l'on peut écrire γ sous la forme $\gamma = \pi^{2l}\varepsilon$, où l est un entier naturel, π une uniformisante de $K_{\mathfrak{p}_2}$, complété en $\mathfrak{p}_2$ de K, et ε une unité de $K_{\mathfrak{p}_2}$. Si $\mathfrak{p}_2$ est toujours totalement ramifié dans cette nouvelle réalisation du plongement, $K_{\mathfrak{p}_2}(\sqrt{\varepsilon})$ est une extension quartique de $\mathbb{Q}_2$ de type diédral et donc $N_{K_{\mathfrak{p}_2}/\mathbb{Q}_2}(\sqrt{\varepsilon}) \equiv d_{k_{\tilde{\mathfrak{p}}}} \bmod \mathbb{Q}_2^{*2}$, où $\tilde{\mathfrak{p}}$ désigne l'unique idéal premier de $\mathcal{O}_k$ situé au-dessus de 2. ∎

LEMME III.4. *Soient $\mathfrak{p}$ et $\mathfrak{p}'$ deux idéaux premiers de $\mathcal{O}_{K'}$ au-dessus d'un même nombre premier p de $\mathbb{Z}$. Alors $\mathfrak{p}$ se ramifie dans $\widetilde{K}'$ si et seulement si $\mathfrak{p}'$ se ramifie dans $\widetilde{K}'$.*

P r e u v e. Comme $\widetilde{N}/K'$ est cyclique d'ordre 6, l'idéal $\mathfrak{p}$ est ramifié dans $\widetilde{K}'$ si et seulement si $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ dans $\mathcal{O}_N$ est ramifié dans $\widetilde{N}$. Soit maintenant $\mathfrak{P}'$ un idéal premier de $\mathcal{O}_N$ au-dessus de $\mathfrak{p}'$. Si $\mathfrak{P}$ est ramifié dans $\widetilde{N}$, alors $\mathfrak{P}'$ l'est aussi car $\mathfrak{P}' = \mathfrak{P}^\sigma$ où $\sigma \in S_4$ et donc $\mathfrak{p}'$ est ramifié dans $\widetilde{K}'$. ∎

P r e u v e d u t h é o r è m e III.2. (1) Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_N$ ramifié dans l'extension L/C. Le groupe d'inertie $g_0(\mathfrak{P})$ de $\mathfrak{P}$ dans l'extension N/L contient au moins un élément d'ordre 2 de g_0 qui n'est pas une transposition. Ainsi, il existe $\sigma \in S_4$ tel que $\mathfrak{P}$ soit ramifié dans N/L'^{σ}. Comme $\widetilde{N}/L'^{\sigma}$ est cyclique d'ordre 4, l'idéal $\mathfrak{P}$ est ramifié dans $\widetilde{N}$.

Si $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_1'^2$, alors le groupe de décomposition de 2 dans l'extension $N/\mathbb{Q}$, défini à conjugaison près, est bicyclique d'ordre 4 et isomorphe à $\mathrm{Gal}(N/L)$. On en déduit que le groupe de décomposition D de 2 dans l'extension $\widetilde{N}/\mathbb{Q}$, défini à conjugaison près, est diédral d'ordre 8. Or, le groupe d'inertie I inclus dans D de 2 dans l'extension $\widetilde{N}/\mathbb{Q}$ est distingué dans D et contient un élément d'ordre 2, relevé dans $\widetilde{S}_4$ d'une transposition de S_4. On en déduit que I est bicyclique d'ordre 4, et donc que $\mathfrak{p}_2$ est totalement ramifié dans $\widetilde{K}'$.

(2) Tout d'abord, les lemmes III.1 et III.4 assurent qu'on peut choisir $\widetilde{K}'$ tel que $\widetilde{K}'/K'$ soit non ramifiée en dehors des idéaux premiers de K' qui sont ramifiés dans $N/\mathbb{Q}$, et donc dans $K/\mathbb{Q}$ puisque N est la clôture galoisienne de K. Soit $K'(\sqrt{\gamma})/K$ une telle réalisation du plongement. Montrons qu'en changeant éventuellement γ par $m\gamma$ où $m \in \mathbb{Z}^*$, on peut éliminer dans $\widetilde{K}'/K'$ toute ramification ne provenant pas d'une ramification dans L/C.

Soit p un nombre premier ramifié dans K et non ramifié dans L/C.

C a s o ù $p \neq 2$. Si p est totalement ramifié dans C, alors $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'^3$. Si $v_{\mathfrak{p}}(\gamma) \equiv 1 \bmod 2$, alors $v_{\mathfrak{p}}(p\gamma) \equiv 0 \bmod 2$ et $\mathfrak{p}$ n'est pas ramifié dans $K(\sqrt{p\gamma})/K$, ni donc dans l'extension $K'(\sqrt{p\gamma})/K'$. Si p est ramifié dans k et non totalement ramifié dans C, $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''^2$ (proposition II.4). Alors, $\mathfrak{p}$ se ramifie dans K' et donc il ne se ramifie pas dans $\widetilde{K}'/K'$.

C a s o ù $p = 2$. Si 2 est totalement ramifié dans C, alors $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'^3$. On se ramène de la même façon que pour $p \neq 2$ au cas où $v_p(\gamma) \equiv 0 \bmod 2$. Si $\mathfrak{p}$ se ramifie dans $K(\sqrt{\gamma})/K$, montrons qu'on peut éliminer cette ramification en remplaçant γ par $-\gamma$. Posons $\gamma = 2^{2l}\varepsilon$ où l désigne un entier naturel et ε une unité de $\mathbb{Z}_2$. Alors d'après la théorie de Kummer (voir [He]), $K(\sqrt{\gamma})/K$ est ramifiée en $\mathfrak{p}$ si et seulement si la congruence $\varepsilon \equiv x^2 \bmod \mathfrak{p}^2$ n'a pas de solution dans $\mathcal{O}_{K_{\mathfrak{p}}}$, l'anneau de valuation du complété de K en $\mathfrak{p}$. Or, dans $(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}^2)^* \simeq (\mathbb{Z}/4\mathbb{Z})^*$, 1 est le seul carré. Par conséquent, si $\mathfrak{p}$ se ramifie dans $K(\sqrt{\gamma})$, alors $\varepsilon \equiv -1 \bmod \mathfrak{p}^2$ et $K(\sqrt{-\gamma})/K$ est non ramifiée en $\mathfrak{p}$, ainsi que $K'(\sqrt{-\gamma})/K'$.

Si $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''^2$, et en particulier si 2 est ramifié dans k et si la ramification en 2 de $k/\mathbb{Q}$ est maximale (lemme III.3), la démonstration exposée ci-dessus s'applique. ∎

En utilisant la théorie de Kummer, on peut alors expliciter le discriminant d'un corps $\widetilde{K}$ réalisant un "$\widetilde{S}_4$ pur" :

PROPOSITION III.5. *On suppose K plongeable. Soit $\widetilde{K}$ une extension quadratique de K réalisant un "$\widetilde{S}_4$ pur". Alors*

$$\mathfrak{d}_{\widetilde{K}/\mathbb{Q}} = \mathfrak{d}_{K/\mathbb{Q}}^2 \cdot 2^n \cdot \prod_{p\in P} p \cdot \prod_{p\in P'} p^2$$

où P désigne l'ensemble des nombres premiers impairs ramifiés dans k et P' l'ensemble des nombres premiers impairs non ramifiés dans k mais admettant une ramification dans l'extension L/C. De plus :

Si d_k est impair : $n = 2$, 4, 6, 8 ou 10 si 2 admet une ramification dans L/C et $n = 0$ sinon.

Si $d_k \equiv 0 \bmod 8$: $n = 9$ si 2 admet une ramification dans L/C et $n = 3$ sinon.

Si $d_k \equiv 4 \bmod 8$: $n = 2$, 4, 6, 8 ou 10 si 2 admet une ramification dans L/C et $n = 6$, 8 ou 10 sinon.

IV. Classes au sens restreint de K'. Nous reprenons les notations des paragraphes précédents, avec comme corps de base $k_0 = \mathbb{Q}$, et étudions $h_{K'}^+$ dans les cas où K est totalement réel ou de signature mixte.

LEMME IV.1. *Si K est totalement réel et si l'extension L/C est ramifiée, ou si K est de signature mixte et si L/C est ramifiée au-dessus d'au moins deux nombres premiers de $\mathbb{Z}$, alors h_K^+ est pair.*

P r e u v e. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_C$ qui se ramifie dans L. Soit $(p) = \mathfrak{p} \cap \mathbb{Z}$. Le tableau I.3 montre qu'il existe un idéal $\mathfrak{I}$ de $\mathcal{O}_K$ tel que $p\mathcal{O}_K = \mathfrak{I}^2$. Alors, soit $\mathfrak{I}$ est d'ordre 2 dans le groupe des classes de K et h_K est pair, soit il est principal. Dans ce dernier cas, si θ_p est un générateur de $\mathfrak{I}$, $\varepsilon_p = \theta_p^2/p$ est une unité totalement positive non carrée de K. De plus, on remarque que les unités ε_p ainsi obtenues sont linéairement indépendantes dans le $\mathbb{F}_2$-espace vectoriel E^+/E^2, où E et E^+ sont respectivement l'ensemble des unités et des unités totalement positives de K. Soit (r_1, r_2) la signature de K; on arrive au résultat grâce à l'égalité $h_K^+/h_K = 2^{-r_2}[E_K^+ : E_K^2]$. ∎

Soit $h_{K'}^{+a}$ le nombre de classes au sens restreint de K' invariantes par $\mathrm{Gal}(K'/K)$. Alors

$$h_{K'}^{+a} = \frac{2^{t-1} h_K^+}{[E_K^+ : E_K^+ \cap N_{K'/K}(K'^*)]} \tag{a}$$

où t désigne le nombre d'idéaux premiers de K ramifiés dans K' (voir [Gr], p. 26). Soit j l'entier naturel tel que $h_K^+/h_K = 2^{-r_2}[E_K^+ : E_K^2] = 2^j$. Si K est totalement réel, $j \le 3$ et $[E_K^+ : E_K^2] = 2^j$. Si par contre K est de signature mixte, $j \le 2$ et l'indice $[E_K^+ : E_K^2]$ est égal à 2^{j+1}. Comme E_K^2 est un sous-groupe de $E_K^+ \cap N_{K'/K}(K'^*)$, on en déduit l'égalité :

$$h_{K'}^{+a} = 2^{t-l-1} h_K^+ \tag{b}$$

où l désigne un entier compris entre 0 et j (resp. entre 0 et $j+1$) si K est totalement réel (resp. de signature mixte). De plus, si l'extension K'/K est non ramifiée en un idéal $\mathfrak{p}$ de K, toute unité ε de K vérifie $(\varepsilon, d_k)_{\mathfrak{p}} = 1$. Par la formule du produit relative au symbole de Hilbert, on en déduit que si l'extension K'/K est ramifiée en au plus un idéal premier de K, toute unité totalement positive de K appartient à $N_{K'/K}(K'^*)$ et donc que dans ce cas, on a l'égalité

$$h_{K'}^{+a} = 2^{t-1} h_K^+. \tag{c}$$

Pour étudier la parité de $h_{K'}^+$, il sera donc utile de compter les idéaux premiers de K qui se ramifient dans K'. Ces idéaux proviennent des nombres premiers ramifiés dans l'extension $k/\mathbb{Q}$. Soit p un nombre premier ramifié dans $k/\mathbb{Q}$. Dans un premier temps, nous écarterons le cas où il existerait un idéal de $\mathcal{O}_C$ au-dessus de p qui soit ramifié dans L. (Ce cas n'est pas du tout gênant dans le cas totalement réel en vertu du lemme IV.1 mais l'est beaucoup plus dans le cas où K est de signature mixte.) Si donc p n'admet pas de ramification dans l'extension L/C, alors le tableau I.3 montre que $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_1'^3$ si p est totalement ramifié dans C et que $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''^2$ ou $\mathfrak{p}_2\mathfrak{p}_1'^2$ sinon, ce qui donne dans K' les décompositions respectives de p : $p\mathcal{O}_{K'} = \mathfrak{P}_1^3\mathfrak{P}_1'^6$, $\mathfrak{P}_1^2\mathfrak{P}_1'^2\mathfrak{P}_1''^2\mathfrak{P}_1'''^2$ ou $\mathfrak{P}_2^2\mathfrak{P}_2'^2$. Rappelons que si p est un nombre premier ramifié dans k qui n'admet pas de ramification dans L/C, alors dans le cas plongeable, p ne peut se décomposer dans $\mathcal{O}_K$ en $\mathfrak{p}_2\mathfrak{p}_1'^2$ que si $p = 2$ et si $d_k \equiv 4 \bmod 8$ (cf. lemme III.3).

Supposons K totalement réel.

• Si l'extension L/C est ramifiée en au moins une place finie, alors le lemme IV.1 donne la parité de h_K^+. Si en outre l'extension K'/K est ramifiée, $h_{K'}^+$ est pair. Sinon, soit p un nombre premier ramifié dans k. Par hypothèse, p n'est pas ramifié dans l'extension K'/K. D'après le tableau I.3, p admet alors une ramification dans l'extension L/C et $p\mathcal{O}_K = \mathfrak{p}^4$. Comme K'/K est supposée non ramifiée, h_K est pair. Or, soit $\mathfrak{p}^2$ est d'ordre 2 dans le groupe des classes Cl_K de K et alors $\mathfrak{p}$ est d'ordre 4 dans Cl_K, soit il est principal et on peut exhiber, de la même façon que dans la preuve du lemme IV.1, une unité de K totalement positive qui n'est pas dans K^{*2}. Dans les deux cas, 4 divise h_K^+. Le fait que K'/K soit non ramifiée montre aussi que l'égalité (c) s'applique et donc que $h_{K'}^{+a} = h_K^+/2$. On en déduit que $h_{K'}^+$ est pair.

• Si l'extension L/C est non ramifiée : si l'extension $k/\mathbb{Q}$ est ramifiée en plusieurs nombres premiers, alors l'égalité (b) montre que $h_{K'}^+$ est pair. Si maintenant l'extension $k/\mathbb{Q}$ est ramifiée en un et un seul nombre premier alors d'après la proposition II.2, l'extension $K/\mathbb{Q}$ est plongeable et le lemme III.3, via l'égalité (b), montrent que dans ce cas aussi, $h_{K'}^+$ est pair. En effet, si K est totalement réel, k est lui aussi réel. Si de plus 2 est le seul

nombre premier ramifié dans k, alors $d_k = 8$ et d'après le lemme III.3, $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''^2$. On obtient donc :

THÉORÈME IV.2. *Si K est totalement réel, alors $h^+_{K'}$ est pair.*

Si K est de signature mixte, $h^+_{K'}$ peut être impair, comme le montre l'exemple du corps K de discriminant $-1984 = -2^6 \cdot 31$ déterminé par le polynôme $P(X) = X^4 + 2X^3 + 2X^2 - 2X - 1$ où l'on a $h^+_K = 1$ et $h^+_{K'} = h_{K'} = 3$. On remarque aussi que dans ce cas, K n'est pas plongeable.

Considérons un corps K de signature mixte, plongeable et tel que l'extension L/C soit non ramifiée, c'est-à-dire tel que $d_K = d_C$.

• Si l'extension $k/\mathbb{Q}$ est ramifiée en au moins deux nombres premiers, l'extension K'/K est ramifiée en au moins trois idéaux premiers de K. Alors, dans l'égalité (b), $t \geq 3$ et $j - l \geq -1$. On en déduit que dans ce cas, $h^+_{K'}$ (ou $h_{K'}$, c'est la même chose) est pair.

• Si l'extension $k/\mathbb{Q}$ est ramifiée en un et un seul nombre premier impair, l'égalité (a) ne dévoile pas la parité de $h_{K'}$. Utilisons les résultats du paragraphe III. Le théorème III.2 établit l'existence d'une réalisation $\widetilde{N}$ du plongement telle que l'extension $\widetilde{N}$ soit non ramifiée. Alors, l'extension $\widetilde{K}'/K'$ correspondante est non ramifiée (lemme III.4). Par la théorie globale du corps de classes (voir par exemple [A-T]), on en déduit que $h_{K'}$ est pair. Nous avons donc démontré le théorème :

THÉORÈME IV.3. *On suppose K plongeable (ce qui impose que K est totalement réel ou de signature mixte). Alors, si K est totalement réel ou si $d_K = d_C$, le nombre de classes $h^+_{K'}$ est pair, sauf peut-être dans le cas particulier où $d_K \equiv -1 \bmod \mathbb{Q}^{*2}$, c'est-à-dire où $k = \mathbb{Q}(\sqrt{-1})$, les corps k et C désignant toujours respectivement les extensions quadratique et cubique de $\mathbb{Q}$ associées à $K/\mathbb{Q}$.*

Nous allons maintenant donner des exemples dans lesquels le corps quartique K est de signature mixte, plongeable et tel que le nombre de classes au sens restreint $h^+_{K'}$ est impair. Pour construire un corps quartique de type S_4, de discriminant modulo les carrés d fixé et tel que l'extension L/C soit non ramifiée, on peut construire d'abord des corps cubiques non galoisiens de discriminant d modulo les carrés en utilisant le théorème I.1 de [M-P] et en choisir un qui soit de nombre de classes au sens restreint pair. Il faut ensuite construire $L = C(\sqrt{\alpha})$ où $\alpha \in C^*\backslash\mathbb{Q}^*$, de norme carrée (théorème I.2), est soit une unité, soit un générateur non carré d'un idéal $\mathfrak{I}^2$ où $\mathfrak{I}$ est d'ordre 2 dans le groupe de classes Cl_C de C. Si l'extension L/C est ramifiée au-dessus de 2, on doit remplacer α par $\alpha\varepsilon$, ε étant une unité de C de norme 1. On vérifie que si α_1, α_2 et α_3 sont les conjugués de α, les nombres $\beta_1 = x_1x_2 + x_2x_3 + x_3x_1$, $\beta_2 = x_1x_2 - x_2x_3 - x_3x_1$, $\beta_3 = -x_1x_2 - x_2x_3 + x_3x_1$ et $\beta_4 = -x_1x_2 + x_2x_3 - x_3x_1$, où pour tout $i \in \{1, 2, 3, 4\}$ x_i est une racine

carrée arbitrairement choisie de α_i, sont alors des éléments primitifs des conjugués de K. On en déduit que le polynôme $P(X) = \prod_{i=1}^{4}(X - \beta_i)$ définit le corps quartique K cherché. Si l'on veut que l'extension L/C soit ramifiée au-dessus d'un nombre premier p donné et non ramifiée ailleurs (si l'on excepte les places à l'infini), il n'est pas nécessaire que h_C^+ soit pair et il faut prendre un élément α de $C^*\backslash\mathbb{Q}^*$ qui soit générateur d'un idéal non carré de $\mathcal{O}_C$ de norme $p^2\mathbb{Z}$. (Si $p = 2$, on ne choisira un tel élément que si l'on cherche une ramification maximale dans L/C.)

Exemple 1. $k = \mathbb{Q}(\sqrt{-1})$ et l'extension L/C est non ramifiée. Dans ce cas, K est plongeable (proposition II.2). Soit C le corps cubique défini par le polynôme $X^3 + 33X + 22$. Son discriminant est égal à -39204. A partir de ce corps C, on construit à l'aide de la méthode exposée ci-dessus le polynôme $P(X) = X^4 - 15X^3 + 297X^2 - 556X + 270$ définissant un corps K de discriminant $-39204 = -2^2 \cdot 3^4 \cdot 11^2$. Alors, $h_K = h_K^+ = 1$ et $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_1'^2$. L'égalité (a) permet de conclure que $h_{K'}^+$ est impair. On montre même que dans ce cas, h_N (ou h_N^+, c'est pareil) est impair. En effet, un calcul sur le système PARI montre que le groupe de classes de $\widetilde{L}$ est cyclique d'ordre 12. Or, l'extension $N/\widetilde{L}$ est non ramifiée : elle est non ramifiée en 3 et 11 car leurs groupes d'inertie dans l'extension $N/\mathbb{Q}$ (définis à conjugaison près) sont cycliques d'ordre 3 et non ramifiée en 2 car son groupe d'inertie est d'ordre 2 et $2\mathcal{O}_{\widetilde{L}}$ de la forme $\mathfrak{p}_1^2\mathfrak{p}_2'^2$ (cf. tableau I.3). Comme l'extension $N/\widetilde{L}$ est cyclique d'ordre 4, un calcul de classes invariantes (cf. [Ja]) permet alors de montrer que $h_N = h_N^+$ est impair.

Exemple 2. $k = \mathbb{Q}(\sqrt{-1})$ et l'extension L/C est ramifiée en tout idéal de C au-dessus de 2 et non ramifiée en tout autre idéal. Soit C le corps cubique défini par le polynôme $X^3 + 6X + 4$. Son discriminant est égal à $-324 = -2^2 \cdot 3^4$. A partir de ce corps C, on construit le polynôme $P(X) = X^4 - 2X^3 + 3X^2 - 6X + 3$ définissant un corps K de discriminant $-5184 = -2^6 \cdot 3^4$. Alors, 3 est totalement ramifié dans C et K est plongeable (proposition II.4). D'autre part, $h_K = h_K^+ = 1$ et $2\mathcal{O}_K = \mathfrak{p}_2^2$. On conclut que $h_{K'}^+$ est impair.

V. Applications numériques. Nous allons appliquer les résultats du paragraphe III aux corps quartiques totalement réels et à ceux de signature mixte pour construire les corps de degré 8 de type $\widetilde{S}_4$ de plus petit discriminant pour les signatures $(8, 0)$, $(0, 4)$ et $(2, 3)$. Pour cela nous disposons des tables de J. Buchmann, D. Ford et M. Pohst (cf. [Bu-Fo] et [Bu-Fo-Po]) qui donnent pour chaque corps quartique K son discriminant d_K, un polynôme le définissant, une base du groupe des unités, le régulateur de K, le groupe de Galois de sa clôture galoisienne et son nombre de classes h_K.

Nous aurons également besoin de savoir décider si un élément γ donné de $K^*\backslash K^{*2}$ définit ou non un corps $K(\sqrt{\gamma})$ de degré 8 de type $\widetilde{S}_4$. Si γ_1, γ_2,

γ_3 et γ_4 sont les conjugués de γ, la clôture galoisienne M de $K(\sqrt{\gamma})/\mathbb{Q}$ est le corps $N(\sqrt{\gamma_1}, \sqrt{\gamma_2}, \sqrt{\gamma_3})$, qui est de degré 48, 96 ou 192 sur $\mathbb{Q}$. Les tables de [B-McK] montrent l'existence d'exactement quatre groupes de permutations impairs sur huit éléments correspondant à un corps de degré 8 contenant un sous-corps de degré 4 et ne contenant pas de sous-corps quadratique : les groupes notés T23, T38, T40 et T44. Le groupe T23 est isomorphe à $\widetilde{S}_4$, T38 et T40 sont d'ordre 192 et T44 est d'ordre 384. On en déduit que $K(\sqrt{\gamma})$ est de type $\widetilde{S}_4$ si et seulement si $M = N(\sqrt{\gamma})$. Le résultat suivant transpose à $\widetilde{S}_4$ un résultat obtenu dans [H-K] par F.-P. Heider et P. Kolvenbach pour le cas $\widetilde{A}_4$.

PROPOSITION V.1. *Le corps $K(\sqrt{\gamma})$ est une réalisation du plongement si et seulement si le polynôme R de degré 24 suivant est réductible sur $\mathbb{Q}$:*

$$R(X) = \prod_{i \neq j} ((X - \delta_i \delta_j (\gamma_i - \gamma_j))^2 - d_k)$$

où pour tout $i \in \{1, 2, 3, 4\}$, δ_i désigne une racine carrée arbitrairement choisie de γ_i. Dans ce cas, le polynôme R sera égal au produit $F_{+1}F_{-1}$ où pour $\varepsilon \in \{\pm 1\}$, F_ε désigne l'un des huit polynômes de degré 12 définis par

$$F_\varepsilon(X) = \prod_{i<j} (X^2 - (\delta_i \delta_j (\gamma_i - \gamma_j) + \varepsilon \varepsilon_{ij} \sqrt{d_k}\,)^2)$$

avec $\varepsilon_{ij} \in \{\pm 1\}$ et

$$(\varepsilon_{12}, \varepsilon_{13}, \varepsilon_{14}, \varepsilon_{23}, \varepsilon_{24}, \varepsilon_{34}) = \begin{cases} (+1,+1,+1,+1,-1,+1), \\ (-1,+1,+1,+1,-1,-1), \\ (+1,+1,-1,+1,+1,-1), \\ (-1,+1,-1,+1,+1,+1), \\ (+1,+1,+1,-1,+1,-1), \\ (-1,+1,+1,-1,+1,+1), \\ (+1,+1,-1,-1,-1,+1), \quad \textit{ou} \\ (-1,+1,-1,-1,-1,-1). \end{cases}$$

Preuve. Notons $\tau_1 = (12)(34)$ et $\tau_2 = (12)$ dans le groupe de permutations S_4 agissant sur l'ensemble $\{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$ par permutations des indices. $N(\sqrt{\gamma})$ est galoisien sur $\mathbb{Q}$ si et seulement si $\gamma_1\gamma_2 \in N^{*2}$. De plus, $\gamma_1\gamma_2 \in L'^*$, groupe multiplicatif du corps L' fixé par $\langle\tau_1\rangle$. Supposons maintenant que l'extension $N(\sqrt{\gamma})/\mathbb{Q}$ soit galoisienne. Alors, son groupe de Galois est isomorphe à $\widetilde{S}_4$. Le relevé $\widetilde{\tau}_1$ de τ_1 dans $\widetilde{S}_4$ est d'ordre 4. Ainsi, $\delta_1^{\tilde{\tau}_1} = \varepsilon\delta_2$ et $\delta_2^{\tilde{\tau}_1} = -\varepsilon\delta_1$ où $\varepsilon \in \{\pm 1\}$. Comme $\delta_1\delta_2 \in N$, on en déduit que $(\delta_1\delta_2)^{\tau_1} = (\delta_1\delta_2)^{\tilde{\tau}_1} = -\delta_1\delta_2$. Soit $\omega = \gamma_1\gamma_2(\gamma_1 - \gamma_2)^2$, $\omega \in N^{*2} \cap L^*$, L étant le corps fixé par le sous-groupe $\langle\tau_1, \tau_2\rangle$. De plus, comme $\delta_1\delta_2(\gamma_1 - \gamma_2)$ est invariant par τ_1, $\omega \in L'^{*2}$. Par contre, $\omega \notin L^2$. En effet, $(\gamma_1 - \gamma_2)^{\tau_2} = \gamma_2 - \gamma_1$. Or, si $\widetilde{\tau}_2$ est le relèvement de τ_2 dans $\widetilde{S}_4$, alors comme $\widetilde{\tau}_2$ est d'ordre 2,

$\delta_1^{\tilde{\tau}_2} = \varepsilon\delta_2$ et $\delta_2^{\tilde{\tau}_2} = \varepsilon\delta_1$ où $\varepsilon \in \{\pm 1\}$. Ainsi, $(\delta_1\delta_2)^{\tilde{\tau}_2} = \delta_1\delta_2$ et $(\delta_1\delta_2)^{\tau_2} = \delta_1\delta_2$. On obtient : $\mathrm{Gal}(N(\sqrt{\gamma})/\mathbb{Q}) \simeq \widetilde{S}_4$ si et seulement si $L(\sqrt{\omega}) = L' = L(\sqrt{d_k})$. La seconde partie de la proposition, qui permet une factorisation très rapide du polynôme R, se montre alors en déterminant les conjugués d'une racine de R pour chacune des huit possibilités dont dispose $\widetilde{S}_4$ pour agir sur l'ensemble $\{\pm\delta_1, \pm\delta_2, \pm\delta_3, \pm\delta_4\}$. ∎

Grâce à ce critère et aux résultats du paragraphe III, on peut, pour un corps quartique K de type S_4 plongeable donné, construire le plongement de K de discriminant minimum. Le tableau V.3 (resp. V.4) donne ce plongement pour chacun des sept premiers corps K totalement réels (resp. de signature mixte) dans l'ordre croissant de leurs discriminants (resp. de la valeur absolue de leurs discriminants). On montre en particulier le résultat suivant :

Théorème V.2. (1) *Le plus petit discriminant des corps de degré* 8 *de type* $\widetilde{S}_4$ *totalement réels est* 2777^3. *Il est atteint par le corps défini par le polynôme* $Q(X) = X^8 - 150X^6 + 5391X^4 - 8615X^2 + 2777$ *et uniquement par ce corps à conjugaison près.*

(2) *Le plus petit discriminant des corps de degré* 8 *de type* $\widetilde{S}_4$ *totalement imaginaires est* $2^4 \cdot 29^3 \cdot 73^3$. *Il est atteint par le corps défini par le polynôme* $Q(X) = X^8 + 160X^6 + 3634X^4 + 18536X^2 + 2117$ *et uniquement par ce corps à conjugaison près.*

(3) *Le plus petit discriminant en valeur absolue des corps de degré* 8 *de type* $\widetilde{S}_4$ *de signature* $(2,3)$ *est* -283^3. *Il est atteint par le corps défini par le polynôme* $Q(X) = X^8 + 24X^6 + 178X^4 + 336X^2 - 283$ *et uniquement par ce corps à conjugaison près.*

Les polynômes donnés dans le théorème V.2 présentent l'intérêt de mettre en évidence la ramification dans l'extension $\widetilde{K}/K$, mais sont "fortement parasités" : le polynôme Q de (3) est de discriminant $-2^{56} \cdot 283^3$ alors que $(\theta+1)/2$ est racine d'un polynôme de discriminant -283^3, θ étant une racine du polynôme Q. (Avant d'essayer ce changement de variable, on remarque que $\theta + 1 \in 2\mathcal{O}_K$ et que le polynôme caractéristique de $(\theta+1)/2$ sera égal à

$$P_{(\theta+1)/2}(X) = \frac{1}{2^8} Q(2X-1).)$$

De même, le polynôme Q de (1) est de discriminant $2^8 \cdot 733^4 \cdot 2777^3$ alors que la fonction "polred" du système PARI donne en réduisant Q un polynôme de discriminant 2777^3. Dans les tableaux qui suivent, nous n'effectuons pas ce genre de simplification. Ainsi, dans le tableau V.4 (resp. V.3), la partie droite de la première ligne pourrait contenir le polynôme $X^8 - 4X^7 + 13X^6 - 25X^5 + 38X^4 - 39X^3 + 28X^2 - 12X + 1$ (resp. $X^8 - 4X^7 - 4X^6 + 26X^5 + 2X^4 - 52X^3 + 31X + 1$), de discriminant -283^3 (resp. 2777^3).

Tableau V.3

Dans ce tableau, les abréviations Re et Im notées entre parenthèses indiquent si le corps de degré 8 réalisant le plongement de plus petit discriminant est totalement réel ou totalement imaginaire

$d_K = 2777$, $d_C = d_K$ $X^4 - X^3 - 4X^2 + X + 2$	$d_{\widetilde{K}} = 2777^3$ (Re) $X^8 - 150X^6 + 5391X^4 - 8615X^2 + 2777$
$d_K = 6224 = 2^4 \cdot 389$, $d_C = 389$ $X^4 - 2X^3 - 4X^2 + 2X + 2$	$d_{\widetilde{K}} = 2^{10} \cdot 389^3$ (Re) $X^8 - 232X^6 + 11794X^4 - 4400X^2 + 389$
$d_K = 7537$, $d_C = d_K$ $X^4 + X^3 - 5X^2 - 4X + 3$	$d_{\widetilde{K}} = 7537^3$ (Im) $X^8 + 126X^6 + 3851X^4 + 30929X^2 + 7537$
$d_K = 8069$, $d_C = d_K$ $X^4 + X^3 - 5X^2 - 5X + 1$	$d_{\widetilde{K}} = 8069^3$ (Re) $X^8 - 215X^6 + 7893X^4 - 39891X^2 + 8069$
$d_K = 8468 = 2^2 \cdot 29 \cdot 73$, $d_C = d_K$ $X^4 + X^3 - 5X^2 - 3X + 4$	$d_{\widetilde{K}} = 2^4 \cdot 29^3 \cdot 73^3$ (Im) $X^8 + 160X^6 + 3634X^4 + 18536X^2 + 2117$
$d_K = 9301 = 71 \cdot 131$, $d_C = d_K$ $X^4 + X^3 - 5X^2 - X + 3$	$d_{\widetilde{K}} = 71^3 \cdot 131^3$ (Im) $X^8 + 396X^6 + 24506X^4 + 77671X^2 + 9301$
$d_K = 9909 = 3^3 \cdot 367$, $d_C = 3 \cdot 367$ $X^4 - 6X^2 + 3X + 3$	$d_{\widetilde{K}} = 3^7 \cdot 367^3$ (Re) $X^8 - 150X^6 + 2775X^4 - 8058X^2 + 1101$

Tableau V.4

Dans tous les exemples cités dans ce tableau, le nombre de classes au sens restreint $h^+_{K'}$ de K' est pair, sauf dans le cas où $d_K = -688$, où $h^+_{K'}$ est impair

$d_K = -283$, $d_C = d_K$ $X^4 + X - 1$	$d_{\widetilde{K}} = -283^3$ $X^8 + 24X^6 + 178X^4 + 336X^2 - 283$
$d_K = -331$, $d_C = d_K$ $X^4 + X^3 - X^2 - X - 1$	$d_{\widetilde{K}} = -331^3$ $X^8 - 7X^6 - 123X^4 - 375X^2 - 331$
$d_K = -491$, $d_C = d_K$ $X^4 - X^3 - X^2 + 3X - 1$	$d_{\widetilde{K}} = -491^3$ $X^8 + 8X^6 + 110X^4 + 1251X^2 - 491$
$d_K = -563$, $d_C = d_K$ $X^4 - X^3 + X^2 - X - 1$	$d_{\widetilde{K}} = -563^3$ $X^8 + 16X^6 + 42X^4 - 264X^2 - 563$
$d_K = -643$, $d_C = d_K$ $X^4 - X^3 - 2X + 1$	$d_{\widetilde{K}} = -643^3$ $X^8 + 3X^6 - 66X^4 - 580X^2 - 643$
$d_K = -688 = -2^4 \cdot 43$, $d_C = -43$ $X^4 - 2X - 1$	$d_{\widetilde{K}} = -2^{10} \cdot 43^3$ $X^8 + 12X^6 - 22X^4 + 96X^2 - 43$
$d_K = -751$, $d_C = d_K$ $X^4 - 2X^3 + X^2 + X - 2$	$d_{\widetilde{K}} = -751^3$ $X^8 + X^6 - 201X^4 + 702X^2 - 751$

Bibliographie

[A-T] E. Artin and J.Tate, *Class Field Theory*, Benjamin, Amsterdam, 1967.

[B-K] C. Bachoc et S.-H. Kwon, *Sur les extensions de groupe de Galois* $\widetilde{A}_4$, Acta Arith. 62 (1992), 1–10.

[Ba-Fr] P. Bayer and G. Frey, *Galois representations of octahedral type and* 2*-coverings of elliptic curves*, Math. Z. 207 (1992), 395–408.

[Bu-Fo] J. Buchmann and D. Ford, *On the computation of totally real quartic fields of small discriminant*, Math. Comp. 52 (1989), 161–174.

[Bu-Fo-Po] J. Buchmann, D. Ford and M. Pohst, *Enumeration of quartic fields with small discriminant*, ibid. 61 (1993), 873–879.

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

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

[Gr] G. Gras, *Sur les* ℓ*-classes d'idéaux dans les extensions cycliques relatives de degré premier* ℓ, Ann. Inst. Fourier (Grenoble) 23 (3) (1973), 1–48.

[He] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, New York, 1981.

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

[Ja] J.-F. Jaulent, *L'arithmétique des* ℓ*-extensions*, Thèse, Publ. Math. Fac. Sci. Besançon, 1986.

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

[M-P] J. Martinet et J.-J. Payan, *Sur les extensions cubiques non galoisiennes des rationnels et leur clôture galoisienne*, J. Reine Angew. Math. 228 (1967), 15–37.

[Sc] I. Schur, *Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen*, ibid. 139 (1911), 155–250.

[Se1] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (1984), 651–676.

[Se2] —, *Corps locaux*, 3e éd., Hermann, Paris, 1980.

[Se3] —, *Représentations linéaires des groupes finis*, 3e éd., Hermann, Paris, 1978.

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

Reçu le 4.1.1994
et révisé le 20.6.1994 (2550)