

## Corps quadratiques à corps de classes de Hilbert principaux et à multiplication complexe

par

STÉPHANE LOUBOUTIN (Caen)

**Introduction.** On sait (voir [Hof] ou [Odl 1]) qu'il n'existe qu'un nombre fini de corps galoisiens à multiplication complexe (i.e., des corps de nombres totalement imaginaires, extensions quadratiques de corps totalement réels) de nombres de classes d'idéaux égaux à 1. Ici : (a) nous déterminons tous ceux qui sont des corps de classes de Hilbert de corps quadratiques imaginaires (il y en a 30 et ils sont abéliens); (b) nous déterminons tous ceux qui sont abéliens et sont des corps de classes de Hilbert de corps quadratiques réels (il y en a 39), (c) nous construisons 26 d'entre eux non abéliens et qui sont des corps de classes de Hilbert de corps quadratiques réels; et (d) nous montrons qu'il est raisonnable de conjecturer que tout corps galoisien, non abélien, à multiplication complexe, de nombre de classes égal à 1 et qui est un corps de classes de Hilbert d'un corps quadratique réel est l'un de ces 26 corps. Autrement dit, il existe au moins et conjecturalement exactement 96 corps quadratiques à corps de classes de Hilbert principaux et à multiplication complexe.

Expliquons maintenant le principe de cette détermination. Si  $\mathbf{k}$  est un corps quadratique imaginaire de corps de classes de Hilbert noté  $\mathbf{H}(\mathbf{k})$ , nous montrons que  $\mathbf{H}(\mathbf{k})$  est un corps à multiplication complexe si et seulement si il est égal au corps des genres  $\mathbf{G}_{\mathbf{k}}$  de  $\mathbf{k}$ . Notre premier objectif est donc de déterminer tous les corps de genres qui sont des corps imaginaires abéliens de nombres de classes relatifs égaux à 1 : il y a 74 tels corps (voir Corollaire 2). Nous en déduisons tous les corps quadratiques imaginaires à corps de classes de Hilbert principaux et à multiplication complexe.

Supposons donc pour la suite de cette introduction que  $\mathbf{k}$  est un corps quadratique réel. Soient  $\mathbf{H}_l(\mathbf{k})$  et  $\mathbf{H}_s(\mathbf{k})$  ses corps de classes de Hilbert aux sens large et restreint. Il est clair que  $\mathbf{H}_l(\mathbf{k})$  qui est totalement réel n'est évidemment pas à multiplication complexe, et que  $\mathbf{H}_s(\mathbf{k})$  contient  $\mathbf{H}_l(\mathbf{k})$  et

---

1991 *Mathematics Subject Classification*: Primary 11R29; Secondary 11R20, 11R37.

en est une extension de degré 1 ou 2 selon que la norme de l'unité fondamentale de  $\mathbf{k}$  est égale à  $-1$  ou  $+1$ . Il en résulte que  $\mathbf{H}_s(\mathbf{k})$  est un corps à multiplication complexe si et seulement si l'unité fondamentale de  $\mathbf{k}$  est de norme  $+1$ , ce que nous supposons pour la suite de cette introduction. Nous remarquons ensuite que si  $\mathbf{H}_s(\mathbf{k})$  est principal, alors tout sous-corps  $\mathbf{M}$  de  $\mathbf{H}_s(\mathbf{k})$  contenant  $\mathbf{k}$  et qui est un corps à multiplication complexe est de nombre de classes relatif égal à 1 (voir Proposition 6). En particulier, nous pouvons aisément déterminer tous les  $\mathbf{k}$  à corps des genres  $\mathbf{G}_\mathbf{k}$  imaginaires tels que  $\mathbf{H}_s(\mathbf{k})$  soit un corps à multiplication complexe principal.

Nous pouvons donc maintenant supposer que  $\mathbf{G}_\mathbf{k}$  est réel. L'étape cruciale consiste alors à montrer au Théorème 8 que si  $\mathbf{H}_s(\mathbf{k})$  est principal, alors le 2-corps de classes de Hilbert au sens restreint  $\mathbf{H}_{s,2}(\mathbf{k})$  de  $\mathbf{k}$  est un corps à multiplication complexe, diédral, de degré  $\geq 8$  une puissance de 2 et de nombre de classes relatif égal à 1. Nous caractérisons alors au Théorème 10 les corps quadratiques réels  $\mathbf{k}$  d'unité fondamentale de norme  $+1$  tels que  $\mathbf{H}_{s,2}(\mathbf{k})$  soit diédral de degré  $\geq 8$  une puissance de 2 et de nombre de classes relatif impair. Puisque la liste des tels corps à nombre de classes relatif égal à 1 est conjecturalement connue, nous pouvons conjecturalement terminer notre détermination.

**Notations.** Pour  $\mathbf{K}$  un corps de nombres, nous notons  $\mathbf{W}_\mathbf{K}$  le groupe des racines de l'unité de  $\mathbf{K}$ ,  $w_\mathbf{K}$  l'ordre de ce groupe,  $\mathbf{U}_\mathbf{K}$  le groupe des unités de l'anneau des entiers de  $\mathbf{K}$ ,  $d_\mathbf{K}$  le discriminant de  $\mathbf{K}$ , et  $h_\mathbf{K}$  le nombre de classes d'idéaux de  $\mathbf{K}$ . Pour  $\mathbf{N}$  un corps à multiplication complexe de sous-corps totalement réel maximal noté  $\mathbf{N}^+$ , on sait que  $h_{\mathbf{N}^+}$  divise  $h_\mathbf{N}$ . Leur quotient noté  $h_{\mathbf{N}^-}$  est appelé le *nombre de classes relatif* de  $\mathbf{N}$ , et l'indice  $Q_\mathbf{N} = (\mathbf{U}_\mathbf{N} : \mathbf{W}_\mathbf{N}\mathbf{U}_{\mathbf{N}^+})$ , appelé l'*indice de Hasse* de  $\mathbf{N}$ , vaut 1 ou 2 (voir [Wa, Chapter 4]). La formule analytique suivante donne le nombre de classes relatif de  $\mathbf{N}$  :

$$(1) \quad h_{\mathbf{N}^-} = \frac{Q_\mathbf{N} w_\mathbf{N}}{(2\pi)^n} \sqrt{\left| \frac{d_\mathbf{N}}{d_{\mathbf{N}^+}} \right|} L(1, \chi_\mathbf{N}),$$

où  $n$  est le degré de  $\mathbf{N}^+$  et  $\chi_\mathbf{N}$  le caractère de l'extension quadratique  $\mathbf{N}/\mathbf{N}^+$ . Finalement, nous notons  $j_{\mathbf{N}/\mathbf{N}^+}$  l'application canonique du groupe des classes de  $\mathbf{N}^+$  dans celui de  $\mathbf{N}$ .

LEMME A (voir le chapitre 10 de [Wa]). *Le noyau de  $j_{\mathbf{N}/\mathbf{N}^+}$  est d'ordre  $\leq 2$ . Si  $Q_\mathbf{N} = 2$  alors ce noyau est d'ordre 1. Si ce noyau est d'ordre 1, alors  $h_{\mathbf{N}^-}$  impair implique  $h_{\mathbf{N}^+}$  impair. En particulier, un corps à multiplication complexe d'indice de Hasse égal à 2 et de nombre de classes relatif impair est également de nombre de classes impair.*

Nous ferons un usage répété de cette propriété.

**1. Corps des genres (de corps quadratiques) à nombres de classes relatifs égaux à 1.** Soit  $\mathbf{k}$  un corps quadratique de discriminant  $d_{\mathbf{k}}$ . Nous notons  $p_i$  ( $1 \leq i \leq t$ ) les diviseurs premiers distincts de  $d_{\mathbf{k}}$  et posons

$$p_i^* = \begin{cases} p_i & \text{si } p_i \equiv 1 \pmod{4}, \\ -p_i & \text{si } p_i \equiv 3 \pmod{4}, \\ -4, -8 \text{ ou } 8 & \text{si } p_i = 2. \end{cases}$$

Il existe alors une unique écriture de  $d_{\mathbf{k}}$  sous la forme  $d_{\mathbf{k}} = \prod_{i=1}^t p_i^*$  (i.e., nous décomposons  $d_{\mathbf{k}}$  en un produit de discriminants fondamentaux, où un discriminant fondamental est un discriminant de corps quadratique ramifié en exactement un seul nombre premier). Le corps

$$(2) \quad \mathbf{G}_t = \mathbb{Q}(\sqrt{p_1^*}, \dots, \sqrt{p_t^*}),$$

est appelé le *corps des genres* de  $\mathbf{k}$ . C'est l'extension abélienne de  $\mathbb{Q}$ , non ramifiée sur  $\mathbf{k}$  aux places finies et maximale pour ces deux propriétés. Réciproquement, pour des  $p_i$  deux à deux distincts, un corps  $\mathbf{G}_t$  est appelé un *corps de genres*. C'est le corps des genres d'un unique corps quadratique : le corps  $\mathbb{Q}(\sqrt{p_1^* p_2^* \dots p_t^*})$ , corps quadratique qui peut être aussi bien réel qu'imaginaire. Nous notons  $r$  le nombre des  $p_i^*$  négatifs et  $s$  le nombre des  $p_i^*$  positifs, de sorte que  $t = r + s$  et que  $\mathbf{G}_t$  est imaginaire si et seulement si  $r \geq 1$ , ce que nous supposons pour toute la suite. Noter que  $\mathbf{G}_t$  est le corps des genres d'un corps quadratique réel pour  $r$  pair, et est le corps des genres d'un corps quadratique imaginaire pour  $r$  impair. Nous notons alors  $h_t^-$  le nombre de classes relatif et  $Q_t$  l'indice de Hasse de  $\mathbf{G}_t$ .

LEMME B (voir [Uch 1, Prop. 3]). *Nous avons  $Q_t = 1$  si  $r = 1$ , et  $Q_t = 2$  si  $r \geq 2$ .*

Un corps des genres imaginaire  $\mathbf{G}_t$  étant un compositum de corps quadratiques de conducteurs deux à deux premiers entre eux, son nombre de classes relatif est très facile à calculer puisque l'on a

$$(3) \quad h_t^- = 2Q_t \prod_{\mathbf{F}} (h_{\mathbf{F}}/2),$$

où ce produit est pris sur tous les sous-corps quadratiques imaginaires  $\mathbf{F}$  de  $\mathbf{G}_t$  (voir [Uch 2, p. 160]).

Finalement, pour des  $p_i^*$  tels que le corps quadratique  $\mathbb{Q}(\sqrt{p_1^* p_2^* \dots p_t^*})$  soit imaginaire, nous notons  $h_{1,2,\dots,t}$  son nombre de classes.

PROPOSITION 1. *Si  $\mathbf{G}_t$  et  $\mathbf{G}_{t'}$  sont deux corps de genres imaginaires et si  $\mathbf{G}_{t'}$  contient  $\mathbf{G}_t$ , alors  $h_t^-$  divise  $h_{t'}^-$ . De plus, si le nombre de classes relatif d'un corps de genres imaginaire  $\mathbf{G}_t$  est impair, alors  $t \leq 3$  et  $(r, s) \in \{(1, 0), (1, 1), (2, 0), (2, 1), (3, 0)\}$ , et nous avons les expressions suivantes de*

$h_t^-$  sous forme de produits d'entiers positifs :

$$h_t^- = \begin{cases} h_1 & \text{si } t = 1 \text{ et } (r, s) = (1, 0), \\ h_1(h_{1,2}/2) & \text{si } t = 2 \text{ et } (r, s) = (1, 1) \\ & \text{(avec le choix } p_2^* > 0), \\ h_1 h_2 & \text{si } t = 2 \text{ et } (r, s) = (2, 0), \\ h_1 h_2 (h_{1,2}/2)(h_{1,3}/2) & \text{si } t = 3 \text{ et } (r, s) = (2, 1) \\ & \text{(avec le choix } p_3^* > 0), \\ h_1 h_2 h_3 (h_{1,2,3}/4) & \text{si } t = 3 \text{ et } (r, s) = (3, 0). \end{cases}$$

En conséquence, la connaissance de tous les corps quadratiques imaginaires de nombres de classes 1 (il y en a 9) ou 2 (il y en a 18) conduit à la détermination de tous les corps de genres imaginaires de nombres de classes relatifs égaux à 1. Finalement, un corps de genres imaginaire de degré  $\geq 8$  et de nombre de classes relatif impair est de degré 8 et de nombre de classes impair, car d'indice de Hasse égal à 2.

*Preuve.* Les deux ingrédients de la preuve sont la formule (3) et le fait qu'un corps quadratique imaginaire de conducteur divisible par  $t$  facteurs premiers est de nombre de classes divisible par  $2^{t-1}$ . Pour la première partie de cette Proposition 1, nous raisonnons par récurrence sur  $t$  en distinguant le cas  $p_{t+1}^* > 0$  du cas  $p_{t+1}^* < 0$ .

Pour  $p_{t+1}^* > 0$  nous avons  $Q_{t+1} = Q_t$  et

$$h_{t+1}^-/h_t^- = \prod_{\mathbf{F}} (h_{\mathbf{F}}/2),$$

où ce produit est pris sur les sous-corps quadratiques imaginaires de  $\mathbf{G}_{t+1}$  non inclus dans  $\mathbf{G}_t$ . Tous ces corps sont de conducteurs divisibles par  $p_{t+1}^*$  et par au moins un autre des  $p_i^*$  avec  $1 \leq i \leq t$  (en fait, divisibles par un nombre impairs de  $p_i^*$  tels que  $p_i^* < 0$  et  $1 \leq i \leq t$ ). Ils sont donc de nombres de classes pairs, c'est-à-dire que tous les  $h_{\mathbf{F}}/2$  de ce produit sont des entiers restreintement positifs.

Pour  $p_{t+1}^* < 0$  nous avons  $Q_{t+1} = 2$  et

$$(4) \quad h_{t+1}^-/h_t^- = (2/Q_t)(h_{t+1}/2) \prod_{\mathbf{F}} (h_{\mathbf{F}}/2),$$

où ce produit est pris sur les sous-corps quadratiques imaginaires de  $\mathbf{G}_{t+1}$  non inclus dans  $\mathbf{G}_t$  et distincts de  $\mathbb{Q}(\sqrt{p_{t+1}^*})$ . Tous ces corps sont de conducteurs divisibles par  $p_{t+1}^*$  et par au moins un autre  $p_i^*$  avec  $1 \leq i \leq t$ , donc ils sont de nombres de classes pairs. Ces corps  $\mathbf{F}$  sont de plus de conducteurs divisibles par un nombre pair éventuellement nul de  $p_i^* < 0$  tels que  $1 \leq i \leq t$ . S'il existe au moins un tel  $\mathbf{F}$  dans ce produit (4) de conducteur divisible par un nombre pair non nul de  $p_i^* < 0$  tels que  $1 \leq i \leq t$ , alors son nombre de classes est divisible par 4 et  $h_{t+1}^-/h_t^-$  est clairement un entier. S'il n'existe pas de tel  $\mathbf{F}$  dans ce produit (4) de conducteur divisible par

un nombre pair non nul de  $p_i^* < 0$  tels que  $1 \leq i \leq t$ , alors  $Q_t = 1$  et  $h_{t+1}^-/h_t^- = h_{t+1} \prod_{\mathbf{F}}(h_{\mathbf{F}}/2)$  est un entier puisque ce produit est pris sur des sous-corps quadratiques imaginaires de conducteurs divisibles par au moins deux facteurs premiers distincts, donc de nombres de classes pairs.

Pour la seconde partie de cette Proposition 1, nous remarquons que pour  $r = 4$  et  $s = 0$  la formule (3) (écrite légèrement différemment) donne

$$h_4^- = 4h_1h_2h_3h_4(h_{1,2,3}/4)(h_{1,2,4}/4)(h_{1,3,4}/4)(h_{2,3,4}/4).$$

D'après la première partie de cette proposition, 4 divise donc  $h_t^-$  pour  $r \geq 4$ . De même, pour  $r = 3$  et  $s = 1$  et en rangeant les  $p_i^*$  de telle sorte que  $p_i^* < 0$  pour  $1 \leq i \leq 3$ , la formule (3) donne

$$h_4^- = 4h_1h_2h_3(h_{1,4}/2)(h_{2,4}/2)(h_{3,4}/2)(h_{1,2,3}/4)(h_{1,2,3,4}/8),$$

ce qui donne que 4 divise  $h_t^-$  pour  $r = 3$  et  $s \geq 1$ . De même, pour  $r = 1$  et  $s = 2$  nous avons

$$h_3^- = 2h_1(h_{1,2}/2)(h_{1,3}/2)(h_{1,2,3}/4),$$

ce qui donne que 2 divise  $h_t^-$  pour  $r \geq 1$  et  $s \geq 2$ . Si  $h_t^-$  est impair, nous avons donc  $r \leq 3$ , et  $r = 3$  implique  $s = 0$ , et  $r = 2$  implique  $s \leq 1$ , et  $r = 1$  implique  $s \leq 1$ , c'est-à-dire que nous sommes dans un des cinq cas considérés dans cette Proposition 1. Finalement, les formules pour  $h_t^-$  de cette Proposition 1 résultent de (3). ■

**COROLLAIRE 2.** *Il y a 73 corps de genres de nombres de classes relatifs égaux à 1, et 30 d'entre eux sont des corps de genres de corps quadratiques imaginaires et 43 d'entre eux sont des corps de genres de corps quadratiques réels. De plus, 69 d'entre eux sont principaux, 3 d'entre eux sont de nombres de classes 3, à savoir les corps des genres des corps quadratiques réels  $\mathbb{Q}(\sqrt{7 \cdot 67})$ ,  $\mathbb{Q}(\sqrt{2 \cdot 163})$ , et  $\mathbb{Q}(\sqrt{11 \cdot 43})$ , et 1 d'entre eux est de nombre de classes 5, à savoir le corps des genres du corps quadratique réel  $\mathbb{Q}(\sqrt{19 \cdot 43})$ .*

**Preuve.** Nous avons la Table 1 suivante des corps quadratiques imaginaires  $\mathbf{k}$  de nombres de classes  $\leq 2$  (voir [M-W], [Sta 1] et [Sta 2]) :

Table 1

$d_{\mathbf{k}}$	$h_{\mathbf{k}}$	$d_{\mathbf{k}}$	$h_{\mathbf{k}}$
-3	1	-19	1
-4	1	-43	1
-7	1	-67	1
-8	1	-163	1
-11	1		

**Table 1** (cont.)

$d_{\mathbf{k}}$	$h_{\mathbf{k}}$	$d_{\mathbf{k}}$	$h_{\mathbf{k}}$
-15 = (-3, 5)	2	-115 = (-23, 5)	2
-20 = (-4, 5)	2	-123 = (-3, 41)	2
-24 = (-3, 8)	2	-148 = (-4, 37)	2
-35 = (-7, 5)	2	-187 = (-11, 17)	2
-40 = (-8, 5)	2	-232 = (-8, 29)	2
-51 = (-3, 17)	2	-235 = (-47, 5)	2
-52 = (-4, 13)	2	-267 = (-3, 89)	2
-88 = (-11, 8)	2	-403 = (-31, 13)	2
-91 = (-7, 13)	2	-427 = (-7, 61)	2

Envisageons successivement les cinq cas de la Proposition 1.

Pour  $(r, s) = (1, 0)$  nous avons  $h_t^- = 1$  pour 9 cas.

Pour  $(r, s) = (1, 1)$  nous avons  $h_t^- = 1$  si et seulement si  $h_1 = 1$  et  $h_{1,2} = 2$ . Cela arrive d'après la Table 1 pour 15 cas (on ne peut pas avoir  $p_1^* \in \{-23, -31, -47\}$ ).

Pour  $(r, s) = (2, 0)$  nous avons  $h_t^- = 1$  si et seulement si  $h_1 = h_2 = 1$ , et nous avons donc  $h_t^- = 1$  pour 35 cas (penser à ne pas inclure le cas  $\mathbb{Q}(\sqrt{-4}, \sqrt{-8})$ ).

Pour  $(r, s) = (2, 1)$  nous avons  $h_t^- = 1$  si et seulement si  $h_1 = h_2 = 1$  et  $h_{1,2} = h_{1,3} = 2$ , c'est-à-dire que  $\mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*}, \sqrt{p_3^*})$  est de nombre de classes relatif égal à 1 si et seulement si  $\mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_3^*})$  et  $\mathbb{Q}(\sqrt{p_2^*}, \sqrt{p_3^*})$  sont de nombres de classes relatifs égaux à 1, i.e. apparaissent tous deux au cas précédent  $(r, s) = (1, 1)$ . Cela arrive pour 8 cas (on ne peut pas avoir  $p_3^* \in \{29, 37, 41, 61, 89\}$ , pour  $p_3^* = 8, 13$  ou  $17$  on a un seul choix possible pour  $(p_1^*, p_2^*, p_3^*)$ , et pour  $p_3^* = 5$  on a 5 choix possibles pour  $(p_1^*, p_2^*, p_3^*)$ ).

Finalement, pour  $(r, s) = (3, 0)$  nous avons  $h_t^- = 1$  si et seulement si  $h_1 = h_2 = h_3 = 1$  et  $h_{1,2,3} = 4$ . Cela arrive pour 6 cas.

Ces occurrences de  $h_t^- = 1$  sont colligées à la Table 2.

**Table 2**

$\{p_i^*\}$	$h_t^+$	$\{p_i^*\}$	$h_t^+$	$\{p_i^*\}$	$h_t^+$	$\{p_i^*\}$	$h_t^+$
$\{-3\}$	1	$\{-3, 5\}$	1	$\{-7, 61\}$	1	$\{-3, -19\}$	1
$\{-4\}$	1	$\{-3, 8\}$	1	$\{-8, 5\}$	1	$\{-3, -43\}$	1
$\{-7\}$	1	$\{-3, 17\}$	1	$\{-8, 29\}$	1	$\{-3, -67\}$	1
$\{-8\}$	1	$\{-3, 41\}$	1	$\{-11, 8\}$	1	$\{-3, -163\}$	1
$\{-11\}$	1	$\{-3, 89\}$	1	$\{-11, 17\}$	1	$\{-4, -7\}$	1
$\{-19\}$	1	$\{-4, 5\}$	1			$\{-4, -11\}$	1
$\{-43\}$	1	$\{-4, 13\}$	1	$\{-3, -4\}$	1	$\{-4, -19\}$	1
$\{-67\}$	1	$\{-4, 37\}$	1	$\{-3, -7\}$	1	$\{-4, -43\}$	1
$\{-163\}$	1	$\{-7, 5\}$	1	$\{-3, -8\}$	1	$\{-4, -67\}$	1
		$\{-7, 13\}$	1	$\{-3, -11\}$	1	$\{-4, -163\}$	1

Table 2 (cont.)

$\{p_i^*\}$	$h_t^+$	$\{p_i^*\}$	$h_t^+$	$\{p_i^*\}$	$h_t^+$	$\{p_i^*\}$	$h_t^+$
$\{-7, -8\}$	1	$\{-8, -163\}$	3	$\{-67, -163\}$	1	$\{-3, -4, -7\}$	1
$\{-7, -11\}$	1	$\{-11, -19\}$	1			$\{-3, -4, -11\}$	1
$\{-7, -19\}$	1	$\{-11, -43\}$	3	$\{-3, -4, 5\}$	1	$\{-3, -4, -19\}$	1
$\{-7, -43\}$	1	$\{-11, -67\}$	1	$\{-3, -7, 5\}$	1	$\{-3, -7, -8\}$	1
$\{-7, -67\}$	3	$\{-11, -163\}$	1	$\{-3, -8, 5\}$	1	$\{-3, -11, -19\}$	1
$\{-7, -163\}$	1	$\{-19, -43\}$	5	$\{-3, -11, 8\}$	1	$\{-4, -7, -19\}$	1
$\{-8, -11\}$	1	$\{-19, -67\}$	1	$\{-3, -11, 17\}$	1		
$\{-8, -19\}$	1	$\{-19, -163\}$	1	$\{-4, -7, 5\}$	1		
$\{-8, -43\}$	1	$\{-43, -67\}$	1	$\{-4, -7, 13\}$	1		
$\{-8, -67\}$	1	$\{-43, -163\}$	1	$\{-7, -8, 5\}$	1		

Les nombres de classes des  $\mathbf{G}_t$  correspondants sont égaux aux nombres de classes  $h_t^+$  des  $\mathbf{G}_t^+$  correspondants. Expliquons comment nous avons déterminé ces  $h_t^+$  donnés dans cette Table 2. Pour  $(r, s) = (1, 0)$  on a  $\mathbf{G}_t^+ = \mathbb{Q}$  qui est principal. Pour  $(r, s) = (2, 0)$  on a  $\mathbf{G}_t^+ = \mathbb{Q}(\sqrt{p_1^* p_2^*})$  qui est quadratique réel donc de nombre de classes aisément calculable. Pour  $(r, s) = (1, 1)$  on a  $\mathbf{G}_t^+ = \mathbb{Q}(\sqrt{p_2^*})$  qui est quadratique réel donc de nombre de classes aisément calculable. Pour  $(r, s) = (3, 0)$  on a  $\mathbf{G}_t^+ = \mathbb{Q}(\sqrt{p_1^* p_2^*}, \sqrt{p_1^* p_3^*})$  qui est biquadratique bicyclique réel donc de nombre de classes moins aisément calculable. Néanmoins, la partie impaire du groupe des classes d'un corps biquadratique bicyclique étant isomorphe au produit des parties impaires des groupes des classes de ses trois sous-corps quadratiques, et puisque  $Q_t = 2$  pour ce cas et que donc on sait que le nombre de classes de  $\mathbf{G}_t^+$  est impair lorsque  $h_t^-$  est impair (voir Lemme A), on obtient que le nombre de classes de  $\mathbf{G}_t^+$  est égal à la partie impaire du produit des trois nombres de classes de ses sous-corps quadratiques réels  $\mathbb{Q}(\sqrt{p_1^* p_2^*})$ ,  $\mathbb{Q}(\sqrt{p_1^* p_3^*})$ , et  $\mathbb{Q}(\sqrt{p_2^* p_3^*})$ . Finalement, le raisonnement est le même pour le dernier cas  $(r, s) = (2, 1)$ , où  $\mathbf{G}_t^+ = \mathbb{Q}(\sqrt{p_1^* p_2^*}, \sqrt{p_3^*})$ . ■

**2. Corps quadratiques imaginaires à corps de classes de Hilbert principaux et à multiplication complexe.** Dans tout ce paragraphe  $\mathbf{k}$  désigne un corps quadratique imaginaire.

**THÉORÈME 3.** *Le corps de classes de Hilbert  $\mathbf{H}$  d'un corps quadratique imaginaire  $\mathbf{k}$  est galoisien sur le corps des nombres rationnels et à groupe de Galois  $\mathbf{G} = \text{Gal}(\mathbf{H}/\mathbb{Q})$  un groupe diédral généralisé, c'est-à-dire que  $\mathbf{G}$  est le produit semi-direct du groupe abélien  $\mathbf{A} = \text{Gal}(\mathbf{H}/\mathbf{k})$  canoniquement isomorphe au groupe des classes d'idéaux de  $\mathbf{k}$  par le groupe  $\{\text{Id}, \sigma\}$  d'ordre 2, où la conjugaison complexe  $\sigma \in \mathbf{G}$  agit sur  $\mathbf{A}$  par  $\sigma a \sigma^{-1} = a^{-1}$ .*

*Ce corps  $\mathbf{H}$  est un corps à multiplication complexe si et seulement si le groupe des classes d'idéaux de  $\mathbf{k}$  est d'exposant  $\leq 2$  (c'est-à-dire isomorphe à*

un produit fini de copies de  $\mathbb{Z}/2\mathbb{Z}$ ), et dans ce cas  $\mathbf{H}$  est le corps des genres  $\mathbf{G}_{\mathbf{k}}$  de  $\mathbf{k}$ . En conséquence, il existe 30 corps quadratiques imaginaires à corps de classes de Hilbert des corps principaux à multiplication complexe.

*Preuve.* Le symbole d'Artin  $\left[\frac{\mathbf{H}/\mathbf{k}}{\bullet}\right]$  induit un isomorphisme du groupe des classes de  $\mathbf{k}$  sur le groupe de Galois  $\text{Gal}(\mathbf{H}/\mathbf{k}) = \mathbf{A}$  de l'extension non ramifiée  $\mathbf{H}/\mathbf{k}$ . Puisque le groupe  $\{\text{Id}, \sigma\}$  est un relèvement du groupe quotient  $\mathbf{G}/\mathbf{A}$ , alors  $\mathbf{G}$  est produit semi-direct du groupe abélien  $\mathbf{A}$  par  $\{\text{Id}, \sigma\}$ , où  $\sigma$  opère sur  $\mathbf{A}$  par automorphismes intérieurs. Reste à voir que  $\sigma$  opère par inversion. Soit  $\mathcal{P}_{\mathbf{k}}$  un idéal premier de  $\mathbf{k}$  au dessus de  $p$ . Alors,

$$\sigma \left[ \frac{\mathbf{H}/\mathbf{k}}{\mathcal{P}_{\mathbf{k}}} \right] \sigma^{-1} = \left[ \frac{\mathbf{H}/\mathbf{k}}{\sigma(\mathcal{P}_{\mathbf{k}})} \right] = \left[ \frac{\mathbf{H}/\mathbf{k}}{\mathcal{P}_{\mathbf{k}}} \right]^{-1},$$

et ce parce que l'idéal  $\mathcal{P}_{\mathbf{k}}\sigma(\mathcal{P}_{\mathbf{k}}) = (N_{\mathbf{k}/\mathbb{Q}}(\mathcal{P}_{\mathbf{k}}))$  étant principal, la classe de l'idéal  $\sigma(\mathcal{P}_{\mathbf{k}})$  est l'inverse de la classe de l'idéal  $\mathcal{P}_{\mathbf{k}}$ . C'est la preuve de [Cox].

Pour la seconde partie de ce Théorème 3, nous remarquons qu'un corps galoisien totalement imaginaire (ce qui est évidemment le cas de  $\mathbf{H}$ ) est un corps à multiplication complexe si et seulement si la conjugaison complexe est dans le centre de son groupe de Galois. Dans notre situation, cela implique  $a^{-1} = \sigma a \sigma^{-1} = a$ , soit  $a^2 = 1$ , pour tout  $a$  de  $\mathbf{A}$ , donc implique que le groupe des classes de  $\mathbf{k}$  est d'exposant  $\leq 2$ . Réciproquement, si le groupe des classes de  $\mathbf{k}$  est d'exposant  $\leq 2$  alors  $\sigma$  commute à  $\mathbf{A}$ , de sorte que  $\mathbf{H}/\mathbb{Q}$  est abélienne et que  $\mathbf{H}$  est donc le corps des genres de  $\mathbf{k}$ .

La dernière partie de ce Théorème 3 résulte du Corollaire 2. ■

### 3. Corps quadratiques réels dont les corps de classes de Hilbert au sens restreint sont principaux et à multiplication complexe.

Dans tout ce paragraphe  $\mathbf{k}$  désigne un corps quadratique réel. Nous notons  $\mathbf{H}_l(\mathbf{k})$  et  $\mathbf{H}_s(\mathbf{k})$  ses corps de classes de Hilbert aux sens large et restreint, i.e.,  $\mathbf{H}_l(\mathbf{k})/\mathbf{k}$  est l'extension de  $\mathbf{k}$  abélienne non ramifiée en toutes places (finies et infinies), et maximale pour ces propriétés (en conséquence,  $\mathbf{H}_s(\mathbf{k})$  est un corps galoisien totalement réel), et  $\mathbf{H}_s(\mathbf{k})/\mathbf{k}$  est l'extension de  $\mathbf{k}$  abélienne non ramifiée en toutes places finies, et maximale pour ces propriétés (en conséquence,  $\mathbf{H}_l(\mathbf{k})$  est un corps galoisien). Remarquons que  $\mathbf{H}_l(\mathbf{k})$  est donc inclus dans  $\mathbf{H}_s(\mathbf{k})$ . On sait que le groupe de Galois de  $\mathbf{H}_l(\mathbf{k})/\mathbf{k}$  est isomorphe au groupe des classes de  $\mathbf{k}$ , alors que le groupe de Galois de  $\mathbf{H}_s(\mathbf{k})/\mathbf{k}$  est isomorphe au groupe des classes au sens restreint de  $\mathbf{k}$ . Le degré relatif  $[\mathbf{H}_s(\mathbf{k}) : \mathbf{H}_l(\mathbf{k})]$  vaut donc 1 ou 2 selon que l'unité fondamentale de  $\mathbf{k}$  est de norme  $-1$  ou  $+1$ . Lorsque ce degré relatif vaut 2, le corps  $\mathbf{H}_s(\mathbf{k})$  ne saurait être totalement réel (par maximalité de  $\mathbf{H}_l(\mathbf{k})$ ), il est donc totalement imaginaire (puisque galoisien), et est donc un corps à multiplication complexe de sous-corps totalement réel maximal  $\mathbf{H}_l(\mathbf{k})$ . Et réciproquement. On considère également  $\mathbf{H}_{l,2}(\mathbf{k})$  et  $\mathbf{H}_{s,2}(\mathbf{k})$ , les 2-corps de classes de Hilbert aux sens large



et restreint de  $\mathbf{k}$ . On a les mêmes résultats pour  $\mathbf{H}_{l,2}(\mathbf{k})$  et  $\mathbf{H}_{s,2}(\mathbf{k})$ . Nous notons  $h_s(\mathbf{k})$  le nombre de classes restreintes de  $\mathbf{k}$  et définissons  $n$  et  $h_{\text{imp}}$  par  $h_s(\mathbf{k}) = 2^n h_{\text{imp}}$  avec  $h_{\text{imp}}$  impair (égal à la partie impaire du nombre de classes  $h_{\mathbf{k}}$ ). Nous avons donc le diagramme de sous-corps suivant :

$$\mathbf{H}_s(\mathbf{k}) \xrightarrow{h_{\text{imp}}} \mathbf{H}_{s,2}(\mathbf{k}) \xrightarrow{2^{n-t+1}} \mathbf{G}_{\mathbf{k}} \xrightarrow{2^{t-1}} \mathbf{k} = \mathbb{Q}(\sqrt{d_{\mathbf{k}}}) \xrightarrow{2} \mathbb{Q}$$

et nous avons prouvé :

LEMME 4. *Les trois propriétés suivantes sont équivalentes :*

- (a)  $\mathbf{H}_s(\mathbf{k})$  est un corps à multiplication complexe.
- (b)  $\mathbf{H}_{s,2}(\mathbf{k})$  est un corps à multiplication complexe.
- (c) La norme de l'unité fondamentale de  $\mathbf{k}$  vaut  $+1$ .

*Si elles sont satisfaites, le corps  $\mathbf{H}_l(\mathbf{k})$  est le sous-corps totalement réel maximal de  $\mathbf{H}_s(\mathbf{k})$ , et  $\mathbf{H}_{l,2}(\mathbf{k})$  est celui de  $\mathbf{H}_{s,2}(\mathbf{k})$ .*

Dans toute la suite, nous supposons l'unité fondamentale de  $\mathbf{k}$  de norme  $+1$ , et cela implique que le 2-Sylow du groupe des classes au sens restreint de  $\mathbf{k}$  est d'ordre supérieur ou égal à 2. Le corps  $\mathbf{H}_s(\mathbf{k})$  est donc un corps à multiplication complexe de sous-corps totalement réel maximal  $\mathbf{H}_l(\mathbf{k})$ , le corps  $\mathbf{H}_{s,2}(\mathbf{k})$  est un corps à multiplication complexe de sous-corps totalement réel maximal  $\mathbf{H}_{l,2}(\mathbf{k})$ , et  $\mathbf{H}_{s,2}(\mathbf{k})$  est au moins quadratique sur  $\mathbf{k}$ , c'est-à-dire que  $\mathbf{H}_s(\mathbf{k})$  est d'ordre  $2^n h$  avec  $n \geq 2$  et  $h$  impair.

THÉORÈME 5. *Soit  $\mathbf{k}$  un corps quadratique réel d'unité fondamentale de norme valant  $+1$ . Alors, le corps de classes de Hilbert au sens restreint  $\mathbf{H}_s(\mathbf{k})$  est un corps à multiplication complexe galoisien sur le corps des nombres rationnels et à groupe de Galois  $\mathbf{G} = \text{Gal}(\mathbf{H}_s(\mathbf{k})/\mathbb{Q})$  un groupe diédral généralisé, c'est-à-dire que  $\mathbf{G}$  est le produit semi-direct d'un groupe abélien  $\mathbf{A} = \text{Gal}(\mathbf{H}_s(\mathbf{k})/\mathbf{k})$  canoniquement isomorphe au groupe des classes au sens restreint de  $\mathbf{k}$  par le groupe  $\{\text{Id}, \sigma\}$  d'ordre 2 (où  $\sigma$  est n'importe quel relèvement en un élément de  $\mathbf{G}$  du  $\mathbb{Q}$ -isomorphisme non trivial de  $\mathbf{k}$ ) qui agit sur  $\mathbf{A}$  par  $\sigma a \sigma^{-1} = a^{-1}$ . Un tel produit semi-direct définit un groupe abélien si et seulement si le groupe  $\mathbf{A}$  est d'exposant  $\leq 2$ , c'est-à-dire est isomorphe à un produit fini de copies de  $\mathbb{Z}/2\mathbb{Z}$ . En conséquence,  $\mathbf{H}_s(\mathbf{k})$  est abélien si et seulement si il est égal à  $\mathbf{G}_{\mathbf{k}}$ , le corps des genres de  $\mathbf{k}$ , et il existe donc précisément 39 corps quadratiques réels à corps de classes de Hilbert au sens restreint des corps à multiplication complexe abéliens principaux.*

Preuve. Posons  $\mathbf{H} = \mathbf{H}_s(\mathbf{k})$ . Le symbole d'Artin  $\left[ \frac{\mathbf{H}/\mathbf{k}}{\bullet} \right]$  induit un isomorphisme du groupe des classes au sens restreint de  $\mathbf{k}$  sur le groupe de Galois  $\mathbf{A} = \text{Gal}(\mathbf{H}/\mathbf{k})$  de l'extension non ramifiée aux places finies  $\mathbf{H}/\mathbf{k}$ . Soit  $\sigma$  l'un quelconque des relèvements en un élément de  $\mathbf{G} = \text{Gal}(\mathbf{H}/\mathbb{Q})$  du  $\mathbb{Q}$ -isomorphisme non trivial de l'extension quadratique  $\mathbf{k}/\mathbb{Q}$ . Nous montrons d'abord que  $\sigma$  est d'ordre 2 dans  $\mathbf{G}$ . En effet, d'après le théorème de

Tchébotarev, il existe un idéal premier  $\mathcal{P}_H$  de  $\mathbf{H}$  non ramifié dans  $\mathbf{H}/\mathbb{Q}$  tel que  $\sigma = \left[ \frac{\mathbf{H}/\mathbb{Q}}{\mathcal{P}_H} \right]$ . Soit  $\mathcal{P}_k$  la trace sur  $\mathbf{k}$  de  $\mathcal{P}_H$ . Alors, la restriction de  $\sigma$  à  $\mathbf{k}$  est égale à  $\left[ \frac{\mathbf{k}/\mathbb{Q}}{\mathcal{P}_k} \right]$ , et agit donc sur  $\sqrt{d_k}$  par multiplication par le symbole de Kronecker  $(d_k/p)$ . Puisque cette restriction est non triviale, ce symbole de Kronecker vaut  $-1$ , c'est-à-dire que  $\mathcal{P}_k$  est inerte dans  $\mathbf{k}/\mathbb{Q}$ , de sorte que  $\mathcal{P}_k$  est de degré résiduel égal à 2. Mais alors,

$$1 = \left[ \frac{\mathbf{H}/\mathbf{k}}{\mathcal{P}_k} \right] = \left[ \frac{\mathbf{H}/\mathbf{k}}{\mathcal{P}_H} \right] = \left[ \frac{\mathbf{H}/\mathbb{Q}}{\mathcal{P}_H} \right]^2 = \sigma^2$$

(cette première égalité résultant de ce que  $\mathcal{P}_k = (p)$  est principal au sens restreint dans  $\mathbf{k}$ , et cette seconde de ce que  $\mathbf{H}/\mathbf{k}$  est abélienne). La preuve suit maintenant celle du Théorème 3. ■

*Remarque.* Le corps des genres  $\mathbf{G}_k$  est imaginaire si et seulement si la conjugaison complexe n'est pas un carré dans  $\mathbf{A}$ . En effet,  $\mathbf{G}_k/\mathbb{Q}$  étant la sous-extension abélienne maximale de  $\mathbf{H}_s(\mathbf{k})/\mathbb{Q}$ , alors  $\text{Gal}(\mathbf{H}_s(\mathbf{k})/\mathbf{G}_k)$  est égal à  $D(\mathbf{G}) = \mathbf{A}^2$ , où  $D(\mathbf{G})$  est le groupe dérivé de  $\mathbf{G}$ .

**PROPOSITION 6.** *Soit  $\mathbf{k}$  un corps quadratique réel dont le corps de classes de Hilbert au sens restreint  $\mathbf{H} = \mathbf{H}_s(\mathbf{k})$  est un corps à multiplication complexe principal. Soit  $\mathbf{M}$  un corps à multiplication complexe tel que  $\mathbf{k} \subseteq \mathbf{M} \subseteq \mathbf{H}$ . Si  $h_{\mathbf{H}} = 1$ , alors  $\mathbf{H}$  est le corps de classes de Hilbert de  $\mathbf{M}$ , et  $h_{\mathbf{M}}^- = 1$  et  $h_{\mathbf{M}} = [\mathbf{H} : \mathbf{M}]$ . En particulier, si  $\mathbf{G}_k$  est imaginaire, alors  $\mathbf{G}_k$  est de nombre de classes relatif égal à 1, donc  $\mathbf{k}$  est l'un des 44 corps quadratiques réels donnés au Corollaire 2, et  $\mathbf{H}_s(\mathbf{k})$  est le corps de classes de Hilbert de  $\mathbf{G}_k$ . En particulier, 39 de ces 43 tels  $\mathbf{H}_s(\mathbf{k})$  sont principaux et égaux à  $\mathbf{G}_k$ .*

*Preuve.* Soit  $\mathbf{H}_M$  le corps de classes de Hilbert de  $\mathbf{M}$ . L'extension  $\mathbf{H}/\mathbf{M}$  étant abélienne et non ramifiée, on a  $\mathbf{H} \subseteq \mathbf{H}_M$ . Réciproquement, puisque  $\mathbf{H}_M/\mathbf{M}$  est abélienne non ramifiée, alors  $\mathbf{H}\mathbf{H}_M/\mathbf{H}$  est abélienne non ramifiée, et  $\mathbf{H}$  étant principal, on a  $\mathbf{H}\mathbf{H}_M \subseteq \mathbf{H}$ , soit  $\mathbf{H}_M \subseteq \mathbf{H}$ . Donc  $\mathbf{H}_M = \mathbf{H}$  et  $h_M = [\mathbf{H} : \mathbf{M}]$ . Maintenant,  $\mathbf{H}^+ = \mathbf{H}_l(\mathbf{k})$  est le corps de classes de Hilbert de  $\mathbf{k}$ , il contient donc  $\mathbf{M}^+$  (puisque  $\mathbf{M}^+/\mathbf{k}$  est non ramifiée aux places finies comme sous-extension de  $\mathbf{H}_s(\mathbf{k})/\mathbf{k}$  et non ramifiée aux places infinies puisque  $\mathbf{M}^+$  est totalement réel), et il est principal. Le même raisonnement que le précédent donne  $h_{M^+} = [\mathbf{H}^+ : \mathbf{M}^+] = [\mathbf{H} : \mathbf{M}]$ . D'où  $h_M^- = 1$ . ■

**PROPOSITION 7.** *Soit  $\mathbf{N}$  un corps à multiplication complexe, diédral et de degré  $8n$  avec  $n \geq 1$ . Alors  $w_{\mathbf{N}} = 2$ . De plus, si  $h_{\mathbf{N}}^-$  est impair, alors  $h_{\mathbf{N}}^-$  est un carré,  $Q_{\mathbf{N}} = 2$ , et  $h_{\mathbf{N}}$  est impair.*

*Preuve.* Soit  $\mathbf{G} = \langle a, b; a^{4n} = b^2 = 1, bab^{-1} = a^{-1} \rangle$  une présentation par générateurs et relations du groupe de Galois  $\mathbf{G} = \text{Gal}(\mathbf{N}/\mathbb{Q})$ . Puisque le centre de  $\mathbf{G}$  est réduit à  $\{1, a^{2n}\}$ , nous identifions la conjugaison complexe

à  $a^{2n}$ . Soient  $\mathbf{N}^+$ ,  $\mathbf{K}_1$ ,  $\mathbf{K}_2$  et  $\mathbf{K}^+$  les sous-corps de  $\mathbf{N}$  laissés fixes par les groupes  $\{1, a^{2n}\}$ ,  $\{1, b\}$ ,  $\{1, a^{2n}b\}$  et  $\{1, b, a^{2n}, a^{2n}b\}$ . Alors,  $\mathbf{N}/\mathbf{K}^+$  est bi-quadratique bicyclique et  $\mathbf{K}_2 = a^n(\mathbf{K}_1)$  est isomorphe à  $\mathbf{K}_1$ . Remarquons que le groupe dérivé de  $\mathbf{G}$  étant le groupe cyclique engendré par  $a^2$  qui contient la conjugaison complexe  $a^{2n}$ , alors le sous-corps abélien maximal de  $\mathbf{N}$  est bi-quadratique bicyclique réel. D'où  $w_{\mathbf{N}} = w_{\mathbf{K}_1} = w_{\mathbf{K}_2} = 2$ . En conséquence, les résultats de [Lou 3, Prop. 13] basés sur (1) et la factorisation de la fonction zêta de  $\mathbf{N}$  donnent

$$(5) \quad h_{\mathbf{N}}^- = (Q_{\mathbf{N}}/2)(h_{\mathbf{K}_1}^-/Q_{\mathbf{K}_1})^2 = (Q_{\mathbf{N}}/2)(h_{\mathbf{K}_2}^-/Q_{\mathbf{K}_2})^2.$$

En supposant  $h_{\mathbf{N}}^-$  impair, nous obtenons bien que  $Q_{\mathbf{N}} = 2$  puis que  $h_{\mathbf{N}}^-$  est un carré. Le dernier résultat découle du Lemme A. ■

**THÉOREME 8.** *Soit  $\mathbf{k}$  un corps quadratique réel d'unité fondamentale de norme valant +1. Supposons  $\mathbf{H}_s(\mathbf{k})$  de nombre de classes égal à 1 et  $\mathbf{G}_{\mathbf{k}}$  réel. Alors,  $\mathbf{H}_{s,2}(\mathbf{k})$  est de nombre de classes relatif égal à 1 et  $\mathbf{A}_2 = \text{Gal}(\mathbf{H}_{s,2}(\mathbf{k})/\mathbf{k})$  est cyclique d'ordre  $\geq 4$ , de sorte que  $\mathbf{H}_{s,2}(\mathbf{k})/\mathbb{Q}$  est diédrale de degré  $\geq 8$  une puissance de 2.*

*Preuve.* Supposons  $\mathbf{A}_2$  non cyclique, de sorte que  $\mathbf{A}/\mathbf{A}^2 = \text{Gal}(\mathbf{G}_{\mathbf{k}}/\mathbf{k})$  est d'ordre  $\geq 4$ , où  $\mathbf{A} = \text{Gal}(\mathbf{H}_s(\mathbf{k})/\mathbf{k})$ . Puisque  $\mathbf{G}_{\mathbf{k}}$  est réel, la conjugaison complexe  $c$  est un carré dans ce groupe de Galois  $\mathbf{A}$  et il existe un sous-groupe cyclique  $\mathbf{C}$  de  $\mathbf{A}$  d'ordre 4 et contenant  $c$ . Puisque  $\mathbf{A}_2$  n'est pas cyclique, il existe un sous-groupe d'ordre pair  $\mathbf{B}$  de  $\mathbf{A}$  tel que  $\mathbf{B} \cap \mathbf{C} = \{\text{Id}\}$  et tel que  $\mathbf{A}/\mathbf{B}$  soit cyclique d'ordre  $4n \geq 4$  (soit  $\chi_{\mathbf{C}}$  un caractère d'ordre 4 sur  $\mathbf{C}$  et  $\chi$  l'un quelconque de ses prolongements en un caractère de  $\mathbf{A}$ ). Il suffit de prendre  $\mathbf{B} = \text{Ker}(\chi)$ , car un tel  $\mathbf{B}$  est bien d'ordre pair puisque sinon  $\chi$  restreint à  $\mathbf{A}_2$  serait injectif et  $\mathbf{A}_2$  qui serait isomorphe à  $\chi(\mathbf{A}_2)$  serait cyclique). Soit  $\mathbf{H}$  le sous-corps de  $\mathbf{H}_s(\mathbf{k})$  obtenu par la correspondance de Galois :  $\text{Gal}(\mathbf{H}_s(\mathbf{k})/\mathbf{H}) = \mathbf{B}$ . Il n'est pas difficile de voir que  $\mathbf{B}$  étant distingué dans  $\mathbf{G} = \text{Gal}(\mathbf{H}_s(\mathbf{k})/\mathbb{Q})$ , alors  $\mathbf{H}$  est un corps galoisien diédral de degré  $8n \geq 8$ . De plus, la conjugaison complexe  $c$  n'appartenant pas à  $\mathbf{B} = \text{Gal}(\mathbf{H}_s(\mathbf{k})/\mathbf{H})$ , alors  $\mathbf{H}$  est totalement imaginaire. Finalement, puisqu'un corps totalement imaginaire galoisien est à multiplication complexe si et seulement la conjugaison complexe est dans le centre de son groupe de Galois, alors  $c$  est dans le centre de  $\text{Gal}(\mathbf{H}_s(\mathbf{k})/\mathbb{Q})$ , donc dans le centre de  $\text{Gal}(\mathbf{H}/\mathbb{Q})$  et  $\mathbf{H}$  est à multiplication complexe. D'après la Proposition 6,  $\mathbf{H}$  est de nombre de classes relatif égal à 1, donc impair, et de nombre de classes pair (égal à l'ordre de  $\mathbf{B}$ ). Cela ne saurait se produire d'après la Proposition 7. ■

**PROPOSITION 9.** *Soit  $\mathbf{H}$  un corps à multiplication complexe, diédral de degré  $8n \geq 8$  une puissance de 2 et cyclique sur un sous-corps quadratique  $\mathbf{k}$ . Si  $\mathbf{H}$  est de nombre de classes relatif impair, alors  $\mathbf{H}$  est de nombre de*

classes impair,  $\mathbf{H} = \mathbf{H}_{s,2}(\mathbf{k})$  est le 2-corps de classes de Hilbert au sens restreint de  $\mathbf{k}$ , et  $\mathbf{k}$  est un corps quadratique réel d'unité fondamentale de norme valant  $+1$  et à 2-groupe des classes au sens restreint cyclique d'ordre  $4n$ , de sorte qu'il existe deux nombres premiers distincts  $p < q$  non congrus à 3 modulo 4 vérifiant  $(p/q) = +1$  et tels que  $\mathbf{k} = \mathbb{Q}(\sqrt{pq})$ .

Preuve. Montrons que  $\mathbf{H}/\mathbf{H}^+$  est non ramifiée aux places finies. En effet, puisque  $w_{\mathbf{H}} = 2$  et  $Q_{\mathbf{H}} = 2$  (voir Proposition 7), il existe une unité  $\varepsilon \in \mathbf{U}_{\mathbf{H}}$  telle que  $\bar{\varepsilon}/\varepsilon = -1$ . Si  $\mathbf{H}/\mathbf{H}^+$  était ramifiée en  $\mathbf{P}$  un idéal premier de  $\mathbf{H}$ , alors la classe dans  $H_{\mathbf{H}}$  de l'idéal  $\mathbf{P}$  ne serait pas dans  $j_{\mathbf{H}/\mathbf{H}^+}(H_{\mathbf{H}^+})$  et d'après le Lemme A, 2 diviserait  $h_{\mathbf{H}}^-$ . Sinon, nous aurions l'existence d'un  $\alpha \in \mathbf{H}$  et d'un idéal  $\mathbf{I}^+$  de  $\mathbf{H}^+$  tels que  $\mathbf{P} = (\alpha)j_{\mathbf{H}/\mathbf{H}^+}(\mathbf{I}^+)$ . Nous aurions alors  $(\bar{\alpha}) = (\alpha)$ , de sorte qu'il existerait une racine de l'unité  $\zeta = \pm 1$  de  $\mathbf{H}$  telle que  $\bar{\alpha} = \zeta\alpha$ . Si nous avons  $\zeta = 1$ , alors  $\alpha$  serait dans  $\mathbf{H}^+$  et l'exposant de  $\mathbf{P}$  dans la décomposition en produit d'idéaux premiers de  $(\alpha)j_{\mathbf{H}/\mathbf{H}^+}(\mathbf{I}^+) = \mathbf{P}$  serait pair, ce qui n'est pas possible. Si nous avons  $\zeta = -1$ , alors en posant  $\beta = \varepsilon\alpha$  nous aurions  $\mathbf{P} = (\beta)j_{\mathbf{H}/\mathbf{H}^+}(\mathbf{I}^+)$  et  $\beta \in \mathbf{H}^+$ , qui comme précédemment est impossible.

Puisque  $\mathbf{H}/\mathbf{H}^+$  est non ramifiée aux places finies et puisque  $\mathbf{H}/\mathbf{k}$  est cyclique de degré une puissance de 2, alors  $\mathbf{H}/\mathbf{k}$  est non ramifiée aux places finies.

Puisque  $Q_{\mathbf{H}} = 2$  et puisque  $h_{\mathbf{H}}^-$  est impair, alors  $h_{\mathbf{H}}$  est impair (voir Lemme A). Il en résulte que  $\mathbf{H}$  contient le corps des genres  $\mathbf{G}_{\mathbf{k}}$  de  $\mathbf{k}$  (car  $\mathbf{G}_{\mathbf{k}}/\mathbf{k}$  étant abélienne, de degré une puissance de 2 et non ramifiée aux places finies, alors  $\mathbf{H}\mathbf{G}_{\mathbf{k}}/\mathbf{H}$  est abélienne, de degré une puissance de 2 et non ramifiée en toutes places. Puisque  $h_{\mathbf{H}}$  est impair, nous avons donc  $\mathbf{H}\mathbf{G}_{\mathbf{k}} \subseteq \mathbf{H}$ , soit  $\mathbf{G}_{\mathbf{k}} \subseteq \mathbf{H}$ ). Puisque  $\mathbf{H}$  est à multiplication complexe et diédral sur  $\mathbb{Q}$ , il contient précisément trois sous-corps quadratiques, tous trois réels, de sorte qu'il existe deux nombres premiers distincts  $p$  et  $q$  non congrus à 3 modulo 4 tels que  $\mathbf{G}_{\mathbf{k}} = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ . D'où  $\mathbf{k} = \mathbb{Q}(\sqrt{pq})$ .

Le 2-rang du groupe des classes aux sens restreint et large d'un tel  $\mathbb{Q}(\sqrt{pq})$  est égal à 1, c'est-à-dire que ses 2-Sylow au sens large et restreint sont cycliques. En particulier,  $\mathbf{H}_{s,2}(\mathbf{k})/\mathbf{k}$  est cyclique. De plus, son 2-Sylow au sens restreint étant d'ordre  $\geq [\mathbf{H} : \mathbf{k}] = 4n \geq 4$ , celui des deux idéaux premiers ramifiés  $\mathbf{P}$  ou  $\mathbf{Q}$  au dessus de  $p$  ou de  $q$  qui engendre une classe restreinte d'ordre 2 est un carré dans ce 2-Sylow au sens restreint, de sorte que  $\mathbf{P}$  ou  $\mathbf{Q}$  est dans le genre principal. Cela implique que le symbole de Legendre  $(p/q)$  vaut bien  $+1$  (les résultats de [D-P] sur les conditions nécessaires et suffisantes de plongement d'un corps réel biquadratique bicyclique dans un corps diédral donne également  $(p/q) = +1$ ).

Puisque  $\mathbf{H}/\mathbf{k}$  est cyclique de degré une puissance de 2 et non ramifiée aux places finies,  $\mathbf{H}$  est inclus dans  $\mathbf{H}_{s,2}(\mathbf{k})$ . Si c'en était un sous-corps propre, alors  $\mathbf{H}_{s,2}(\mathbf{k})/\mathbf{k}$  étant cyclique,  $\mathbf{H}$  serait un sous-corps de  $\mathbf{H}_{l,2}(\mathbf{k})$ ,

donc serait totalement réel, et ne saurait donc être un corps à multiplication complexe. D'où  $\mathbf{H} = \mathbf{H}_{s,2}(\mathbf{k})$ . ■

**4. Caractérisation des corps à multiplication complexe diédraux de degré une puissance de 2 et à nombres de classes relatifs impairs.** Nous complétons l'énoncé de la Proposition 9.

**THÉOREME 10.** *Soit  $\mathbf{H}$  un corps galoisien diédral de degré  $\geq 8$  et une puissance de 2. Soit  $\mathbf{k}$  le seul sous-corps quadratique de  $\mathbf{H}$  sur lequel  $\mathbf{H}$  est cyclique. Alors,  $\mathbf{H}$  est un corps à multiplication complexe de nombre de classes relatif impair si et seulement si  $\mathbf{H}$  est le 2-corps de classes de Hilbert au sens restreint de  $\mathbf{k}$  et  $\mathbf{k}$  est un corps quadratique réel d'unité fondamentale de norme +1 et à 2-groupe des classes au sens restreint cyclique. Il existe donc  $p$  et  $q$  premiers distincts non congrus à 3 modulo 4 vérifiant  $(p/q) = +1$  et tels que  $\mathbf{k} = \mathbb{Q}(\sqrt{pq})$ . De plus,  $Q_{\mathbf{H}} = 2$ ,  $h_{\mathbf{H}}^-$  est un carré et  $h_{\mathbf{H}}$  est impair.*

Un sens en est prouvé à la Proposition 9. La réciproque résulte du Corollaire 12 ci-dessous et du Théorème 5.

**PROPOSITION 11** (voir [C-C]). *Soient  $p$  un nombre premier et  $\mathbf{K}/\mathbf{L}$  une extension cyclique de degré  $p$  qui soit de plus non ramifiée en toutes places (finies et infinies). Supposons le  $p$ -Sylow du groupe des classes de  $\mathbf{L}$  cyclique d'ordre  $p^n$ . Alors, le  $p$ -Sylow du groupe des classes de  $\mathbf{K}$  est cyclique d'ordre  $p^{n-1}$  et le morphisme canonique  $j_{\mathbf{K}/\mathbf{L}}$  du groupe des idéaux fractionnaires de  $\mathbf{L}$  dans celui de  $\mathbf{K}$  est surjectif de noyau de cardinal  $p$ . De plus, pour  $p = 2$  ce résultat est conservé pour  $\mathbf{K}/\mathbf{L}$  non ramifiée en toute place finie pourvu que l'on parle de groupe de classes au sens restreint.*

*Preuve.* Soient  $\mathbf{H}_{\mathbf{K}}$  et  $\mathbf{H}_{\mathbf{L}}$  les  $p$ -corps de classes de Hilbert de  $\mathbf{K}$  et  $\mathbf{L}$ . Puisque  $\mathbf{K}/\mathbf{L}$  est abélienne non ramifiée en toutes places, alors  $\mathbf{H}_{\mathbf{K}}$  contient  $\mathbf{H}_{\mathbf{L}}$ . De plus, nous remarquons que l'extension  $\mathbf{K}/\mathbf{L}$  étant galoisienne, alors il en est de même de  $\mathbf{H}_{\mathbf{K}}/\mathbf{L}$ . Nous avons le diagramme suivant de corps :

$$\mathbf{H}_{\mathbf{K}} \text{ — } \mathbf{H}_{\mathbf{L}} \text{ — } \mathbf{K} \text{ — } \mathbf{L}.$$

Supposons que  $\mathbf{G} = \text{Gal}(\mathbf{H}_{\mathbf{K}}/\mathbf{L})$  qui est un  $p$ -groupe ne soit pas cyclique. D'après le théorème de la base de Burnside (voir [Hal, p. 176]), il existe un sous-groupe normal  $\mathbf{A}$  de  $\mathbf{G}$  tel que  $\mathbf{G}/\mathbf{A}$  soit  $p$ -élémentaire de rang  $\geq 2$ , donc ne soit pas cyclique. Considérons  $\mathbf{M}$  donné par la correspondance de Galois tel que  $\mathbf{L} \subseteq \mathbf{M} \subseteq \mathbf{H}_{\mathbf{K}}$  et tel que  $\text{Gal}(\mathbf{H}_{\mathbf{K}}/\mathbf{M}) = \mathbf{A}$ . Alors  $\mathbf{M}/\mathbf{L}$  est abélienne, non cyclique et non ramifiée. Contradiction. Donc  $\mathbf{G}$  est cyclique. Mais alors,  $\mathbf{H}_{\mathbf{K}}/\mathbf{L}$  étant une extension abélienne non ramifiée, nous avons  $\mathbf{H}_{\mathbf{K}} \subseteq \mathbf{H}_{\mathbf{L}}$ , puis  $\mathbf{H}_{\mathbf{K}} = \mathbf{H}_{\mathbf{L}}$  et  $\mathbf{H}_{\mathbf{K}}/\mathbf{K} = \mathbf{H}_{\mathbf{L}}/\mathbf{K}$  est cyclique de degré  $p^{n-1}$ . D'où la première partie de cette Proposition 11. Le reste en est prouvé dans [C-C, p. 369]. ■

**COROLLAIRE 12.** *Soit  $\mathbf{k}$  un corps quadratique réel d'unité fondamentale de norme valant  $+1$  et à 2-Sylow du groupe des classes au sens restreint cyclique. Le 2-corps de classes de Hilbert  $H_{l,2}(\mathbf{k})$  de  $\mathbf{k}$  et le 2-corps de classes de Hilbert au sens restreint  $H_{s,2}(\mathbf{k})$  de  $\mathbf{k}$  sont alors tous deux de nombres de classes impairs.*

**Remarque.** Ces résultats peuvent tomber en défaut lorsque le  $p$ -Sylow du groupe des classes de  $\mathbf{L}$  n'est pas supposé cyclique. Par exemple, on peut facilement construire des extensions quadratiques  $\mathbf{K}/\mathbf{L}$  non ramifiées en toutes places telles que si  $2^n$  est la plus grande puissance de 2 divisant le nombre de classes de  $\mathbf{L}$ , alors  $2^n$  divise le nombre de classes de  $\mathbf{K}$ . En effet, soit  $q \equiv 3 \pmod{4}$  premier et soient  $p_i \equiv 1 \pmod{4}$ ,  $1 \leq i \leq n$ , des nombres premiers deux à deux distincts. Posons  $d = qp_1 \dots p_n$ , puis  $\mathbf{L} = \mathbb{Q}(\sqrt{d})$  et  $\mathbf{K} = \mathbb{Q}(i, \sqrt{d})$ . Alors, le 2-rang du groupe des classes de  $\mathbf{L}$  vaut  $n$  alors que d'après [Lou 1, Corollaire 10(a)] celui du groupe des classes de  $\mathbf{K}$  vaut  $2n - 1$  si un des  $p_i$  est congru à 5 modulo 8 et vaut  $2n$  sinon (et ce parce que  $2n + 1$  idéaux premiers de  $\mathbb{Q}(i)$  sont ramifiés dans l'extension quadratique  $\mathbf{K}/\mathbb{Q}(i)$ ). En conséquence, pour  $n \geq 1$  on aura bien un contre-exemple pourvu que le 2-Sylow du groupe des classes de  $\mathbf{L}$  soit réduit à ses classes d'ordre 2, i.e. soit d'exposant  $\leq 2$ . Par exemple, le choix  $d = 15$  donne  $h_{\mathbf{L}} = h_{\mathbf{K}} = 2$ .

**5. Détermination des corps quadratiques réels dont les corps de classes de Hilbert au sens restreint sont à multiplication complexe, non abéliens et principaux.** Nous avons développé dans [Lou 2] une approche rigoureuse, car inconditionnelle, du calcul des nombres de classes relatifs des corps à multiplication complexe. Malheureusement, les techniques de minorations de discriminants développées par Odlyzko (voir [Odl 2]) ne nous ont pas permis de prouver la principalité de tous les sous-corps totalement réels maximaux des corps à multiplication complexe de nombres de classes relatifs égaux à 1 que nous aurons à considérer. Nous donnerons donc une approche numérique du calcul des nombres de classes de  $\mathbf{H}_l(\mathbf{k})$  et  $\mathbf{H}_s(\mathbf{k})$ . Notons que cette approche est non rigoureuse puisque le calcul d'un nombre de classes avec le logiciel Pari/GP n'est garanti que sous l'assomption de l'hypothèse de Riemann généralisée (voir [Coh, p. 348]). De toutes manières, notre détermination reposant sur une conjecture non encore prouvée (voir ci-dessous), il sera toujours temps d'essayer de se passer de l'utilisation de Pari/GP lorsqu'elle sera prouvée.

**5A. Détermination pour  $\mathbf{k}$  quadratique réel des  $\mathbf{H}_s(\mathbf{k})$  à multiplication complexe, non abéliens, principaux et pour lesquels  $\mathbf{G}_{\mathbf{k}}$  est imaginaire.**

**THÉOREME 13.** *Soit  $\mathbf{H}_s(\mathbf{k})$  le corps de classes de Hilbert au sens restreint d'un corps quadratique réel  $\mathbf{k}$  à corps des genres  $\mathbf{G}_{\mathbf{k}}$  imaginaire. Alors,  $\mathbf{H}_s(\mathbf{k})$  est un corps à multiplication complexe non abélien et principal si et*

seulement si  $\mathbf{k} = \mathbb{Q}(\sqrt{pq})$  avec  $pq \in \{7 \cdot 67, 11 \cdot 43, 2 \cdot 163\}$ , auxquels cas  $\mathbf{H}_s(\mathbf{k})$  est diédral de degré 12, ou  $\mathbf{k} = \mathbb{Q}(\sqrt{19 \cdot 43})$ , auquel cas  $\mathbf{H}_s(\mathbf{k})$  est diédral de degré 20.

*Preuve.* Soient  $\mathbf{k} = \mathbb{Q}(\sqrt{pq})$  avec  $p$  et  $q$  premiers distincts non congrus à 1 modulo 4,  $\mathbf{M} = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ , et  $\mathbf{K}$  un corps de nombres de degré premier  $l \geq 3$  de clôture galoisienne  $\mathbf{H}^+$  un corps diédral totalement réel de degré  $2l$ , et tel que  $d_{\mathbf{K}} = d_{\mathbf{k}}^{(l-1)/2}$ . Alors,  $\mathbf{H}^+/\mathbb{Q}$  étant diédrale, nous avons  $d_{\mathbf{H}^+} = d_{\mathbf{k}} d_{\mathbf{K}}^2 = d_{\mathbf{k}}^l$ . L'extension  $\mathbf{H}^+/\mathbf{k}$  est donc non ramifiée. De plus,  $\mathbf{H} = \mathbf{KM}$  est clairement diédral sur  $\mathbb{Q}$ , de degré  $4l$ , à multiplication complexe, et non ramifié sur  $\mathbf{k}$ . En particulier, si  $\mathbf{k}$  est de nombre de classes restreintes égal à  $2l$ , alors  $\mathbf{H} = \mathbf{H}_s(\mathbf{k})$ . Or, d'après [Coh, Appendix B4], les trois corps engendrés respectivement par une racine des polynômes  $X^3 + X^2 - 5X - 4$ , et  $X^3 - 5X - 1$  et  $X^3 - X^2 - 11X - 1$  sont respectivement de discriminants  $469 = 7 \cdot 67$ , et  $473 = 11 \cdot 43$  et  $1304 = 8 \cdot 163$ , et à clôtures galoisiennes des corps sextiques diédraux. On peut donc aisément construire un polynôme de degré 12 dont les racines engendrent  $\mathbf{H}_s(\mathbf{k})$ . Par utilisation du système de calcul pour la théorie des nombres Pari/GP, on montrerait que ces trois corps de classes de Hilbert sont de nombre de classes égaux à 1. En fait, en raisonnant de manière identique à celle du cas suivant, il suffit d'utiliser ce logiciel avec des corps de degré 6, ce qui est nettement plus efficace. En effet, soit  $\mathbf{K}$  le corps de degré 5 engendré par une racine du polynôme  $X^5 + X^4 - 6X^3 - 5X^2 + 3X + 1$ . D'après [S-P-D, Table 2] ce corps  $\mathbf{K}$  est de discriminant  $d_{\mathbf{K}} = 19^2 \cdot 43^2$  et à clôture galoisienne un corps totalement réel, diédral de degré 10. Ici encore on montre aisément que  $\mathbf{H}_s(\mathbf{k}) = \mathbf{KM}$  et par utilisation de Pari/GP que ce corps de classes de Hilbert est de nombre de classes égal à 1. Plus précisément, ce corps étant de degré 20 relativement élevé, nous remarquons que  $\mathbf{KM}/\mathbf{K}$  est biquadratique bicyclique de sous extensions quadratiques  $\mathbf{K}(\sqrt{-19})/\mathbf{K}$ ,  $\mathbf{K}(\sqrt{-43})/\mathbf{K}$  et  $\mathbf{K}(\sqrt{19 \cdot 43})/\mathbf{K}$ . En conséquence, si  $p$  premier impair divise le nombre de classes de  $\mathbf{H}_s(\mathbf{k}) = \mathbf{KM}$  alors d'après [M-M, Lemma 9] il divise le nombre de classes d'un des trois corps de degré 10 suivants :  $\mathbf{K}(\sqrt{-19})$ ,  $\mathbf{K}(\sqrt{-43})$  et  $\mathbf{K}(\sqrt{19 \cdot 43}) = \mathbf{H}_l(\mathbf{k})$ . Par utilisation du logiciel Pari/GP on obtient aisément qu'ils sont tous trois principaux. Il en résulte que  $\mathbf{KM} = \mathbf{H}_s(\mathbf{k})$  est de nombre de classes une puissance de 2. Puisque ce nombre de classes est impair (Théorème 10), il est égal à 1. ■

**5B.** *Détermination pour  $\mathbf{k}$  quadratique réel des  $\mathbf{H}_s(\mathbf{k})$  à multiplication complexe, non abéliens, principaux et pour lesquels  $\mathbf{G}_{\mathbf{k}}$  est réel.* Dans ce cas,  $\mathbf{H}_s(\mathbf{k})$  est une extension de degré  $h \geq 1$  impair de  $\mathbf{H}_{s,2}(\mathbf{k})$ , et  $\mathbf{H}_{s,2}(\mathbf{k})$  est diédral de degré  $2^n \geq 8$ , à multiplication complexe de nombre de classes relatif égal à 1 et de nombre de classes  $h \geq 1$ . Nous verrons ci-dessous que lorsque  $\mathbf{H}_{s,2}(\mathbf{k})$  est diédral de degré une puissance de 2 et de nombre de classes relatif égal à 1, alors il est de degré  $\leq 128$ . Nous déterminons donc

les  $\mathbf{H}_s(\mathbf{k})$  principaux en les cherchant à  $\mathbf{H}_{s,2}(\mathbf{k})$  de degré une puissance de 2 croissante.

Supposons premièrement  $\mathbf{H}_{s,2}(\mathbf{k})$  de degré 8. Nous savons (voir [Lou-Oka]) qu'il y a exactement 19 corps diédraux de degré 8 et de nombres de classes relatifs égaux à 1, et 17 d'entre eux sont de nombres de classes égaux à 1, les deux autres associés à  $\mathbb{Q}(\sqrt{5 \cdot 269})$  et  $\mathbb{Q}(\sqrt{17 \cdot 257})$  étant de nombres de classes égaux à 3. Si  $\mathbf{k} = \mathbb{Q}(\sqrt{17 \cdot 257})$  qui est de nombre de classes restreintes égal à 4, alors  $\mathbf{H}_s(\mathbf{k}) = \mathbf{H}_{s,2}(\mathbf{k})$  sont diédraux de degré 8, de nombres de classes relatifs égaux à 1 et de nombre de classes égaux à 3 (voir [Lou-Oka, p. 61]).

**THÉORÈME 14.** *Soit  $\mathbf{H}_s(\mathbf{k})$  le corps de classes de Hilbert au sens restreint d'un corps quadratique réel  $\mathbf{k}$ . Alors,  $\mathbf{H}_s(\mathbf{k})$  est un corps à multiplication complexe non-abélien, principal et de degré  $8h$  avec  $h$  impair si et seulement si  $\mathbf{k}$  est l'un des 17 corps  $\mathbb{Q}(\sqrt{pq})$  avec  $pq \in \{2 \cdot 17, 2 \cdot 73, 2 \cdot 89, 2 \cdot 233, 2 \cdot 281, 5 \cdot 41, 5 \cdot 61, 5 \cdot 109, 5 \cdot 149, 5 \cdot 389, 13 \cdot 17, 13 \cdot 29, 13 \cdot 157, 13 \cdot 181, 17 \cdot 137, 29 \cdot 53, 73 \cdot 97\}$ , auxquels cas  $\mathbf{H}_s(\mathbf{k})$  est diédral de degré 8, où  $\mathbf{k} = \mathbb{Q}(\sqrt{5 \cdot 269})$ , auquel cas  $\mathbf{H}_s(\mathbf{k})$  est diédral de degré 24.*

*Preuve.* Reste à expliquer la construction de  $\mathbf{H}_s(\mathbf{k})$  pour  $\mathbf{k} = \mathbb{Q}(\sqrt{5 \cdot 269})$  de nombre de classes restreintes égal à 12 et tel que  $\mathbf{H}_{s,2}(\mathbf{k})$  est de nombre de classes relatif égal à 1 et de nombre de classes  $h = 3$  impair, c'est-à-dire à en donner un polynôme dont ce soit le corps de décomposition, ce qui nous permet d'utiliser Pari/GP. Pour cela, nous remarquons que toute racine du polynôme  $X^3 - 7X - 1$  engendre un corps cubique  $\mathbf{K}$  de discriminant  $d_{\mathbf{K}} = 1345 = 5 \cdot 269 = d_{\mathbf{k}}$  de clôture galoisienne  $\mathbf{N}$  un corps sextique diédral totalement réel donc non ramifié sur  $\mathbf{k}$  (même raisonnement que pour la preuve du Théorème 13). Il en résulte aisément que  $\mathbf{H}_l(\mathbf{k}) = \mathbf{K}(\sqrt{5}, \sqrt{269})$  et  $\mathbf{H}_s(\mathbf{k}) = \mathbf{K}\mathbf{H}_{s,2}(\mathbf{k})$ . Par utilisation de Pari/GP on obtient que  $\mathbf{H}_l(\mathbf{k})$  est principal. Pour  $\mathbf{H}_s(\mathbf{k})$  qui est de degré 24, le calcul de son nombre de classes avec Pari/GP étant trop difficile, nous calculons le nombre de classes du corps à multiplication complexe

$$\mathbf{N} = \mathbf{K} \left( \sqrt{-\frac{17 + \sqrt{269}}{2}} \right)$$

de degré 12, nombre de classes qui s'avère valoir 1, donc de nombre de classes relatif égal à 1. Nous remarquons ensuite que avec les notations de la preuve de la Proposition 7 ce corps est un des  $\mathbf{K}_i$ . Il résulte alors de (5) que  $\mathbf{H}_s(\mathbf{k})$  est de nombre de classes relatif égal à 1, donc de nombre de classes égal à 1. ■

Supposons deuxièmement  $\mathbf{H}_{s,2}(\mathbf{k})$  de degré 16. Nous connaissons (voir [Lou 2]) au moins cinq corps à multiplication complexe, diédraux, de degré 16 et de nombres de classes relatifs égaux à 1 : les 2-corps de classes de Hilbert



au sens restreint des  $\mathbb{Q}(\sqrt{pq})$  avec  $pq \in \{5 \cdot 101, 2 \cdot 257, 13 \cdot 53, 13 \cdot 61, 5 \cdot 181\}$ . Notons que ces cinq corps quadratiques réels sont principaux, donc que  $\mathbf{H}_{s,2}(\mathbf{k}) = \mathbf{H}_s(\mathbf{k})$  dans ces cinq cas. Puisque le corps quadratique réel  $\mathbb{Q}(\sqrt{257})$  est de nombre de classes égal à 3, alors pour  $\mathbf{k} = \mathbb{Q}(\sqrt{2 \cdot 257})$  les corps  $\mathbf{H}_{s,2}(\mathbf{k})$  et  $\mathbf{H}_s(\mathbf{k})$  qui sont de nombre de classes divisible par 3 ne sont donc pas principaux.

**THÉORÈME 15.** *Si  $\mathbf{k} = \mathbb{Q}(\sqrt{pq})$  avec  $pq \in \{5 \cdot 101, 5 \cdot 181, 13 \cdot 53, 13 \cdot 61\}$ , alors  $\mathbf{H}_s(\mathbf{k})$  est un corps à multiplication complexe non-abélien, diédral, principal et de degré 16.*

*Preuve.* Nous savons que ces 4 corps de classes de Hilbert sont de nombres de classes relatifs égaux à 1. Il reste à montrer que leurs sous-corps totalement réels maximaux  $\mathbf{H}_{l,2}(\mathbf{k})$  (qui sont diédraux de degré 8) sont principaux. Pour cela, nous remarquons que les équations  $x^2 - py^2 = 4q$  ont des solutions  $x \geq 1$  et  $y \geq 1$ , et que nous avons alors

$$\mathbf{H}_l(\mathbf{k}) = \mathbb{Q}\left(\sqrt{q}, \sqrt{\frac{x + y\sqrt{p}}{2}}\right).$$

Par exemple, pour  $\mathbf{k} = \mathbb{Q}(\sqrt{5 \cdot 181})$  nous avons  $\mathbf{H}_l(\mathbf{k}) = \mathbb{Q}(\sqrt{181}, \sqrt{(27 + \sqrt{5})/2})$ . Noter que le polynôme  $P(X) = X^4 - xX^2 + q$  est générateur du corps quartique  $\mathbb{Q}(\sqrt{(x + y\sqrt{p})/2})$ , de sorte que

$$Q(X) = P\left(X - \frac{1 + \sqrt{q}}{2}\right)P\left(X - \frac{1 - \sqrt{q}}{2}\right)$$

est générateur de  $\mathbf{H}_l(\mathbf{k})$ . Le calcul des nombres de classes de ces corps avec Pari/GP montrent qu'ils valent 1. ■

**5C. Conclusion.** Les Théorèmes 13, 14 et 15 nous donnent 26 corps quadratiques réels  $\mathbf{k} = \mathbb{Q}(\sqrt{pq})$  dont les corps de classes de Hilbert au sens restreint  $\mathbf{H}_s(\mathbf{k})$  sont à multiplication complexe, non abéliens et principaux, à savoir ceux donnés à la Table 3 suivante, où nous avons posé  $n_{pq} = [\mathbf{H}_s(\mathbf{k}) : \mathbb{Q}] = 4h_{\mathbf{k}}$ .

Table 3

$(p, q)$	$n_{pq}$	$(p, q)$	$n_{pq}$	$(p, q)$	$n_{pq}$
(2, 17)	8	(5, 389)	8	(2, 163)	12
(2, 73)	8	(13, 17)	8	(7, 67)	12
(2, 89)	8	(13, 29)	8	(11, 43)	12
(2, 233)	8	(13, 157)	8	(5, 101)	16
(2, 281)	8	(13, 181)	8	(5, 181)	16
(5, 41)	8	(17, 137)	8	(13, 53)	16
(5, 61)	8	(29, 53)	8	(13, 61)	16
(5, 109)	8	(73, 97)	8	(19, 43)	20
(5, 149)	8			(5, 269)	24

En vertu du Théorème 10, la conjecture que nous faisons dans [Lou 2] peut être reformulée de la manière suivante :

CONJECTURE. *Il n'existe pas de corps à multiplication complexe, diédral de degré  $2n \geq 32$  une puissance de 2 et de nombre de classes relatif égal à 1. Il existe précisément 5 corps à multiplication complexe, diédraux de degré  $2n = 16$  et de nombres de classes relatifs égaux à 1* <sup>(1)</sup>.

D'après la Proposition 6, le Théorème 8 et les résultats des paragraphes 5A et 5B, il est clair que sous l'assomption de la conjecture précédente il existe précisément 26 corps quadratiques réels dont les corps de classes de Hilbert au sens restreint sont à multiplication complexe, non abéliens et principaux : ceux donnés à la Table 3. Nous concluons cet article en expliquant pourquoi cette conjecture est raisonnable.

THÉORÈME 16. *Le nombre de classes relatif  $h_{\mathbf{H}}^-$  de tout corps  $\mathbf{H}$  à multiplication complexe, diédral de degré  $2n \geq 256$  une puissance de 2 vérifie  $h_{\mathbf{H}}^- > 1$*

Preuve. D'après [Hof, Table p. 47], si  $\mathbf{H}$  est de degré  $2n \geq 256$  et de nombre de classes relatif égal à 1, alors  $d_{\mathbf{H}^+}^{1/n} = \sqrt{d_{\mathbf{k}}} \leq 115$ , soit  $d_{\mathbf{k}} \leq 13225$ . Maintenant,  $\mathbf{H} = \mathbf{H}_{s,2}(\mathbf{k})$  où  $\mathbf{k} = \mathbb{Q}(\sqrt{pq})$  est un corps quadratique réel d'unité fondamentale de norme +1, à 2-Sylow de groupe des classes au sens restreint cyclique et de nombre de classes au sens large  $h_{\mathbf{k}}$  divisible par 64 (voir Proposition 9). D'où  $d_{\mathbf{k}} \geq 268361$  (voir ci-dessous). Contradiction. ■

Plus précisément, la Table 4 suivante donne pour chaque puissance  $2^m \in \{8, 16, 32, 64\}$  les plus petites valeurs de  $d = pq$  avec  $2 \leq p < q$  non congrus à 3 modulo 4 tels que la norme de l'unité fondamentale de  $\mathbf{k} = \mathbb{Q}(\sqrt{pq})$  soit égale à +1, et tels que la plus grande puissance de 2 qui divise  $h_{\mathbf{k}}$  soit  $2^m$  (voir [W-B] pour la méthode de calcul du nombre de classes des corps quadratiques réels que nous avons utilisée pour établir cette table).

Table 4

$d$	$2^m$	$h^-$	$d$	$2^m$	$d$	$2^m$	$d$	$2^m$
2434	8	$17^2$	28981	16	55906	32	268361	64
5186	8	$127^2$	38021	16	96994	32	412162	64
5249	8	$47^2$	39961	16	114469	32		
5513	8	$47^2$	46082	16	152113	32		

Dans cette Table 4 figurent également quelques nombres de classes relatifs  $h^-$  des  $\mathbf{H}_{s,2}(\mathbf{k})$  correspondants (ils sont de degré  $2^{m+2}$ ). Ces nombres

<sup>(1)</sup> Ajouté le 11 Novembre 1995: S. Louboutin et R. Okazaki viennent de montrer que cette conjecture est vraie.

de classes relatifs ont été calculés non rigoureusement en partant du produit infini de la fonction  $L$  apparaissant dans la formule (1) (noter que d'après la Proposition 7, on a  $Q_{\mathbf{H}} = w_{\mathbf{H}} = 2$  dans cette formule). On dispose du test de confiance assurant que ces nombres de classes relatifs doivent être des carrés et être impairs (Proposition 7). Les discriminants pour lesquels nous ne donnons pas de valeur pour  $h^-$  sont tels que le produit infini pour  $h^-$  en suggère une valeur très grande, trop grande pour que la lente convergence de ce produit infini puisse permettre de supputer une valeur exacte pour  $h^-$ .

Le Théorème 16, cette Table 4 et ces calculs montrent bien que la conjecture précédente est raisonnable.

### Références

- [Coh] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1994.
- [C-C] H. Cohn and G. Cooke, *Parametric form of an eight class field*, Acta Arith. 30 (1976), 367–377.
- [Cox] D. A. Cox, *Primes of the Form  $x^2 + ny^2$* , Wiley, 1989.
- [D-P] P. Damey et J. J. Payan, *Existence et construction des extensions galoisiennes et non abéliennes de degré 8 d'un corps de caractéristique différente de 2*, J. Reine Angew. Math. 244 (1970), 37–54.
- [Hal] M. Hall, *The Theory of Groups*, Chapter 12, Macmillan, New York, 1959.
- [Hof] J. Hoffstein, *Some analytic bounds for zeta functions and class numbers*, Invent. Math. 55 (1979), 37–47.
- [Lou 1] S. Louboutin, *Norme relative de l'unité fondamentale et 2-rang du groupe des classes d'idéaux de certains corps biquadratiques*, Acta Arith. 58 (1991), 273–288.
- [Lou 2] —, *Calcul des nombres de classes relatifs de certains corps de classes de Hilbert*, C. R. Acad. Sci. Paris 319 (1994), 321–325.
- [Lou 3] —, *Determination of all quaternion octic CM-fields with class number two*, J. London Math. Soc., to appear.
- [Lou-Oka] S. Louboutin and R. Okazaki, *Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one*, Acta Arith. 67 (1994), 47–62.
- [M-M] J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. 286/287 (1976), 248–256.
- [M-W] H. L. Montgomery and P. J. Weinberger, *Notes on small class numbers*, Acta Arith. 24 (1974), 529–542.
- [Odl 1] A. M. Odlyzko, *Some analytic estimates of class numbers and discriminants*, Invent. Math. 29 (1975), 275–286.
- [Odl 2] —, *On conductors and discriminants*, in: Algebraic Number Fields:  $L$ -functions and Galois Properties, Proc. Sympos., Univ. Durham, Durham 1975, Academic Press, London, 1977, 377–407.
- [S-P-D] A. Schwarz, M. Pohst and F. Diaz y Diaz, *A table of quintic number fields*, Math. Comp. 63 (1994), 361–376.
- [Sta 1] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. 14 (1967), 1–27.

- [Sta 2] H. M. Stark, *On complex quadratic fields with class-number two*, Math. Comp. 29 (1975), 289–302.
- [Uch 1] K. Uchida, *Imaginary abelian number fields with class number one*, Tôhoku Math. J. 24 (1972), 487–499.
- [Uch 2] —, *Imaginary abelian number fields of degrees  $2^m$  with class number one*, in: Class Numbers and Fundamental Units of Algebraic Number Fields, Proc. Internat. Conf. Katata/Jap., 1986, 151–170.
- [Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer, 1982.
- [W-B] H. C. Williams and J. Broere, *A computational technique for evaluating  $L(1, \chi)$  and the class number of a real quadratic field*, Math. Comp. 30 (1976), 887–893.
- [Yam] K. Yamamura, *The determination of the imaginary abelian number fields with class-number one*, *ibid.* 62 (1994), 899–921.

DÉPARTEMENT DE MATHÉMATIQUES  
UNIVERSITÉ DE CAEN, U.F.R. SCIENCES  
ESPLANADE DE LA PAIX  
14032 CAEN CEDEX, FRANCE  
E-mail: LOUBOUTI@MATH.UNICAEN.FR

*Reçu le 19.12.1994*

(2714)