

# ANNALES DE L'INSTITUT FOURIER

YANN LEFEUVRE

## Corps diédraux à multiplication complexe principaux

*Annales de l'institut Fourier*, tome 50, n° 1 (2000), p. 67-103

[http://www.numdam.org/item?id=AIF\\_2000\\_\\_50\\_1\\_67\\_0](http://www.numdam.org/item?id=AIF_2000__50_1_67_0)

© Annales de l'institut Fourier, 2000, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (<http://annalif.ujf-grenoble.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

# CORPS DIÉDRAUX À MULTIPLICATION COMPLEXE PRINCIPAUX

par Yann LEFEUVRE

---

## 1. Introduction.

Rappelons qu'un corps de nombres  $E$  est dit à multiplication complexe s'il est totalement imaginaire et est une extension quadratique de son sous-corps totalement réel maximal  $E^+$ . Dans cette situation, le nombre de classes d'idéaux  $h_{E^+}$  de  $E^+$  divise celui  $h_E$  de  $E$  et l'entier  $h_E^- = h_E/h_{E^+}$  est appelé le nombre de classes relatif de  $E$ . Notons que  $h_E^-$  divise  $h_E$  et que  $h_E = 1$  implique  $h_E^- = 1$ .

A.M. Odlyzko a montré qu'il n'existe qu'un nombre fini de corps galoisiens à multiplication complexe de nombre de classes un (voir [20]) et J. Hoffstein a prouvé que le degré d'un tel corps est inférieur ou égal à 436 (voir [6]). La question naturelle qui en découlait était de déterminer tous les corps galoisiens à multiplication complexe principaux.

Une réponse partielle à cette question a été apportée par K. Yamamura qui a déterminé tous les corps abéliens à multiplication complexe principaux : en particulier il n'existe pas de corps à multiplication complexe abélien principal de degré strictement supérieur à 24 (voir [24]). Le cas abélien est relativement simple car nous disposons d'une part d'une agréable et très maniable description de ces corps à l'aide de groupes de caractères de Dirichlet primitifs, et d'autre part d'une technique élémentaire de calcul de leurs nombres de classes relatifs à l'aide de nombres de Bernoulli généralisés (voir [23]).

---

*Mots-clés* : Corps à multiplication complexe – Corps diédraux – Nombre de classes – Nombre de classes relatif – Théorie du corps de classes.  
*Classification math.* : 11R29 – 11R37 – 11R21 – 11R42.

Dans cet article nous nous plaçons dans le premier cadre non abélien qui vienne à l'esprit et déterminons donc tous les corps à multiplication complexe galoisiens principaux à groupe de Galois n'importe quel groupe diédral. Nous obtenons le résultat principal de cet article, similaire à celui obtenu par K. Yamamura dans le cas abélien :

THÉORÈME 1.1. — *Il existe exactement 43 corps diédraux, non abéliens, à multiplication complexe de nombre de classes relatif un, et 32 d'entre eux sont de plus principaux, à savoir :*

- 1) 19 de degré 8 dont 17 sont principaux (voir [15]);
- 2) 16 de degré 12 dont 9 sont principaux (voir [17]);
- 3) 5 de degré 16 dont 4 sont principaux (voir [16]);
- 4) 2 de degré 20 dont 1 est principal;
- 5) 1 de degré 24 et il est principal.

*En particulier, il n'existe aucun corps diédral à multiplication complexe de nombre de classes relatif un de degré  $2^r \ell$  avec  $r \geq 5$  ou  $\ell \geq 7$  impair.*

Rappelons d'abord que pour  $E$  un corps de nombres à multiplication complexe de degré  $2n$ , et en notant respectivement  $\zeta_E, \zeta_{E^+}, d_E, d_{E^+}, Q_E \in \{1, 2\}$  et  $w_E$  les fonctions zêta de Dedekind de  $E$  et  $E^+$ , les valeurs absolues des discriminants de  $E$  et  $E^+$ , l'indice de Hasse de  $E$  et le nombre de racines de l'unité complexes contenues dans  $E$ , nous avons

$$(1) \quad h_E^- = \frac{Q_E w_E}{(2\pi)^n} \sqrt{\frac{d_E}{d_{E^+}} \frac{\text{Res}_{s=1}(\zeta_E)}{\text{Res}_{s=1}(\zeta_{E^+})}}.$$

Soit maintenant  $N$  un corps de nombres à multiplication complexe, galoisien et à groupe de Galois  $G = \text{Gal}(N/\mathbb{Q})$  un groupe diédral. La conjugaison complexe devant appartenir au centre  $Z(G)$  de  $G$  (voir [17]), ce centre doit contenir un élément d'ordre 2 et l'ordre de  $G$  doit donc être divisible par 4, soit  $[N : \mathbb{Q}] = 4m$  et

$$G = D_{4m} = \langle a, b : a^{2m} = b^2 = 1 \text{ et } b^{-1}ab = a^{-1} \rangle.$$

Alors  $Z(G) = \{1, a^m\}$  et la conjugaison complexe  $c$  est donc donnée par  $c = a^m$ . Le sous-corps totalement réel maximal  $N^+$  de  $N$  étant le sous-corps

de  $N$  fixé par  $\langle c \rangle$ , l'extension  $N^+/\mathbb{Q}$  est galoisienne et à groupe de Galois diédral d'ordre  $2m$ .

- Nous notons  $L$  l'unique sous-corps quadratique de  $N$  tel que  $N/L$  soit cyclique : c'est le sous-corps de  $N$  fixé par le sous-groupe cyclique d'ordre  $2m$  engendré par  $a$ , et  $L$  est donc réel.

- Nous notons  $2^r$  la plus grande puissance de 2 divisant le degré  $4m$  de  $N$  et définissons  $\ell \geq 1$  impair par

$$[N : \mathbb{Q}] = 4m = 2^r \ell.$$

- Nous notons  $M$  le sous-corps de  $N$  fixé par le groupe cyclique d'ordre  $\ell$  engendré par  $a^{2^{r-1}}$ . Il est facile de voir que  $M$  est un corps à multiplication complexe diédral de degré  $2^r$  de sous-corps totalement réel maximal noté  $M^+$  contenant  $L$ .

- Finalement, pour  $p$  un premier impair, si  $p^s$  divise  $\ell$  nous notons  $F_{p^s}$  le sous-corps de  $N$  fixé par le groupe cyclique d'ordre  $\ell/p^s$  engendré par  $a^{p^s}$ . L'extension  $F_{p^s}/\mathbb{Q}$  est alors galoisienne, diédrale de degré  $2p^s$  et  $F_{p^s}$  est réel.

Nous renvoyons le lecteur à la figure 1 où apparaît le diagramme de ces sous-corps, diagramme auquel nous nous référerons de manière répétée.

PROPOSITION 1.2 (voir [17], th. 5). — *Si  $E/F$  est une extension de degré impair de corps à multiplication complexe, alors  $h_F^-$  divise  $h_E^-$  et  $Q_E = Q_F$ .*

En conséquence,  $h_N = 1$  implique  $h_N^- = 1$ , qui implique  $h_M^- = h_{N_p}^- = h_{N_{p^s}}^- = 1$ . Notre détermination des corps à multiplication complexe  $N$  diédraux (non abéliens) de degré  $4m \geq 8$  et de nombre de classes relatif un va alors se décomposer en trois étapes :

1) Détermination préalable (à la proposition 3.3) de l'ensemble fini  $\mathcal{D}_2$  (à 171 éléments) des corps diédraux à multiplication complexe  $M$  de nombre de classes relatif un et de degré  $2^r \geq 4$  une puissance de 2 faite dans [15] et [16]. Il est très important de ne pas exclure de cette étape la détermination des corps à multiplication complexe diédraux abéliens de degré  $2^r = 4$  et de nombre de classes relatif un (il y en a 147).

2) Pour  $M \in \mathcal{D}_2$  fixé, détermination de tous les corps à multiplication complexe  $N_p$  diédraux de degré  $2^r p$  ( $p \geq 3$  premier quelconque) contenant  $M$  et de nombre de classes relatif un. D'où la détermination (au

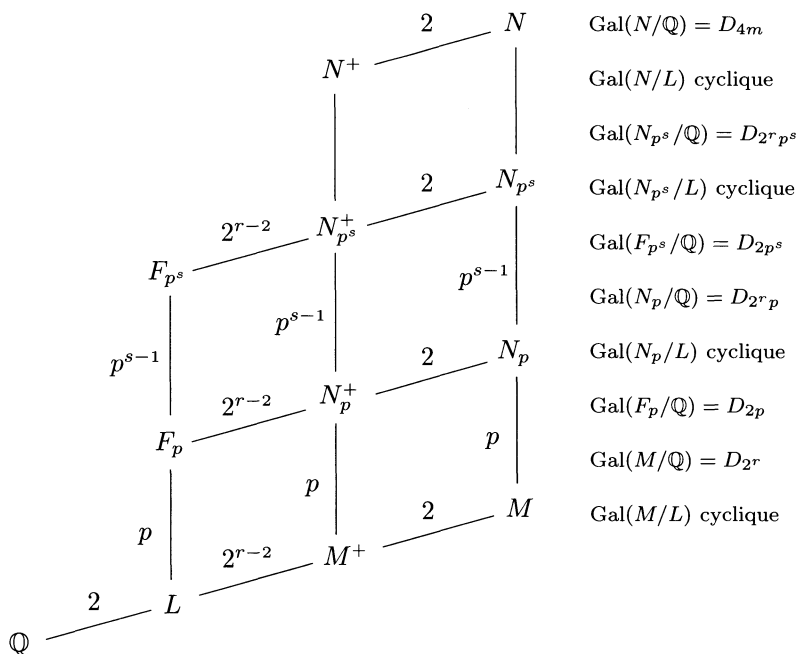


Figure 1

théorème 4.1) de l'ensemble  $\mathcal{D}_p$  des corps à multiplication complexe diédraux  $N_p$  de degré  $2^r p$  et de nombre de classes relatif un (il y en a 19). En particulier, nous trouvons que  $N_p$ , s'il existe, est entièrement déterminé par le choix de  $M \in \mathcal{D}_2$  (et même celui de  $L$ ), de sorte que si  $N$  est un corps à multiplication complexe diédral de nombre de classes relatif un alors il est de degré  $2^r p^s$ , avec  $p \in \{3, 5\}$ ,  $r \geq 2$  et  $s \geq 0$  (voir point 4) du théorème 4.1).

3) Finalement, pour  $N_p \in \mathcal{D}_p$  fixé de degré  $2^r p$ , utilisation de minoration sur  $h_{N_p}^-$  pour montrer (au théorème 5.2) que tout corps à multiplication complexe diédral  $N_{p^2}$  de degré  $2^r p^2$  contenant un  $N_p \in \mathcal{D}_p$  est de nombre de classes relatif strictement supérieur à un.

Donnons maintenant quelques indications sur le cheminement que nous allons suivre. La première étape est très importante : elle nous permet de travailler à  $M \in \mathcal{D}_2$  fixé, donc également à  $L$  fixé, ce qui aura deux conséquences. Nous observerons d'abord que  $\zeta_M$  est négative ou nulle sur l'intervalle  $]0, 1[$ . Cela nous permettra de montrer que, si  $N$  est tel que son

sous-corps  $M$  associé est dans  $\mathcal{D}_2$ , alors  $\zeta_N$  est également négative ou nulle sur l'intervalle  $]0, 1[$ , ce qui nous permettra de minorer le terme  $\text{Res}_{s=1}(\zeta_N)$  du numérateur de (1). En utilisant les techniques développées dans [9] et [12], nous majorerons ensuite le terme  $\text{Res}_{s=1}(\zeta_{N^+})$  du dénominateur de (1) en fonction de la norme du conducteur de l'extension cyclique  $N^+/L$  et de quantités ne dépendant que de  $L$ , quantités que nous pourrons précalculer pour chacun des 155 corps quadratiques réels  $L$  qui sont sous-corps d'un des 171 corps  $M \in \mathcal{D}_2$ . Nous obtiendrons ainsi de bonnes minoration de  $h_N^-$ , sous l'hypothèse que  $N$  varie parmi les corps à multiplication complexe diédraux dont le sous-corps  $M$  est dans  $\mathcal{D}_2$ . Ces minoration nous permettront de décomposer la deuxième étape en deux parties. Nous commencerons par montrer que si  $N_p$  est de nombre de classes relatif un alors  $p \leq 17$  (voir théorème 3.8). À  $M \in \mathcal{D}_2$  de degré  $2^r \geq 4$  et  $p$  fixés, nous déterminerons alors tous les  $N_p$  de degré  $2^r p$  contenant  $M$  et de nombre de classes relatif un : en utilisant nos minoration précédentes sur  $h_{N_p}^-$  nous construirons une liste de corps  $N_p$  contenant  $\mathcal{D}_p$  et nous en extrairons l'ensemble  $\mathcal{D}_p$  en calculant numériquement les nombres de classes relatifs de tous les corps  $N_p$  de cette liste.

Nous fixons une clôture algébrique du corps des rationnels, et considérons donc que tout corps de nombres est sous-corps du corps des nombres complexes. Pour tout corps de nombres  $E$  nous notons  $\mathcal{O}_E$  son anneau des entiers et  $d_E$  la valeur absolue de son discriminant. De plus,  $p$  désignera toujours un nombre premier impair et  $L$  un corps quadratique réel.

Cet article reprend les résultats principaux d'un travail de thèse effectuée sous la direction de S. Louboutin (voir [7]). Tous les calculs ont été effectués en utilisant le logiciel UBASIC du Pr. Y. Kida et les programmes sont disponibles sur simple demande.

## 2. Corps diédraux de degré $2p^s$ avec $p$ premier impair.

Que ce soit pour des questions de minoration de nombres de classes relatifs, pour des questions de calculs explicites de nombres de classes relatifs ou tout simplement pour de simples questions de présentation des résultats de notre détermination, il nous faut maintenant expliquer comment nous construisons tous les corps diédraux qui apparaissent à la figure 1. Nous commençons par remarquer que nous n'aurons que des  $N_{p^s}$  à

construire (voir point 4) du théorème 4.1), que ces  $N_{p^s}$  sont des composita  $N_{p^s} = F_{p^s}M$  et que les  $M$  que nous aurons à considérer seront (voir point 2) de la proposition 3.3) ou bien biquadratiques bicycliques donc faciles à construire, ou bien des 2-corps de classes de Hilbert au sens strict de corps quadratiques réels  $L$  à 2-Sylow de groupe de classes au sens strict cyclique, donc également relativement faciles à construire. La véritable question est donc, pour  $L$  et  $p^s$  donnés, de savoir construire les corps diédraux  $F_{p^s}$  cycliques de degré  $p^s$  sur  $L$ . Tel est l'objet de ce second paragraphe. Nous allons, par l'utilisation de la théorie du corps de classes, ramener la construction de ces  $F_{p^s}$  à celle de caractères primitifs sur des groupes de classes de rayon de  $L$  (théorème 2.1), puis ramener cette dernière construction à celle, plus facile, de caractères modulaires primitifs sur des groupes  $(\mathcal{O}_L/(f))^*$  pour  $f \geq 1$  entier (théorème 2.2). Pour  $L$  et  $p^s$  donnés, nous pourrons alors déterminer tous les corps diédraux réels  $F_{p^s}$  cycliques de degré  $p^s$  sur  $L$  et de conducteur donné.

### 2.1. Lien avec la théorie du corps de classes.

Dans tout cet article,  $L$  désigne un corps quadratique réel de discriminant  $d_L$  et d'unité fondamentale  $\varepsilon_L > 1$ . Notons  $\chi_L$  le caractère primitif, quadratique et de conducteur  $d_L$  associé à  $L$  et posons

$$\omega_L = \frac{1}{2}(d_L + \sqrt{d_L}),$$

de sorte que  $\mathcal{O}_L = \mathbb{Z} + \omega_L\mathbb{Z}$  est l'anneau des entiers de  $L$ .

Soit  $\mathcal{M}$  un idéal entier. Notons :

- $I_L(\mathcal{M})$  le sous-groupe des idéaux fractionnaires de  $L$  premiers à  $\mathcal{M}$  ;
- $P_{L,1}(\mathcal{M})$  le sous-groupe de  $I_L(\mathcal{M})$  engendré par les idéaux principaux  $\alpha\mathcal{O}_L$  pour lesquels  $\alpha \in \mathcal{O}_L$  vérifie  $\alpha \equiv 1 \pmod{\mathcal{M}}$  ;
- $\text{Cl}_L(\mathcal{M}) = I_L(\mathcal{M})/P_{L,1}(\mathcal{M})$ .

Selon la théorie du corps de classe, pour toute extension abélienne  $E/L$  dont le conducteur  $\mathcal{F}_{E/L}$  divise  $\mathcal{M}$ , le noyau  $H$  de la fonction surjective d'Artin

$$\Phi_{E/L} : I_L(\mathcal{M}) \longrightarrow \text{Gal}(E/L)$$

vérifie  $P_{L,1}(\mathcal{M}) \subseteq H \subseteq I_L(\mathcal{M})$ . En particulier il y a une correspondance bijective entre les groupes de caractères engendrés par un caractère primitif  $\chi$  d'ordre  $\ell$  sur le groupe  $\text{Cl}_L(\mathcal{M})$  des classes de rayon modulo  $\mathcal{M}$  et les extensions cycliques  $E/L$  de degré  $\ell$  et de conducteur  $\mathcal{M}$ .

• Si  $\chi$  est un caractère primitif d'ordre  $\ell$  sur  $\text{Cl}_L(\mathcal{M})$ , nous notons  $\chi_0$  le caractère modulaire associé sur  $(\mathcal{O}_L/\mathcal{M})^*$  défini par

$$\chi_0(\alpha) = \chi((\alpha)).$$

Ce caractère modulaire  $\chi_0$  est primitif, d'ordre divisant  $\ell$  (mais pas nécessairement d'ordre  $\ell$ ) et trivial sur l'unité fondamentale  $\varepsilon_L$ .

• Enfin, notons  $P_{L,\mathbb{Z}}(\mathcal{M})$  le sous-groupe de  $I_L(\mathcal{M})$  engendré par les idéaux principaux  $\alpha\mathcal{O}_L$  pour lesquels  $\alpha \in \mathcal{O}_L$  est tel qu'il existe un entier relatif  $a$  premier à  $\mathcal{M}$  vérifiant  $\alpha \equiv a \pmod{\mathcal{M}}$ .

**THÉORÈME 2.1.** — *Soient  $\ell$  un entier impair,  $p \geq 3$  un nombre premier impair,  $s$  un entier non nul,  $L$  un corps quadratique réel et  $F_\ell$  un corps diédral de degré  $2\ell$  cyclique sur  $L$ .*

1) *Le conducteur  $\mathcal{F}_{F_\ell/L}$  de l'extension cyclique  $F_\ell/L$  est invariant sous l'action de  $\text{Gal}(L/\mathbb{Q})$ ,  $\ker(\Phi_{F_\ell/L})$  contient  $P_{L,\mathbb{Z}}(\mathcal{F}_{F_\ell/L})$  et il existe un entier relatif  $f_\ell \geq 1$  tel que  $\mathcal{F}_{F_\ell/L} = f_\ell\mathcal{O}_L$ . Réciproquement (voir [18]), pour  $f \geq 1$  entier donné, nous avons une correspondance bijective entre d'une part les groupes de caractères engendrés par les caractères primitifs d'ordre  $\ell$  sur  $\text{Cl}_L((f))$  triviaux sur  $P_{L,\mathbb{Z}}((f))$  et d'autre part les corps diédraux réels  $F$  de degré  $2\ell$ , cycliques sur  $L$  et pour lesquels le conducteur  $\mathcal{F}_{F/L}$  est  $f\mathcal{O}_L$ .*

2) *Soit  $f \geq 1$  entier. Posons*

$$n_L(f) = \min\{k \geq 1; \exists a \in \mathbb{Z} \mid \varepsilon_L^k \equiv a \pmod{(f)}\}.$$

*Le groupe  $\text{Cl}_{L,\mathbb{Z}}((f)) = I_L((f))/P_{L,\mathbb{Z}}((f))$  est alors d'ordre*

$$h_L(f) \doteq h_L \frac{f}{n_L(f)} \prod_{\substack{q \mid f \\ q \text{ premier}}} \left(1 - \frac{\chi_L(q)}{q}\right)$$

*divisible par  $h_L$ , et si il existe un  $F_{p^s}$  tel que le conducteur  $\mathcal{F}_{F_{p^s}/L} = f_{p^s}\mathcal{O}_L$  de l'extension  $F_{p^s}/L$  vérifie  $f_{p^s} > 1$ , alors  $p$  divise  $i_L(f_{p^s}) = h_L(f_{p^s})/h_L$ .*

*Preuve.*

1) Soit  $\tilde{\sigma} \in \text{Gal}(F_\ell/\mathbb{Q})$  un prolongement de  $\sigma \in \text{Gal}(L/\mathbb{Q})$ . Comme  $\sigma(\mathcal{F}_{F_\ell/L})$  est le conducteur de  $\tilde{\sigma}(F_\ell)/\tilde{\sigma}(L) = F_\ell/L$ , le conducteur  $\mathcal{F}_{F_\ell/L}$  est bien invariant sous l'action de  $\text{Gal}(L/\mathbb{Q})$ .



Soient  $\sigma \in \text{Gal}(F_\ell/\mathbb{Q})$  et  $a \in \mathbb{Z}$ . Nous avons :

$$\sigma \Phi_{F_\ell/L}((a)) \sigma^{-1} = \Phi_{\sigma(F_\ell)/\sigma(L)}((\sigma(a))) = \Phi_{F_\ell/L}((a)).$$

Donc  $\Phi_{F_\ell/L}((a))$  est dans le centre  $Z(\text{Gal}(F_\ell/\mathbb{Q})) = \{\text{Id}\}$  du groupe diédral  $D_{2\ell}$ , puis  $(a) \in \ker(\Phi_{F_\ell/L})$  et  $P_{L,\mathbb{Z}}(\mathcal{F}_{F_\ell/L}) \subseteq \ker(\Phi_{F_\ell/L})$ .

Puisque  $\mathcal{F}_{F_\ell/L}$  est invariant sous l'action de  $\text{Gal}(L/\mathbb{Q})$ , il suffit alors de montrer que si un premier  $\mathcal{Q}$  ramifié dans  $L$  divise  $\mathcal{F}_{F_\ell/L}$ , alors l'exposant  $e$  de  $\mathcal{Q}$  dans  $\mathcal{F}_{F_\ell/L}$  est pair. Soient  $\chi$  l'un quelconque des caractères primitifs associés à  $F_\ell/L$  et  $\chi_0$  son caractère modulaire. Alors  $\chi_0$  est primitif et trivial sur l'image de  $\mathbb{Z}$ . Notons  $\chi_{\mathcal{Q}}$  la composante de  $\chi_0$  sur  $(\mathcal{O}_L/\mathcal{Q}^e)^*$ , qui est donc primitive modulo  $\mathcal{Q}^e$  et triviale sur l'image de  $\mathbb{Z}$ , et supposons  $e = 2m + 1$  impair. Soit alors  $\alpha \equiv 1 \pmod{\mathcal{Q}^{2m}}$ . Il existe  $\beta \in \mathcal{O}_L$  tel que  $\alpha = 1 + \beta q^m$ . Le morphisme canonique  $\mathbb{Z}/q\mathbb{Z} \rightarrow \mathcal{O}_L/\mathcal{Q}$  étant bijectif, il existe  $b \in \mathbb{Z}$  tel que  $\beta \equiv b \pmod{\mathcal{Q}}$  et nous obtenons  $\alpha \equiv 1 + bq^m \pmod{\mathcal{Q}^e}$  et  $\chi_{\mathcal{Q}}(\alpha) = \chi_{\mathcal{Q}}(1 + bq^m) = 1$ , car  $\chi_{\mathcal{Q}}$  est trivial sur  $\mathbb{Z}$ . Ceci contredit la primitivité de  $\chi_{\mathcal{Q}}$ .

2) Le caractère modulaire  $\chi_0$  (associé à l'un quelconque des caractères  $\chi$  d'ordre  $p^s$  associé à l'extension cyclique  $F_{p^s}/L$ ) est d'ordre  $p^t > 1$  divisant  $p^s$  et trivial sur  $\mathbb{Z}$ . Donc  $\chi_0$  peut être considéré comme un caractère sur le groupe  $G = (\mathcal{O}_L/f_{p^s}\mathcal{O}_L)^* / (\mathbb{Z}/f_{p^s}\mathbb{Z})^*$ . Puisque  $\chi_0$  est de plus trivial sur  $\varepsilon_L$  qui engendre un sous-groupe d'ordre  $n_L(f_{p^s})$  de  $G$  alors  $p^t$ , et donc également  $p$ , divisent  $|G|/n_L(f_{p^s}) = i_L(f_{p^s})$ .  $\square$

Les résultats de ce théorème sont très importants car ils vont nous permettre de ramener la construction des corps diédraux de degré  $2p^s$  à celle de leurs caractères primitifs associés puis à celle de leurs caractères modulaires associés (voir théorème 2.2 et paragraphe 2.2). Par composition, nous pourrions alors construire les corps diédraux  $N_{p^s} = MF_{p^s}$  de degré  $2^r p^s$  si nous connaissons le corps diédral  $M$  de degré  $2^r$ . Avant d'énoncer le théorème permettant ces constructions, remarquons tout d'abord que, dans le cas où  $p$  divise  $h_L$ , nous n'aurons à considérer que des  $L$  pour lesquels  $h_L = ph$  avec  $p$  premier impair ne divisant pas  $h$  (voir point 3 du lemme 3.4). Nous expliquons ici seulement la construction des extensions  $F_p/L$  et  $F_{p^2}/L$  qui interviendront au cours de la résolution de notre problème. Le cas général est expliqué dans [18].

**THÉORÈME 2.2.** — *Soient  $L$  un corps quadratique réel et  $p \geq 3$  premier impair donnés.*

1) Soit  $f \geq 1$  entier. Supposons que  $p$  ne divise pas  $h_L$ . Il y a alors une correspondance bijective entre d'une part les corps diédraux  $F_{p^s}$  d'ordre  $2p^s$  cycliques sur  $L$  tels que  $\mathcal{F}_{F_{p^s}/L} = f\mathcal{O}_L$  et d'autre part les groupes engendrés par les caractères primitifs  $\chi_0$  d'ordre  $p^s$  sur  $(\mathcal{O}_L/f\mathcal{O}_L)^*$  triviaux sur  $(\mathbb{Z}/f\mathbb{Z})^*$  et sur  $\varepsilon_L$ .

2) Supposons que le  $p$ -Sylow  $\text{Cl}_p$ , sous-groupe du groupe des classes  $\text{Cl}_L$ , soit cyclique d'ordre  $p$ , engendré par la classe d'un idéal entier  $I_g$ . Soit alors  $\alpha_g \in \mathcal{O}_L$  tel que  $I_g^p = (\alpha_g)$ .

(a) Soit  $f > 1$  entier.

(i) Soit  $F_p$  un corps diédral de degré  $2p$  cyclique sur  $L$  tel que  $\mathcal{F}_{F_p/L} = f\mathcal{O}_L$ . Alors le groupe des caractères modulaires qui lui correspond est cyclique d'ordre  $p$  engendré par un caractère  $\chi_0$  primitif sur  $(\mathcal{O}_L/f\mathcal{O}_L)^*$  trivial sur  $(\mathbb{Z}/f\mathbb{Z})^*$ , sur  $\varepsilon_L$  et sur  $\alpha_g$ .

(ii) Réciproquement, soit  $\chi_0$  un caractère primitif sur  $(\mathcal{O}_L/f\mathcal{O}_L)^*$  trivial sur  $(\mathbb{Z}/f\mathbb{Z})^*$ , sur  $\varepsilon_L$  et sur  $\alpha_g$ . Il existe alors  $p$  corps diédraux distincts  $F_p$  de degré  $2p$  cycliques sur  $L$  tels que  $\mathcal{F}_{F_p/L} = f\mathcal{O}_L$  et tels que leur groupe de caractères modulaires associé soit engendré par  $\chi_0$ .

(b) Soient  $H_p$  le  $p$ -corps de classes de Hilbert de  $L$  et  $f \geq 1$  entier. Notons que  $H_p$  est un corps diédral de degré  $2p$ . Il y a une bijection entre d'une part les corps diédraux  $F_{p^2}$  de degré  $2p^2$  cycliques sur  $H_p$  tels que  $\mathcal{F}_{F_{p^2}/L} = f\mathcal{O}_L$  et d'autre part les groupes engendrés par un caractère primitif  $\chi_0$  d'ordre  $p$  sur  $(\mathcal{O}_L/f\mathcal{O}_L)^*$  trivial sur  $(\mathbb{Z}/f\mathbb{Z})^*$  et sur  $\varepsilon_L$  mais pas sur  $\alpha_g$ .

Preuve. — Posons  $\mu_p = \{z \in \mathbb{C}; z^p = 1\}$ .

1) Soit  $\chi$  l'un des caractères primitifs associés à  $F_p$ . Puisque  $p$  ne divise pas  $h_L$ , il existe  $h'$  tel que  $h_L h' \equiv 1 \pmod{p}$ . Soit alors  $I \in I_L((f))$  : il existe  $\alpha_I \in \mathcal{O}_L$  tel que  $I^{h_L} = (\alpha_I)$  et nous devons donc avoir

$$\chi(I) = \chi(I)^{h_L h'} = \chi((\alpha_I))^{h'} = \chi_0(\alpha_I)^{h'},$$

de sorte que  $\chi$  est entièrement déterminé par  $\chi_0$ . D'où la bijection.

2) (a) (i) Soient  $F_p$  diédral d'ordre  $2p$  et  $\chi$  l'un de ses caractères primitifs associés. Nous savons que  $\chi_0$  est primitif d'ordre  $p$  trivial sur  $\mathbb{Z}$  et sur  $\varepsilon_L$ . De plus  $\chi_0(\alpha_g) = \chi((\alpha_g)) = \chi(I_g)^p = 1$ , donc  $\chi_0$  est trivial sur  $\alpha_g$ .

(ii) Réciproquement soit  $\chi_0$  un caractère primitif d'ordre  $p$  sur  $(\mathcal{O}_L/f\mathcal{O}_L)^*$  trivial sur  $(\mathbb{Z}/f\mathbb{Z})^*$ , sur  $\varepsilon_L$  et sur  $\alpha_g$ . Posons  $h = h_L/p$ . Nous cherchons à construire  $\chi$  primitif d'ordre  $p$  sur  $\text{Cl}_L((f))$  trivial sur  $P_{L,\mathbb{Z}}((f))$  tel que  $\chi_0$  soit son caractère modulaire associé. Soit donc  $I \in I_L((f))$ . Puisque  $I^h \in \text{Cl}_p$ , il existe  $v_I \in \{0, \dots, p-1\}$  et  $\alpha_I \in \mathcal{O}_L$  tels que  $I^h I_g^{v_I} = (\alpha_I)$ . Comme  $p$  ne divise pas  $h$ , il existe  $h'$  tel que  $hh' \equiv 1 \pmod{p}$ . Nous devons alors avoir

$$\chi(I) = \chi_0(\alpha_I)^{h'} \zeta^{-v_I h'} \text{ où } \zeta = \chi(I_g) \in \mu_p.$$

Réciproquement, pour les  $p$  choix possibles de  $\zeta \in \mu_p$  ces relations définissent  $p$  caractères auxquels correspondront  $p$  corps diédraux différents  $F_p$  de degré  $2p$  et tels que  $\mathcal{F}_{F_p/L} = f\mathcal{O}_L$ .

2) (b) Soient  $F_{p^2}$  diédral d'ordre  $2p^2$  contenant  $H_p$  et  $\chi$  l'un de ses caractères primitifs associés. Puisque  $H_p$  est le sous-corps de  $F_{p^2}$  qui est associé au groupe de caractères engendré par  $\chi^p$ , alors  $\chi_0^p = 1$  et puisqu'avec les notations précédentes pour tout  $I$  nous avons  $\chi(I) = \chi_0(\alpha_I)^{h'} \chi(I_g)^{-v_I h'}$ , alors  $\chi(I_g)$  doit être une racine primitive  $p^2$ -ième de l'unité et  $\chi_0(\alpha_g) = \chi((\alpha_g)) = \chi(I_g)^p \neq 1$ .

Réciproquement soit  $\chi_0$  un caractère primitif d'ordre  $p$  sur  $(\mathcal{O}_L/f\mathcal{O}_L)^*/(\mathbb{Z}/f\mathbb{Z})^*$  trivial sur  $\varepsilon_L$  mais pas sur  $\alpha_g$ . Nous cherchons à construire  $\chi$  primitif d'ordre  $p^2$  sur  $\text{Cl}_L((f))$  trivial sur  $P_{L,\mathbb{Z}}((f))$  tel que  $\chi_0$  soit son caractère modulaire associé. Comme ci-dessus, nous devons avoir

$$\chi(I) = \chi_0(\alpha_I)^{h'} \zeta^{-v_I h'} \text{ où } \zeta = \chi(I_g) \text{ vérifie } \zeta^p = \chi_0(\alpha_g) \in \mu_p.$$

Réciproquement, pour les  $p$  tels choix possibles de  $\zeta$  ces relations définissent  $p$  caractères engendrant un même groupe cyclique, donc auxquels correspondront un unique corps diédral  $F_{p^2}$  de degré  $2p^2$  et tel que  $\mathcal{F}_{F_{p^2}/L} = f\mathcal{O}_L$ .  $\square$

## 2.2. Caractères modulaires primitifs associés aux corps diédraux de degré $2p^s$ .

Nous expliquons ici comment construire les caractères modulaires primitifs  $\chi_0$  associés aux corps diédraux  $F_{p^s}$  de degré  $2p^s$ . Nous pourrons ainsi grâce au théorème 2.2 construire les corps diédraux réels  $F_p$  et  $F_{p^2}$  cycliques sur  $L$  et de degré respectif  $2p$  et  $2p^2$ .

**THÉORÈME 2.3.** — *Soient  $L$  un corps quadratique réel,  $p$  un premier impair,  $q$  un premier,  $e$  et  $k$  deux entiers naturels non nuls. Posons*

$$G_{q^e} = (\mathcal{O}_L/q^e\mathcal{O}_L)^* \quad \text{et} \quad H_{q^e} = (\mathbb{Z}/q^e\mathbb{Z})^*.$$

1) Supposons  $q \neq p$ . Alors il existe un caractère  $\chi_0$  primitif d'ordre  $p^k$  sur  $G_{q^e}$  trivial sur  $H_{q^e}$  si et seulement si  $e = 1$  et  $q \equiv \chi_L(q) \pmod{p^k}$ .

(a) Si  $\chi_L(q) = -1$  alors  $G_q/H_q$  est cyclique et les tels  $\chi_0$  sont faciles à construire.

(b) Si  $\chi_L(q) = 1$  alors  $(q) = \mathcal{Q}\mathcal{Q}'$ , le groupe  $G_{\mathcal{Q}} = (\mathcal{O}_L/\mathcal{Q})^*$  est cyclique et les tels  $\chi_0$  sont les caractères de la forme

$$\chi_0(\alpha) = \varphi_0(\alpha/\alpha'),$$

où  $\alpha'$  désigne le conjugué de  $\alpha$  et où  $\varphi_0$  est un caractère primitif d'ordre  $p^k$  sur  $G_{\mathcal{Q}}$ .

2) Supposons  $q = p$  et  $\chi_L(p) \neq 0$ . Alors il existe un caractère  $\chi_0$  primitif d'ordre  $p^k$  sur  $G_{p^e}$  trivial sur  $H_{p^e}$  si et seulement si  $e = k + 1$ .

(a) Si  $\chi_L(p) = -1$  alors  $G_{p^{k+1}}/H_{p^{k+1}}$  est cyclique et les tels  $\chi_0$  sont faciles à construire.

(b) Si  $\chi_L(p) = 1$  alors  $(p) = \mathcal{P}\mathcal{P}'$ , le groupe  $G_{\mathcal{P}^{k+1}} = (\mathcal{O}_L/\mathcal{P}^{k+1})^*$  est cyclique et les tels  $\chi_0$  sont de la forme

$$\chi_0(\alpha) = \varphi_0(\alpha/\alpha'),$$

où  $\alpha'$  désigne le conjugué de  $\alpha$  et où  $\varphi_0$  est un caractère primitif d'ordre  $p^k$  sur  $G_{\mathcal{P}^{k+1}}$ .

3) Supposons  $q = p$  et  $\chi_L(p) = 0$ .

(a) Si  $p > 3$  ou si  $d_L \equiv 3 \pmod{9}$  alors il existe un caractère  $\chi_0$  primitif d'ordre  $p^k$  sur  $G_{p^e}$  trivial sur  $H_{p^e}$  si et seulement si  $e = k$ . Dans ce cas  $G_{p^k}/H_{p^k}$  est cyclique.

(b) Si  $p = 3$  et  $d_L \equiv 6 \pmod{9}$  alors il existe un caractère  $\chi_0$  primitif d'ordre  $p^k$  sur  $G_{p^e}$  trivial sur  $H_{p^e}$  si et seulement si  $(k \geq 2$  et  $e = k + 1)$  ou si  $(k = 1$  et  $e = 1$  ou  $2)$ . Nous avons  $G_p/H_p \simeq \mathbb{Z}/3\mathbb{Z}$  et, pour  $e > 1$ ,  $G_{p^e}/H_{p^e} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^{e-1}\mathbb{Z}$ .

*Preuve.* — Nous donnons seulement une idée de la preuve (voir [7] pour les détails). Il est facile de voir que  $G_{q^e}/H_{q^e}$  est d'ordre  $q^{e-1}(q - \chi_L(q))$ . Comme  $\chi_0$  est d'ordre  $p^k$  modulo  $q^e$  et trivial sur l'image de  $\mathbb{Z}$ , nous devons avoir dans le premier cas  $q \equiv \chi_L(q) \pmod{p^k}$  et nous montrons que si  $e \geq 2$  alors  $\chi_0$  n'est pas primitif, dans le second cas  $e - 1 \geq k$  et nous montrons que si  $e \geq k + 2$  alors  $\chi_0$  n'est pas primitif, et dans le dernier cas  $e - 1 \geq k - 1$  et nous montrons que si  $e \geq k + 2$  alors  $\chi_0$  n'est pas primitif. Pour montrer les équivalences nous travaillons sur la structure des groupes  $G_{q^e}/H_{q^e}$ .  $\square$

COROLLAIRE 2.4 (voir également [19], th. III.1, cor. 2, p. 55). — Soit  $F_p$  un corps diédral réel de degré  $2p$ , avec  $p$  premier impair, cyclique sur  $L$ . Notons  $f_p \mathcal{O}_L$  le conducteur de  $F_p/L$ , avec donc  $f_p \geq 1$  entier. Il existe des nombres premiers deux à deux distincts  $q_i$  non-égaux à  $p$  et vérifiant  $q_i \equiv \chi_L(q_i) \pmod{p}$  tels que  $f_p = p^a \prod_{i=1}^r q_i$  avec  $a = 0$  ou

$$a = \begin{cases} 2 & \text{si } \chi_L(p) \neq 0, \\ 1 & \text{si } \chi_L(p) = 0 \text{ avec } p \geq 5 \text{ ou } d_L \equiv 3 \pmod{9}, \\ 1 \text{ ou } 2 & \text{si } p = 3 \text{ et } d_L \equiv 6 \pmod{9}. \end{cases}$$

### 3. Minorations de nombres de classes relatifs.

Le but de ce paragraphe est d'expliquer comment, pour  $M \in \mathcal{D}_2$  fixé, nous pouvons obtenir des minorations de  $h_N^-$  tendant vers l'infini avec  $d_N$  lorsque  $N$  varie parmi les corps à multiplication complexe diédraux ayant pour 2-sous-corps maximal  $M$ . Nous montrons ensuite comment ces minorations sont suffisamment bonnes pour ramener la détermination de tous les corps à multiplication complexe diédraux  $N$  de nombre de classes relatif un au calcul des nombres de classes relatifs d'une liste raisonnable de tels corps  $N$ . En particulier, notre première étape est de montrer (au théorème 3.8) que si  $h_{N_p}^- = 1$  alors  $p \leq 17$ , borne vraiment très raisonnable et qui montre clairement que la détermination de tous les  $N_p$  tels que  $h_{N_p}^- = 1$  est assurée d'aboutir, en les déterminant à  $M \in \mathcal{D}_2$  et  $p \leq 17$  donnés.

#### 3.1. Définition de $\mu_L$ et majorations de $|L(1, \chi)|$ .

Soit  $L$  un corps quadratique réel de caractère quadratique associé  $\chi_L$ . Posons (voir [11])

$$\mu_L = 1 + \frac{L'(1, \chi_L)}{L(1, \chi_L)} + \log \left( \frac{\sqrt{d_L}}{4\pi} \right).$$

Nous avons  $L(1, \chi_L) > 0$  et  $\mu_L > 0$ ; le calcul numérique de ces  $\mu_L$  est expliqué dans [12].

PROPOSITION 3.1 (voir [11]). — Soit  $E/L$  une extension abélienne de corps de nombres totalement réels, avec  $L$  quadratique. Alors, pour tout caractère  $\chi$  de degré un associé à l'extension abélienne  $E/L$ , nous avons

$$(2) \quad |L(1, \chi)| \leq \operatorname{Res}_{s=1}(\zeta_L) \left( \frac{1}{2} \log f_\chi + 2\mu_L \right)$$

où  $f_\chi = N_{L/\mathbb{Q}}(\mathcal{F}_\chi)$  désigne la norme du conducteur  $\mathcal{F}_\chi$  de  $\chi$ . Si  $f_\chi = 1$  ou si  $f_\chi \geq e^{2\mu_L}$ , nous avons la meilleure majoration

$$(3) \quad |L(1, \chi)| \leq \operatorname{Res}_{s=1}(\zeta_L) \left( \frac{1}{2} \log f_\chi + \mu_L \right).$$

**COROLLAIRE 3.2.** — Soit  $N_p = MF_p$  un corps diédral à multiplication complexe de degré  $4m = 2^r p$  avec  $p$  premier impair (voir figure 1 pour les notations), de sorte que  $N_p^+/L$  est cyclique de degré  $m = 2^{r-2}p$ . Supposons que  $M^+/L$  est non ramifiée et notons  $f_p \mathcal{O}_L$  le conducteur de l'extension  $F_p/L$ . Alors

$$\operatorname{Res}_{s=1}(\zeta_{N_p^+}) \leq \left( \operatorname{Res}_{s=1}(\zeta_L) \right)^m (\log f_p + 2\mu_L)^{m-1}.$$

Si de plus  $f_p = 1$  ou  $f_p \geq e^{\mu_L}$ , alors

$$\operatorname{Res}_{s=1}(\zeta_{N_p^+}) \leq \left( \operatorname{Res}_{s=1}(\zeta_L) \right)^m (\log f_p + \mu_L)^{m-1}.$$

*Preuve.* — Il suffit de remarquer que

$$\operatorname{Res}_{s=1}(\zeta_{N_p^+}) = \operatorname{Res}_{s=1}(\zeta_L) \prod_{\chi \neq 1} L(1, \chi)$$

où le produit est étendu aux  $m - 1$  caractères  $\chi$  non triviaux associés à l'extension cyclique  $N_p^+/L$ . Comme  $M^+/L$  est non ramifiée,  $\chi$  est soit de conducteur  $f_p \mathcal{O}_L$  soit de conducteur  $\mathcal{O}_L$ , ce qui donne le résultat en utilisant (2) ou (3) selon le cas.  $\square$

### 3.2. Minoration de $h_N^-$ lorsque $h_M^- = 1$ .

Rappelons pour commencer les résultats de la détermination par S. Louboutin et R. Okazaki de l'ensemble  $\mathcal{D}_2$  des corps diédraux à multiplication complexe de degré  $2^r \geq 4$  n'importe quelle puissance de deux qui sont de nombre de classes relatif un :

#### PROPOSITION 3.3.

1) Il y a 147 corps imaginaires biquadratiques bicycliques  $M$  tels que  $h_M^- = 1$  (voir [17]).

2) Soit  $M$  un corps diédral à multiplication complexe de degré  $2^r \geq 8$  une puissance de deux. Alors  $h_M^-$  est impair si et seulement si  $M$  est le 2-corps de classes de Hilbert au sens strict d'un corps quadratique réel  $L$  d'unité fondamentale de norme  $+1$  et dont le 2-Sylow du groupe des classes au sens strict est cyclique (voir [10]).

3) En particulier, si  $M$  est un corps à multiplication complexe diédral de degré  $2^r \geq 4$  une puissance de 2 et si son nombre de classes relatif est impair, alors  $M^+/L$  est non ramifiée.

4) Il existe exactement 19 corps diédraux à multiplication complexe  $M$  de degré 8 de nombre de classes relatif un, à savoir les 2-corps de classes de Hilbert au sens strict des  $L = \mathbb{Q}(\sqrt{rs})$  avec  $rs \in \{2.17; 2.73; 2.89; 2.233; 2.281; 5.41; 5.61; 5.109; 5.149; 5.269; 5.389; 13.17; 13.29; 13.157; 13.181; 17.137; 17.257; 29.53; 73.97\}$ . De plus tous ces corps  $M$  sont principaux excepté ceux associés à  $L = \mathbb{Q}(\sqrt{1345})$  ou  $\mathbb{Q}(\sqrt{4369})$ , pour lesquels  $h_M = 3$  (voir [15]).

5) Il existe exactement 5 corps diédraux à multiplication complexe  $M$  de degré 16 et de nombre de classes relatif un, à savoir les 2-corps de classes de Hilbert au sens strict des  $L = \mathbb{Q}(\sqrt{rs})$  avec  $rs \in \{2.257; 5.101; 5.181; 13.53; 13.61\}$ . De plus tous ces corps  $M$  sont principaux excepté celui associé à  $L = \mathbb{Q}(\sqrt{514})$ , pour lequel  $h_M = 3$  (voir [16]).

6) Il n'existe aucun corps diédral à multiplication complexe  $M$  de degré  $2^r \geq 32$  de nombre de classes relatif un (voir [16]).

#### LEMME 3.4.

1) Soit  $N_{p^s}$  un corps diédral de degré  $2^r p^s$ , avec  $p$  premier impair. Supposons  $h_{N_{p^s}}^-$  impair. Alors  $M^+/L$  est non ramifiée, ce qui donne  $d_{N_{p^s}^+} = d_{F_{p^s}}^{2^r-2}$  (remarquons que  $d_{F_p} = d_L^p f_p^{2(p-1)}$  et  $d_{F_{p^2}} = d_L^{p^2} f_p^{2(p-1)} f_{p^2}^{2(p^2-p)}$  où  $f_p \mathcal{O}_L$  et  $f_{p^2} \mathcal{O}_L$  désignent respectivement les conducteurs des extensions  $F_p/L$  et  $F_{p^2}/L$ ). De plus  $d_M/d_L^{2^r-1}$  est le carré d'un entier.

2) Soit  $M$  l'un quelconque des  $171 = 147 + 19 + 5$  corps diédraux de  $\mathcal{D}_2$ . Alors  $\zeta_M(s) < 0$  pour  $0 < s < 1$ .

3) Soit  $L$  l'un quelconque des  $155 = 131 + 19 + 5$  sous-corps quadratiques réels avec  $M/L$  cyclique et  $M \in \mathcal{D}_2$ . Alors  $\mu_L < 3$  et si  $p$  premier impair divise  $h_L$  alors  $p \in \{3, 5, 7\}$  et  $p^2$  ne divise pas  $h_L$ .

*Preuve.* — Le point 1) découle du point 3) de la proposition 3.3.

Le point 2) se prouve en utilisant les techniques introduites dans [2] et [3] (voir [7]). Pour le point 3), nous renvoyons à [8] où se trouvent les valeurs numériques approchées des constantes  $\mu_L$  attachées à ces 155 corps quadratiques réels  $L$ , valeurs numériques calculées à l'aide des techniques exposées dans [12]. □

**THÉORÈME 3.5.** — *Soit  $N$  un corps diédral à multiplication complexe de degré  $4m = 2^r \ell$  avec  $\ell$  entier impair. Supposons que son 2-sous-corps maximal  $M$  est dans  $\mathcal{D}_2$ , ce qui est en particulier le cas lorsque  $h_N^- = 1$  (voir proposition 1.2). Alors*

$$h_N^- \geq \varepsilon_{N^+} \frac{Q_M w_M}{(2\pi)^{2m}} \frac{2\sqrt{d_N/d_{N^+}}}{e(\log d_N) \operatorname{Res}_{s=1}(\zeta_{N^+})}$$

où

$$\varepsilon_{N^+} = \frac{2}{5} \exp(-4\pi m d_{N^+}^{-1/2m}).$$

*Preuve.* — Soit  $\mathcal{X}_{N/L}$  l'ensemble des  $2^{r-1}(\ell - 1)$  caractères d'ordre ne divisant pas  $2^{r-1}$  associés à l'extension  $N/L$  cyclique de degré  $2^{r-1}\ell$ . Puisque

$$(\zeta_N/\zeta_M)(s) = \prod_{\chi \in \mathcal{X}_{N/L}} L(s, \chi),$$

puisque les caractères de  $\mathcal{X}_{N/L}$  apparaissent en  $2^{r-2}(\ell - 1)$  paires de caractères conjugués  $\{\chi, \bar{\chi}\}$  et puisque pour  $s$  réel  $L(s, \bar{\chi}) = \overline{L(s, \chi)}$ , nous avons alors  $(\zeta_N/\zeta_M)(s) \geq 0$  pour  $s$  réel. D'après le point 2) du lemme 3.4, nous avons donc  $\zeta_N(1 - 2/\log d_N) \leq 0$ . En utilisant [9], prop. A, point (b), avec  $s_0 = 1 - 2/\log d_N$ , nous obtenons

$$\operatorname{Res}_{s=1}(\zeta_N) \geq \frac{2\varepsilon_{N^+}}{e \log d_N}.$$

En remarquant que  $w_N = w_M$ , la proposition 1.2 et la formule (1) donnent alors le résultat. □

### 3.3. Borne sur $p$ lorsque $h_{N_p}^- = 1$ .

Une première et très importante application de cette minoration de  $h_N^-$  est, d'après la proposition 1.2, de trouver une borne sur les facteurs premiers du degré des corps diédraux à multiplication complexe de nombre de classes relatif un (voir théorème 3.8 ci-dessous).



LEMME 3.6. — Soit  $M \in \mathcal{D}_2$  fixé, de degré  $2^r \geq 4$ . Posons

$$b_L = \max(\log \sqrt{d_L}, 2\mu_L).$$

Soit  $p \geq 3$  premier impair,  $N = N_p = F_p M$  un corps diédral à multiplication complexe de degré  $4m = 2^r p$  et  $f_p \mathcal{O}_L$  le conducteur de l'extension  $F_p/L$ . Supposons également  $f_p > 2$  et posons

$$\alpha_L(f_p) = \frac{f_p \sqrt{d_L}}{4\pi^2 L(1, \chi_L)(\log f_p + b_L)}$$

(remarquons que  $f_p \mapsto \alpha_L(f_p)$  est croissante). Alors

$$(4) \quad h_{N_p}^- \geq \frac{2}{5e} \cdot \frac{\exp(-2^r \pi p^{1/p} / \sqrt{d_L})}{2^{r-2} p f_p^{2^{r-2}}} \alpha_L(f_p)^{2^{r-2} p}.$$

Preuve. — Puisque  $d_{N_p} \geq d_{N_p}^2$ , la minoration du théorème 3.5 donne :

$$h_{N_p}^- \geq \frac{2\varepsilon_{N_p^+} \sqrt{d_{N_p^+}}}{(2\pi)^{2m} e (\log d_{N_p^+}) \operatorname{Res}_{s=1} \zeta_{N_p^+}(s)}.$$

De plus (voir lemme 3.4, point 1)

$$\log d_{N_p^+} = 2m \left( \log \sqrt{d_L} + \left(1 - \frac{1}{p}\right) \log f_p \right) \leq 2m(\log f_p + b_L)$$

et (voir corollaire 3.2) nous avons

$$\operatorname{Res}_{s=1} (\zeta_{N_p^+}) \leq L(1, \chi_L)^m (\log f_p + 2\mu_L)^{m-1}.$$

Puisque  $f_p > 2$  implique  $f_p \geq p$  (voir corollaire 2.4), nous obtenons

$$\varepsilon_{N_p^+} = \frac{2}{5} \exp(-4m\pi f_p^{-1+1/p} / \sqrt{d_L}) \geq \frac{2}{5} \exp(-2^r \pi p^{1/p} / \sqrt{d_L}).$$

Nous obtenons donc bien (4).  $\square$

Soit  $M \in \mathcal{D}_2$  donné. Nous voulons utiliser ce lemme pour prouver que si  $p$  est suffisamment grand alors, pour tout  $N_p = F_p M$ , nous avons  $h_{N_p}^- > 1$ . Pour cela, nous développons d'abord un moyen efficace de calcul de minorants  $F_L(p)$  des conducteurs  $f_q$  des corps diédraux  $F_q$  de degré  $2q \geq 2p$  (avec  $q$  premier impair), l'idée étant alors de trouver pour  $M$  donné un  $p$  tel que  $F_L(p)$  soit suffisamment grand pour que, pour  $q \geq p$ , la minoration  $f_q \geq F_L(p)$  et le lemme précédent impliquent  $h_{N_q}^- > 1$ .

DÉFINITION 3.7. — Soient  $L$  un corps quadratique réel et  $p > 3$  un premier supérieur à tous les facteurs premiers de  $h_L$  (pour les 155 corps quadratiques que nous considérons, il suffit d'après le point 3 du lemme 3.4 de prendre  $p \geq 11$ ). Posons

$$f_L(p) = \min\{f > 1; f \text{ tel qu'au corollaire 2.4 et } p \text{ divise } i_L(f)\},$$

de sorte que, pour tout corps diédral  $F_p$  de degré  $2p$  contenant  $L$ , le conducteur  $f_p \mathcal{O}_L$  de l'extension  $F_p/L$  vérifie  $f_p \geq f_L(p)$ . Posons ensuite

$$F_L(p) = \min\{f_L(q); q \text{ premier et } q \geq p\},$$

de sorte que pour, tout corps diédral  $F_q$  de degré  $2q \geq 2p$  contenant  $L$ , le conducteur  $f_q \mathcal{O}_L$  de l'extension  $F_q/L$  vérifie  $f_q \geq F_L(p)$ . Remarquons qu'alors  $f_L(p) \geq p$  et donc que

$$F_L(p) = \min\{f_L(q); q \text{ premier et } p \leq q \leq f_L(p)\},$$

ce qui conduit à l'algorithme de calcul numérique de  $F_L(p)$  suivant :

```

input :  $q$  et  $L$ 
begin
   $F_L(p) := f_L(p); q := p + 2;$ 
  while  $q \leq F_L(p)$  do begin
    if  $q$  est premier then  $F_L(p) := \min(F_L(p), f_L(q));$ 
     $q := q + 2;$ 
  end
  return  $F_L(p);$ 
end

```

Nous renvoyons le lecteur à [8] où il y trouvera les valeurs de  $F_L(19)$  (calculées à l'aide de cet algorithme) pour les 155 corps quadratiques réels  $L$  dont il est question au point 3) du lemme 3.4. Nous allons utiliser ces valeurs pour prouver :

THÉORÈME 3.8. — Si  $h_{N_p}^- = 1$  alors  $p \leq 17$ .

*Preuve.* — Pour chacun des 171 corps  $M \in \mathcal{D}_2$  à considérer, nous calculons une borne  $p_M \geq 11$  sur  $p$  telle que  $M \subseteq N_p$  et  $p \geq p_M \geq 11$  impliquent  $h_{N_p}^- > 1$ . Notons  $L$  le sous-corps quadratique réel de  $M$  sur

lequel  $M$  est cyclique. Notons que  $p \geq 11$  implique que  $p$  ne divise pas  $h_L$  (voir point 3 du lemme 3.4). Les fonctions

$$p \mapsto a^p/p \quad \text{et} \quad f_p \mapsto f_p^{1-1/p}/(\log f_p + b_L)$$

étant croissantes dès que  $a \geq e^{1/11}$  (car  $f_p \geq p \geq 11$  et  $b_L \geq \log \sqrt{5}$ ), la minoration (4) est croissante en  $p$  et  $f_p$  dès que  $\alpha_L(f_p) \geq e^{1/11}$ . Notons  $p_M$  le plus petit premier  $p \geq 11$  pour lequel  $\alpha_L(F_L(p)) \geq e^{1/11}$  et pour lequel la minoration (4) avec  $f_p = F_L(p)$  donne  $h_{N_p}^- > 1$ . Si  $p \geq p_M$  nous avons alors  $F_L(p) \geq F_L(p_M)$ , puis  $\alpha_L(F_L(p)) \geq \alpha_L(F_L(p_M)) \geq e^{1/11}$  et la minoration (4) étant croissante avec  $p$  et  $f_p$ , nous obtenons  $h_{N_p}^- > 1$ . Après calcul, tous ces  $p_M$  vérifient  $p_M \leq 19$  (voir tables de [8]). Donc  $p \geq 19$  implique  $h_{N_p}^- > 1$ .  $\square$

#### 4. Résolution du problème en degré $4m=2^r p$ .

Notre objectif est maintenant de prouver le résultat suivant qui d'une part donne la liste complète des corps à multiplication complexe diédraux de degré  $2^r p$  de nombre de classes relatif un, et d'autre part montre que les corps à multiplication complexe diédraux de nombre de classes relatif un sont d'ordre  $2^r p^s$  avec  $p \in \{3, 5\}$ ,  $r \geq 2$  et  $s \geq 0$  :

##### THÉORÈME 4.1.

1) Il y a exactement 16 corps de nombres diédraux à multiplication complexe  $N_p$  de degré 12 de nombre de classes relatif un, à savoir les composita  $N_p = KM$  (avec  $K$  totalement réel de degré 3 non-galoisien et  $M$  imaginaire bicyclique biquadratique) donnés dans la table 1 (voir [17]).

2) Il y a exactement deux corps de nombres diédraux à multiplication complexe  $N_p$  de degré 20 et de nombre de classes relatif un, à savoir les composita  $N_p = KM$  (avec  $K$  totalement réel de degré 5 non-galoisien et  $M$  imaginaire bicyclique biquadratique) donnés dans la table 2.

De plus il n'existe aucun corps de nombres diédral à multiplication complexe de nombre de classes relatif un de degré  $4p$  avec  $p$  premier,  $p > 5$ .

3) Il n'y a qu'un corps de nombres diédral  $N_p$  à multiplication complexe de degré  $2^r p$  avec  $r \geq 3$  et  $p$  premier impair, et de nombre de classes relatif un, à savoir le corps de classes de Hilbert au sens strict de  $L = \mathbb{Q}(\sqrt{1345})$  qui est de degré 24 et est le compositum  $N_p = KM$  (avec  $K$

totallement réel de degré 3 non-galoisien et  $M$  imaginaire diédral de degré 8) donné dans la table 3.

4) Si un corps à multiplication complexe diédral  $N$  est de nombre de classes relatif un, alors il est de degré  $2^r p^s$  avec  $p \in \{3, 5\}$ ,  $r \geq 2$  et  $s \geq 0$ .

indice	$P_K(X)$	$d_L$	$M$	$f_p$	$h_{N_p^-}$	$h_{N_p^+}$
1	$X^3 - 12X - 14$	5	$\mathbb{Q}(\sqrt{-3}, \sqrt{-15})$	18	1	1
2	$X^3 - 15X - 20$	12	$\mathbb{Q}(\sqrt{-3}, \sqrt{-4})$	15	1	1
3	$X^3 - 6X - 2$	21	$\mathbb{Q}(\sqrt{-3}, \sqrt{-7})$	6	1	1
4	$X^3 - 9X - 6$	24	$\mathbb{Q}(\sqrt{-3}, \sqrt{-8})$	9	1	1
5	$X^3 + X^2 - 3X - 1$	37	$\mathbb{Q}(\sqrt{-4}, \sqrt{-148})$	2	1	1
6	$X^3 - X^2 - 8X - 3$	57	$\mathbb{Q}(\sqrt{-3}, \sqrt{-19})$	5	1	1
7	$X^3 - 18X - 12$	60	$\mathbb{Q}(\sqrt{-3}, \sqrt{-20})$	9	1	2
8	$X^3 + X^2 - 16X - 8$	88	$\mathbb{Q}(\sqrt{-8}, \sqrt{-11})$	7	1	3
9	$X^3 - 27X - 51$	105	$\mathbb{Q}(\sqrt{-7}, \sqrt{-15})$	9	1	2
10	$X^3 - 33X - 22$	120	$\mathbb{Q}(\sqrt{-3}, \sqrt{-40})$	11	1	2
11	$X^3 - 18X - 16$	456	$\mathbb{Q}(\sqrt{-19}, \sqrt{-24})$	3	1	2
12	$X^3 + X^2 - 5X - 4$	469	$\mathbb{Q}(\sqrt{-7}, \sqrt{-67})$	1	1	1
13	$X^3 - 5X - 1$	473	$\mathbb{Q}(\sqrt{-11}, \sqrt{-43})$	1	1	1
14	$X^3 - 7X - 4$	940	$\mathbb{Q}(\sqrt{-4}, \sqrt{-235})$	1	1	2
15	$X^3 - X^2 - 11X - 1$	1304	$\mathbb{Q}(\sqrt{-8}, \sqrt{-163})$	1	1	1
16	$X^3 - X^2 - 8X - 2$	1708	$\mathbb{Q}(\sqrt{-4}, \sqrt{-427})$	1	1	2

Table 1

17	$X^5 - 35X^3 - 30X^2 + 10X + 4$	280	$\mathbb{Q}(\sqrt{-8}, \sqrt{-35})$	5	1	2
18	$X^5 + X^4 - 6X^3 - 5X^2 + 3X + 1$	817	$\mathbb{Q}(\sqrt{-19}, \sqrt{-43})$	1	1	1

Table 2

19	$X^3 - 7X - 1$	1345	$\mathbb{Q}\left(\sqrt{5}, \sqrt{269}, \sqrt{-(17+2 \cdot \sqrt{5})}\right)$	1	1	1
----	----------------	------	--	---	---	---

Table 3

*Preuve.* — Prouvons les points 2) et 3) du théorème. Nous travaillons à  $M \in \mathcal{D}_2$  et  $p$  fixés. Rappelons qu'alors  $M^+/L$  est non ramifiée (voir point 3 de la proposition 3.3). Soit  $N_p = F_p M$  un corps à multiplication complexe diédral de degré  $4m = 2^r p$ . Notons

$$\mathcal{F}_{F_p/L}, \quad \mathcal{F}_{M/L}, \quad \mathcal{F}_{N_p/L} = \text{ppcm}(\mathcal{F}_{F_p/L}, \mathcal{F}_{M/L})$$

les conducteurs respectifs des extensions cycliques  $F_p/L$ ,  $M/L$  et  $N_p/L$ . Ces conducteurs étant invariants sous l'action de  $\text{Gal}(L/\mathbb{Q})$  et  $M^+/L$  étant non ramifiée, nous avons

$$N_{L/\mathbb{Q}}(\mathcal{F}_{N_p/L}) = \text{ppcm}(N_{L/\mathbb{Q}}(\mathcal{F}_{F_p/L}), N_{L/\mathbb{Q}}(\mathcal{F}_{M/L})) = \text{ppcm}(f_p^2, d_M/d_L^{2^{r-1}}).$$

En posant  $f_{M/L} = \sqrt{d_M/d_L^{2^{r-1}}}$  qui est entier (voir lemme 3.4, point 1), nous obtenons

$$d_{N_p} = d_{N_p^+}^2 (f_{M/L}^p / \text{pgcd}(f_p, f_{M/L})^{p-1})^{2^{r-1}} \geq f_{M/L}^2 d_{N_p^+}^2.$$

Posons  $c_L = \mu_L$  si  $f_p = 1$  ou  $f_p \geq e^{\mu_L}$ , et  $c_L = 2\mu_L$  sinon. En combinant le théorème 3.5 et le corollaire 3.2, nous obtenons alors

$$h_{N_p}^- \geq \varepsilon_{N_p^+} \frac{Q_M w_M}{(2\pi)^{2m}} \frac{2\sqrt{d_{N_p}/d_{N_p^+}}}{e(\log d_{N_p}) \text{Res}_{s=1}(\zeta_L)^m (\log f_p + c_L)^{m-1}}.$$

Cette minoration étant croissante en  $d_{N_p}$  qui vérifie  $d_{N_p} \geq (f_{M/L} d_{N_p^+})^2$ , nous obtenons

$$(5) \quad h_{N_p}^- \geq \varepsilon_{N_p^+} \frac{w_M Q_M f_{M/L}}{e} \left( \frac{\sqrt{d_L}}{4\pi^2 L(1, \chi_L)} \right)^m \times \frac{f_p^{m-2^{r-2}}}{\log(f_{M/L} d_{N_p^+}) (\log f_p + c_L)^{m-1}}.$$

Cette minoration est croissante en  $f_p$ , dès que  $f_p \geq 8 > e^2$ .

Pour chaque  $M \in \mathcal{D}_2$  et  $p \leq 17$ , nous calculons une borne entière  $B(M, p)$  telle que  $f_p > B(M, p)$  implique  $h_{N_p}^- > 1$ , 1 dans (5). En utilisant les résultats du paragraphe 2, nous construisons alors tous les corps diédraux réels  $F_p$  pour lesquels les  $f_p \geq 1$  des conducteurs  $\mathcal{F}_{F_p/L} = f_p \mathcal{O}_L$  sont inférieurs ou égaux à  $B(M, p)$  et obtenons ainsi une liste finie de corps diédraux  $N_p = F_p M$  de laquelle nous éliminons tous les  $N_p$  pour lesquels la proposition 4.2 ci-dessous donne  $h_{N_p}^- > 1$ . Nous obtenons ainsi une liste

finie et restreinte de (environ 800) corps diédraux  $N_p$  contenant tous ceux de degré  $2^r p$  et de nombre de classes relatif un. Cette liste est donnée aux tables 4, 5 et 6 (sauf ceux de degré 12 ce qui aurait demandé trop de place).

Pour chacun des  $N_p$  de cette liste, nous calculons  $h_{N_p}^-$  grâce à la méthode qui sera exposée au paragraphe 7 et nous obtenons ainsi la liste  $\mathcal{D}_p$  de tous les corps diédraux  $N_p$  de degré  $2^r p$  et de nombre de classes relatif un. En particulier, nous avons revérifié en un temps très raisonnable (seulement 600 calculs de nombres de classes relatifs, et ce en environ 15 heures de calcul sur microordinateur) les résultats trouvés dans [17] en degré 12 (où il avait fallu calculer plus de 10 000 nombres de classes relatifs, et ce en 40 jours de calcul sur stations de travail).

Pour chaque  $N_p \in \mathcal{D}_p$ , nous calculons finalement  $h_{N_p} = h_{N_p}^- h_{N_p}^+$ , ce qui revient à calculer  $h_{N_p}^+$ . Ces calculs de  $h_{N_p}^+$  seront expliqués au paragraphe 6 et permettent de conclure la preuve des points 2) et 3).

Prouvons finalement le point 4) du théorème. Supposons  $h_N^- = 1$  et  $[N : \mathbb{Q}] = 4m = 2^r \ell$  avec  $\ell > 1$  entier divisible par deux premiers distincts  $p_1$  et  $p_2$ . Dans ce cas  $N$  posséderait deux sous-corps diédraux à multiplication complexe  $N_{p_1}$  et  $N_{p_2}$  de degrés respectifs  $2^r p_1$  et  $2^r p_2$ . Ces deux corps  $N_{p_1}$  et  $N_{p_2}$  seraient cycliques sur le même sous-corps quadratique réel  $L$  et tels que  $h_{N_{p_1}}^- = h_{N_{p_2}}^- = 1$  (car  $[N : N_{p_i}]$  étant impair  $h_{N_{p_i}}^-$  divise  $h_N^-$  d'après la proposition 1.2). D'après les points 1), 2) et 3) du théorème, cette situation est impossible.  $\square$

Comme indiqué, pour nettement diminuer le nombre de nombres de classes relatifs à calculer, nous utilisons le résultat suivant qui nous permet dans certains cas de conclure directement que  $h_{N_p}^- > 1$ .

PROPOSITION 4.2. — Soit  $N_p$  un corps diédral à multiplication complexe de degré  $2^r p$  avec  $p$  premier impair.

1) Si  $t$  idéaux premiers de  $N_p^+$  sont ramifiés dans  $N_p/N_p^+$  alors  $2^{t-1}$  divise  $h_{N_p}^-$  (voir [15]).

2) Si  $T$  idéaux premiers de  $M^+$  sont ramifiés dans  $N_p^+/M^+$  et décomposés dans  $M/M^+$  alors  $p^{T-1}$  divise  $h_{N_p}^-$  et si de plus  $p$  ne divise pas  $w_M$  alors  $p^T$  divise  $h_{N_p}^-$  (voir [17]). Remarquons que pour  $M \in \mathcal{D}_2$ ,  $w_M = 2$  pour  $[M : \mathbb{Q}] = 2^r \geq 8$  et que si  $[M : \mathbb{Q}] = 4$ , alors les seuls diviseurs premiers de  $w_M$  sont 2 et 3.

## 5. Résolution du problème en degré quelconque.

LEMME 5.1. — Les 10 corps  $N_p \in \mathcal{D}_p$  d'indice 1, 2, 3, 4, 5, 6, 7, 8, 10 et 11 (dans les tables 1 à 3) ne sont sous-corps d'aucun corps à multiplication complexe  $N_{p^2}$  diédral de degré  $2^r p^2$ . En fait, leurs 10 sous-corps diédraux réels  $F_p$  ne sont sous-corps d'aucun corps réel diédral  $F_{p^2}$  de degré  $2p^2$ .

Preuve. — Reprenons les notations de la figure 1. Supposons qu'il existe  $F_{p^2}$  diédral réel de degré  $2p^2$  contenant l'un de ces  $F_p$ . Notons

$$\mathcal{F}_{F_p/L} = f_p \mathcal{O}_L \quad \text{et} \quad \mathcal{F}_{F_{p^2}/L} = f_{p^2} \mathcal{O}_L$$

(avec  $f_p$  et  $f_{p^2}$  entiers d'après le point 1) du théorème 2.1) les conducteurs des extensions cycliques  $F_p/L$  de degré  $p$  et  $F_{p^2}/L$  de degré  $p^2$ . Soient  $\chi$  l'un des caractères primitifs associés à  $F_p/L$  et  $\chi_0$  le caractère modulaire associé à  $\chi$ . Puisque  $\chi^p$  est associé à  $F_p/L$ , alors  $\chi_0^p$  doit être de conducteur  $f_p$ . Selon la valeur de  $f_p$  ceci n'est pas toujours possible (voir paragraphe 2.2). Ainsi pour les indices 1, 2, 3, 5, 6, 8 et 10, nous obtenons qu'il n'existe aucun corps diédral  $F_{p^2}$  de degré  $2p^2$  contenant  $F_p$ .

• *Exemple (indice 1).* — Pour  $N_p \in \mathcal{D}_p$  d'indice 1 dans la table 1, il faudrait construire un caractère  $\chi_0$  primitif d'ordre 9 tel que  $\chi_0^3$  soit de conducteur 18. En particulier il faudrait construire un caractère primitif d'ordre 9 sur  $(\mathcal{O}_L/2^e \mathcal{O}_L)^*$  trivial sur  $(\mathbb{Z}/2^e \mathbb{Z})^*$ . Comme 2 est inerte dans  $L$ , d'après le théorème 2.3, ceci implique  $e = 1$  et  $2 \equiv -1 \pmod{9}$  : absurde.

De même, il faut que  $\chi_0(\varepsilon_L) = 1$ . Aussi pour les indices 4, 7 et 11, nous concluons qu'il n'existe aucun corps diédral  $F_{p^2}$  de degré  $2p^2$  contenant  $F_p$ .

• *Exemple (indice 4).* — Pour  $N_p \in \mathcal{D}_p$  d'indice 4 dans la table 1, nous avons  $\varepsilon_L = 5 + 2\sqrt{6}$ . Pour que  $\chi_0^3$  soit de conducteur 9, il faudrait que  $\chi_0$  admette une composante  $\chi_3$  primitive d'ordre 9 sur  $(\mathcal{O}_L/27\mathcal{O}_L)^*/(\mathbb{Z}/27\mathbb{Z})^*$ , toutes ses autres composantes étant primitives d'ordre 3. Pour que  $\chi_0(\varepsilon_L) = 1$  il faudrait donc que  $\chi_3(\varepsilon_L)$  soit une racine 3-ième de l'unité. Or  $(\mathcal{O}_L/27\mathcal{O}_L)^*/(\mathbb{Z}/27\mathbb{Z})^*$  étant engendré par  $\varepsilon_L$  d'ordre 9 et  $1 + 2\sqrt{24}$  d'ordre 3 et  $\chi_3$  étant d'ordre 9, alors  $\chi_3(\varepsilon_L)$  est une racine primitive 9-ième de l'unité. D'où l'impossibilité de construire  $F_{p^2}$ .  $\square$

THÉORÈME 5.2. — Si  $N_{p^2}$  est un corps diédral à multiplication complexe de degré  $4m = 2^r p^2$  avec  $p$  premier impair alors  $h_{N_{p^2}}^- > 1$ . Donc,

si  $N$  est un corps diédral à multiplication complexe de degré  $2^r \ell$  avec  $\ell$  impair et de nombre de classes relatif un alors  $\ell = 1$  ou  $\ell$  est premier.

*Preuve.* — La preuve est similaire à celle du théorème 4.1 où nous travaillons à  $M \in \mathcal{D}_2$  fixé, alors qu'ici nous travaillons à  $N_p \in \mathcal{D}_p$  d'indice 9, 12, 13, 14, 15, 16, 17, 18 et 19 (dans les tables 1 à 3) fixé (voir lemme 5.1). Supposons  $h_{N_{p^2}}^- = 1$  avec  $[N_{p^2} : \mathbb{Q}] = 2^r p^2$ . Alors  $h_{N_p}^- = 1$  et  $N_p$  est l'un des 9 corps cités précédemment. Les caractères de l'extension cyclique  $N_{p^2}^+/L$  sont de conducteur  $\mathcal{O}_L$ , de conducteur  $f_p \mathcal{O}_L$ , ou de conducteur  $f_{p^2} \mathcal{O}_L$  (car  $M^+/L$  est non ramifiée d'après le point 1 du lemme 3.4). Puisque  $f_p = 1$  ou  $f_p \geq e^{\mu_L}$ , la proposition 3.1 donne

$$\text{Res}_{s=1}(\zeta_{N_{p^2}}^+) \leq L(1, \chi_L)^{2^{r-2} p^2} \mu_L^{2^{r-2}-1} (\log f_p + \mu_L)^{2^{r-2}(p-1)} (\log f_{p^2} + c_L)^{2^{r-2}(p^2-p)},$$

avec  $c_L = \mu_L$  si  $f_{p^2} = 1$  ou  $f_{p^2} \geq e^{\mu_L}$ , et  $c_L = 2\mu_L$  sinon. Or  $d_{N_{p^2}} \geq d_{N_p}^2$  donc

$$(6) \quad h_{N_{p^2}}^- \geq C_{N_p} \frac{\varepsilon_{N_{p^2}}^+}{\log(d_L^{p^2} f_p^{2(p-1)} f_{p^2}^{2(p^2-p)})} \left( \frac{f_{p^2}}{\log f_{p^2} + c_L} \right)^{2^{r-2}(p^2-p)}$$

où

$$C_{N_p} = \frac{Q_M w_M}{2^{r-2} e^{\mu_L^{2^{r-2}-1}}} \left( \frac{\sqrt{d_L}}{4\pi^2 L(1, \chi_L)} \right)^{2^{r-2} p^2} \left( \frac{f_p}{\log f_p + \mu_L} \right)^{2^{r-2}(p-1)}.$$

Cette minoration est croissante avec  $f_{p^2}$  dès que  $f_{p^2} \geq 8 > e^2$ . Nous trouvons d'abord une borne entière  $B(N_p)$  pour laquelle  $f_{p^2} > B(N_p)$  donne  $h_{N_{p^2}}^- > 1$  dans la minoration (6). Puis pour chaque conducteur  $f_{p^2} \leq B(N_p)$  nous calculons effectivement  $h_{N_{p^2}}^-$  (voir tables 7 et 8). Nous concluons ainsi qu'il n'y a aucun corps diédral à multiplication complexe de degré  $2^r p^2$  de nombre de classes relatif un.

Prouvons maintenant la seconde partie du théorème. Supposons  $h_N^- = 1$  et  $\ell > 1$  non premier. Nous savons déjà d'après le point 4) du théorème 4.1 que  $\ell = p^s$  est alors puissance d'un premier  $p$  avec  $s \geq 2$ . Dans ce cas  $N$  posséderait un sous-corps diédral à multiplication complexe  $N_{p^2}$  de degré  $2^r p^2$  tel que  $h_{N_{p^2}}^- = 1$  (voir proposition 1.2). D'après la première partie du théorème, c'est impossible. □



## 6. Calcul des nombres de classes des sous-corps réels maximaux.

Expliquons comment nous calculons les  $P_K(X)$  et les  $h_{N_p^+}$  pour les trois corps diédraux  $N_p \in \mathcal{D}_p$  à multiplication complexe de nombre de classes relatif un d'indice 17, 18 et 19 des points 2) et 3) du théorème 4.1.

- $P_K(X) = X^5 - 35X^3 - 30X^2 + 10X + 4,$   
 $M = \mathbb{Q}(\sqrt{-2}, \sqrt{-35})$  et  $f_p = 5.$

Ce polynôme a été calculé par X. Roblot (voir [22], § 4.6) dans le cadre de sa thèse. Puisque  $h_M = 2$  et  $[N_p : M] = 5$  est impair, alors  $h_{N_p}$  est pair et donc  $h_{N_p^+} = h_{N_p} > 1$ . En fait un calcul avec le logiciel GP/PARI Calculator version 2.0.5 donne  $h_{N_p^+} = 2$  (mais ce calcul est valable seulement sous l'hypothèse de Riemann généralisée).

- $P_K(X) = X^5 + X^4 - 6X^3 - 5X^2 + 3X + 1,$   
 $M = \mathbb{Q}(\sqrt{-19}, \sqrt{-43})$  et  $f_p = 1.$

Ici  $N_p$  est le corps de classes de Hilbert au sens strict de  $L$ . Le polynôme a été obtenu dans les tables de [1]. Notons  $H_{N_p^+}$  le corps de classes de Hilbert de  $N_p^+$  et  $n_+$  le degré de  $H_{N_p^+}$  sur  $\mathbb{Q}$ . Nous avons donc  $n_+ = 10h_{N_p^+}$ . Si nous avions  $h_{N_p^+} \geq 7$  nous aurions  $n_+ > 68$  et d'après les bornes de A. Odlyzko (voir [21]), nous aurions

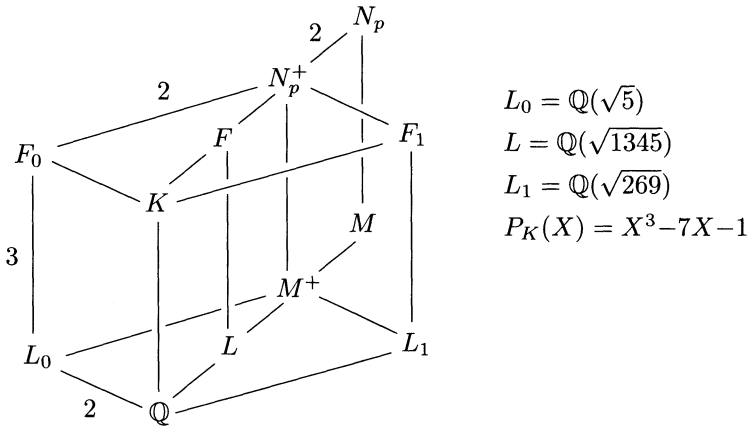
$$28,8 < d_{H_{N_p^+}}^{1/n_+} = \sqrt{d_L} = \sqrt{817} < 28,6.$$

D'où  $h_{N_p^+} \leq 6$ . Or  $Q_{N_p} = 2$  et  $h_{N_p^-} = 1$  donc  $h_{N_p^+}$  est impair (adapter dans la preuve du [23], th. 10.2, en utilisant que  $Q_N = 2$  implique l'injectivité de l'application  $C^+ \rightarrow C$ ). Comme  $N_p^+/L$  est cyclique de degré 5, que  $h_L = 5$  et que 3 est d'ordre 4 modulo 5, nous obtenons (voir [23], th. 10.8) que  $3 \mid h_{N_p^+}$  implique  $3^4 \mid h_{N_p^+}$ . Donc il ne reste plus comme valeur possible de  $h_{N_p^+}$  que 1 ou 5. Or le groupe des classes de  $L$  est cyclique d'ordre 5 donc 5 ne divise pas  $h_{N_p^+}$  (voir [10], prop. 11). D'où  $h_{N_p^+} = 1$ .

- $P_K(X) = X^3 - 7X - 1,$   
 $M = \mathbb{Q}(\sqrt{5}, \sqrt{269}, \sqrt{-(17 + 2\sqrt{5})})$  et  $f_p = 1.$

Ce polynôme a été obtenu dans les tables de [1]. En utilisant le même genre d'argument que dans le point précédent, nous pouvons montrer que  $h_{N_p^+} = 1$  ou 7, mais nous n'arrivons pas à éliminer la possibilité  $h_{N_p^+} = 7$ .

Il nous faut donc développer un autre raisonnement. Notons que  $h_{N_p^+}$  est impair. Nous sommes dans la situation suivante :



Notons  $\tilde{h}_k$  la partie impaire du nombre de classes d'un corps de nombre  $k$ . Nous avons :

$$\tilde{h}_{N_p^+}(\tilde{h}_K)^2 = \tilde{h}_{F_0}\tilde{h}_F\tilde{h}_{F_1}.$$

En utilisant le logiciel GP/PARI Calculator version 2.0.5 nous pouvons calculer, sans utiliser l'hypothèse de Riemann, les nombres de classes  $h_K$ ,  $h_{F_0}$ ,  $h_F$  et  $h_{F_1}$ . Nous obtenons que  $h_K = 1$ ,  $h_{F_0} = 1$ ,  $h_F = 2$  et  $h_{F_1} = 1$  et donc  $\tilde{h}_{N_p^+} = 1$  et,  $h_{N_p^+}$  étant impair, nous trouvons finalement  $h_{N_p^+} = 1$ .

## 7. Calculs de $h_{\bar{N}}$ .

### 7.1. Calculs de $L(0, \chi)$ .

Remarquons que nous avons seulement besoin de calculer  $h_{\bar{N}}$  pour des corps diédraux  $N$  de degré  $2^r p^s$  (voir point 4 du théorème 4.1). Soit donc  $N_{p^s}$  un corps à multiplication complexe diédral de degré  $4m = 2^r p^s$  et cyclique sur  $L$  quadratique réel. Rappelons (voir figure 1) que pour  $0 \leq k \leq s$  nous avons un sous-corps à multiplication complexe  $N_{p^k}$  diédral de degré  $2^r p^k$  et cyclique sur  $L$ , avec la convention  $N_{p^0} = M$ . D'après la proposition 1.2 le nombre de classes relatif  $h_{p^{k-1}}^-$  de  $N_{p^{k-1}}$  divise le nombre de classes relatif  $h_{p^k}^-$  de  $N_{p^k}$ . En notant  $\mathcal{X}_k$  l'ensemble des  $2^{r-2} p^{k-1} (p-1)$

caractères d'ordre  $2^{r-1}p^k$  associés à l'extension cyclique  $N_{p^k}/L$ , nous avons

$$(7) \quad \frac{h_{p^k}^-}{h_{p^{k-1}}^-} = \prod_{\chi \in \mathcal{X}_k} \frac{1}{4} L(0, \chi).$$

Or, d'après [5],  $L(0, \chi) \in \mathbb{Q}(\mathcal{X}_k)$ , où  $\mathbb{Q}(\mathcal{X}_k)$  désigne le corps cyclotomique engendré par les valeurs des  $\chi \in \mathcal{X}_k$ . Si nous définissons, pour  $\ell$  premier à  $2p$ ,  $\sigma_\ell \in \text{Gal}(\mathbb{Q}(\mathcal{X}_k)/\mathbb{Q})$  par  $\sigma_\ell(\zeta) = \zeta^\ell$  (pour n'importe quelle racine primitive de  $\mathbb{Q}(\mathcal{X}_k)$ ), nous avons  $\sigma_\ell(L(0, \chi)) = L(0, \chi^\ell)$  et la formule (7) s'écrit :

$$\frac{h_{p^k}^-}{h_{p^{k-1}}^-} = N_{\mathbb{Q}(\mathcal{X}_k)/\mathbb{Q}}\left(\frac{1}{4} L(0, \chi)\right),$$

où  $\chi$  est l'un quelconque des caractères de  $\mathcal{X}_k$ . De plus, puisque les  $m-1$  caractères irréductibles de degré 2 de tout groupe diédral  $D_{4m}$  sont à valeurs réelles, nous avons en fait  $L(0, \chi) \in \mathbb{Q}^+(\mathcal{X}_k)$  et donc

$$(8) \quad \frac{h_{p^k}^-}{h_{p^{k-1}}^-} = \left(N_{\mathbb{Q}^+(\mathcal{X}_k)/\mathbb{Q}}\left(\frac{1}{4} L(0, \chi)\right)\right)^2 = (h_{p^k/p^{k-1}}^-)^2$$

est le carré d'un entier.

Supposons que  $M \in \mathcal{D}_2$ . Le conducteur

$$\mathcal{F}_k = \text{ppcm}(\mathcal{F}_{F_{p^k}/L}, \mathcal{F}_{M/L}) = \infty_1 \infty_2 f_k \mathcal{O}_L$$

de n'importe quel  $\chi \in \mathcal{X}_k$  est entier et nous posons

$$A_k = \sqrt{\frac{d_L f_k^2}{\pi^2}} \quad \text{et} \quad a_n(\chi) = \sum_{N_{L/\mathbb{Q}}(\mathcal{I})=n} \chi(\mathcal{I}).$$

D'après [4], la constante d'Artin qui apparaît dans l'équation fonctionnelle de la fonction  $s \mapsto L(s, \chi)$  est égale à  $+1$ ,  $L(0, \chi)$ ,  $L(1, \chi)$  et les  $a_n(\chi)$  sont réels. Pour calculer des approximations numériques des  $L(0, \chi)$ ,  $\chi \in \mathcal{X}_k$ , desquelles nous déduirons  $h_{p^k}^-/h_{p^{k-1}}^-$  grâce à (7), nous utiliserons :

PROPOSITION 7.1 (voir [13]). — Posons  $K(B) = K_1(B) + K_2(B)$  avec

$$K_1(B) = 1 + 4 \sum_{n \geq 0} \left( \gamma + \log B - \frac{1}{2n+2} - \sum_{k=1}^n \frac{1}{k} \right) \frac{B^{2n+2}}{(2n+2)(n!)^2},$$

$$K_2(B) = \pi B + 4 \sum_{n \geq 0} \left( \gamma + \log B - \frac{1}{2n+1} - \sum_{k=1}^n \frac{1}{k} \right) \frac{B^{2n+2}}{(2n+1)(n!)^2}.$$

Alors  $0 \leq K(B) \leq 4e^{-B}$  et

$$0 < L(0, \chi) = \frac{A_k}{\pi} L(1, \chi) = \frac{A_k}{\pi} \sum_{n \geq 1} \frac{a_n(\chi)}{n} K\left(\frac{n}{A_k}\right).$$

Nous pouvons également trouver la valeur exacte de  $L(0, \chi)$ . La méthode est expliquée dans [14] et elle revient à calculer les entiers relatifs qui sont les coordonnées de  $w_M L(0, \chi) \in \mathbb{Z}[\mathcal{X}_k]$  (l'anneau des entiers de  $\mathbb{Q}(\mathcal{X}_k)$ ) dans une base quelconque de  $\mathbb{Z}[\mathcal{X}_k]$ . Grâce aux calculs de bonnes approximations de tous les  $L(0, \psi)$  lorsque  $\psi$  décrit  $\mathcal{X}_k$ , nous pouvons calculer de bonnes approximations de ces coordonnées qui sont entières et ainsi en déduire leurs valeurs exactes. Nous avons ainsi la valeur exacte de  $L(0, \chi)$  et en calculant sa norme nous trouvons  $h_{p^k/p^{k-1}}^-$  grâce à (8). Cette seconde approche n'est utilisée que lorsque les nombres de classes relatifs à calculer sont très grands (essentiellement pour le cas  $d_L = 745$  et  $p = 11$  de la table 5).

## 7.2. Calculs des $a_n(\chi)$ .

Rappelons que nous n'avons besoin d'effectuer le calcul de  $h_N^-$  que pour des  $N = N_{p^s}$  de degré  $2^r p^s$  avec  $p$  premier impair (voir point 4 du théorème 4.1). Nous expliquons dans ce cas comment calculer les  $a_n(\chi)$  où  $\chi$  est l'un quelconque des caractères primitifs associés à  $N_{p^s}/L$ . Nous aurons besoin d'un lemme préliminaire pour le faire.

LEMME 7.2.

1) Soient  $F_{p^s}$  un corps diédral de degré  $2p^s$ ,  $p$  premier impair et  $s \geq 1$  entier, cyclique sur le corps quadratique réel  $L$ , et  $q$  un nombre premier.

(a) Supposons  $q$  ramifié dans  $L : q\mathcal{O}_L = \mathcal{Q}^2$ .

(i) Si  $q$  est distinct de  $p$  alors  $\mathcal{Q}$  est totalement décomposé dans  $F_{p^s}/L$ .

(ii) Si  $q = p$  et si  $\mathcal{Q}$  n'est pas ramifié dans  $F_{p^s}/L$  alors  $\mathcal{Q}$  est totalement décomposé dans  $F_{p^s}/L$ .

(b) Supposons  $q$  inerte dans  $L : q\mathcal{O}_L = \mathcal{Q}$ . Alors, si  $\mathcal{Q}$  n'est pas ramifié dans  $F_{p^s}/L$ ,  $\mathcal{Q}$  est totalement décomposé dans  $F_{p^s}/L$ .

2) Soient  $M \in \mathcal{D}_2$  cyclique sur le corps quadratique réel  $L$  et  $q$  un premier inerte dans  $L : q\mathcal{O}_L = \mathcal{Q}$ . Si  $\mathcal{Q}$  n'est pas ramifié dans  $M/L$ , alors  $\mathcal{Q}$  est totalement décomposé dans  $M/L$ .

*Preuve.*

1) Soit  $f_{p^s} \mathcal{O}_L$  avec  $f_{p^s} \geq 1$  le conducteur de l'extension  $F_{p^s}/L$ .

(a) Si  $q \neq p$ , le théorème 2.3 donne que  $q$  ne divise pas  $f_{p^s}$ , et  $\mathcal{Q}$  n'est donc pas ramifié dans  $F_{p^s}/L$ . Soit alors  $\chi$  l'un des caractères primitifs associés à  $F_{p^s}$ . D'après le point 1) du théorème 2.1,  $\chi$  est trivial sur  $P_{L, \mathbb{Z}}((f_{p^s}))$ , et donc  $\chi(\mathcal{Q})^2 = \chi((q)) = 1$  d'où  $\chi(\mathcal{Q}) = \pm 1$  et  $\chi$  étant à valeurs dans les racines  $p^s$ -ième de l'unité avec  $p$  impair, on obtient  $\chi(\mathcal{Q}) = 1$ , et  $\mathcal{Q}$  est totalement décomposé dans  $F_{p^s}/L$ .

(b) Si  $\mathcal{Q}$  n'est pas ramifié dans  $F_{p^s}/L$ , la même méthode donne  $\chi(\mathcal{Q}) = \chi((q)) = 1$ , et  $\mathcal{Q}$  est totalement décomposé dans  $F_{p^s}/L$ .

2) Si le degré de  $M$  est supérieur à 8, on sait qu'alors  $M$  est le 2-corps de Hilbert au sens strict de  $L$ . Comme  $\mathcal{Q}$  est principal au sens strict, il est totalement décomposé dans  $M/L$ . Sinon  $M$  est biquadratique bicyclique et le lemme est alors évident.  $\square$

Soit  $N_{p^s} = MF_{p^s}$  un corps diédral à multiplication complexe de degré  $2^r p^s$ ,  $p$  premier impair, cyclique sur le corps quadratique réel  $L$  et où  $M \in \mathcal{D}_2$  est de degré  $2^r$  et  $F_{p^s}$  est diédral de degré  $2p^s$ . Soit  $\chi$  l'un quelconque des caractères primitifs associés à  $N_{p^s}/L$  de conducteur  $\infty_1 \infty_2 f \mathcal{O}_L$  qui est entier. En fait  $\chi = \chi_+ \chi_-$  où  $\chi_+$  est un caractère primitif associé à  $F_{p^s}/L$  et  $\chi_-$  est un caractère primitif associé à  $M/L$ .

**THÉORÈME 7.3.** — *Conservons les notations précédentes. La fonction  $n \mapsto a_n(\chi)$  étant multiplicative (i.e. si  $n_1$  et  $n_2$  sont premiers entre eux alors  $a_{n_1 n_2}(\chi) = a_{n_1}(\chi) a_{n_2}(\chi)$ ), il suffit de connaître les  $a_{q^k}(\chi)$  quand  $q$  est un nombre premier, et nous avons :*

1) Si  $q|f$  alors  $a_{q^k}(\chi) = 0$ .

2) Si  $q \nmid f$  et  $q\mathcal{O}_L = \mathcal{Q}$  alors  $\chi_+(\mathcal{Q}) = \chi_-(\mathcal{Q}) = 1$  et donc

$$a_{q^k}(\chi) = \begin{cases} 0 & \text{si } k \text{ impair,} \\ 1 & \text{si } k \text{ pair.} \end{cases}$$

3) Si  $q \nmid f$  et  $q\mathcal{O}_L = \mathcal{Q}^2$  alors  $\chi_+(\mathcal{Q}) = 1$ ,  $\chi_-(\mathcal{Q}) = \pm 1$  et donc

$$a_{q^k}(\chi) = \chi_-(\mathcal{Q})^k = \pm 1.$$

4) Si  $q \nmid f$  et  $q\mathcal{O}_L = \mathcal{Q}\mathcal{Q}'$  nous avons

$$a_{q^k}(\chi) = \sum_{\ell=0}^k \chi(\mathcal{Q})^\ell \chi(\mathcal{Q}')^{k-\ell} = \chi(\mathcal{Q})^{-k} \sum_{\ell=0}^k \chi(\mathcal{Q})^{2\ell}$$

$$= \begin{cases} (k+1) & \text{si } \chi(\mathcal{Q}) = 1, \\ (-1)^k(k+1) & \text{si } \chi(\mathcal{Q}) = -1, \\ \text{im}(\chi(\mathcal{Q})^{k+1})/\text{im}(\chi(\mathcal{Q})) & \text{sinon.} \end{cases}$$

*Preuve.* — Prouvons les trois derniers points. Si  $q$  est inerte dans  $L$ , le lemme 7.2 donne  $\chi_+(\mathcal{Q}) = \chi_-(\mathcal{Q}) = 1$ , ce qui prouve le point 2). Si  $q$  est ramifié dans  $L$  et  $\mathcal{Q}$  n'est pas ramifié dans  $F_{p^s}/L$ , le lemme 7.2 donne

$$\chi_+(\mathcal{Q}) = 1.$$

Comme  $\mathcal{Q}^2$  est principal strict et non ramifié dans  $M/L$  alors

$$\chi_-(\mathcal{Q}) = \pm 1.$$

Donc  $\chi(\mathcal{Q}) = \chi_-(\mathcal{Q}) = \pm 1$ , ce qui prouve le point 3). Enfin si  $q$  est décomposé dans  $L$ , comme  $\chi_+$  est trivial sur  $P_{L,\mathbb{Z}}((f_{p^s}))$  et  $\mathcal{Q}$  n'est pas ramifié dans  $F_{p^s}/L$ , on a

$$\chi_+(\mathcal{Q}\mathcal{Q}') = 1.$$

De même, comme  $\mathcal{Q}\mathcal{Q}' = q\mathcal{O}_L$  est principal strict et  $\mathcal{Q}$  n'est pas ramifié dans  $M/L$ , alors

$$\chi_-(\mathcal{Q}\mathcal{Q}') = 1.$$

Donc  $\chi(\mathcal{Q}\mathcal{Q}') = 1$  et  $\chi(\mathcal{Q}') = \chi(\mathcal{Q})^{-1}$  d'où le dernier point.  $\square$

Les calculs des  $\chi_+(\mathcal{Q})$  sont expliqués au paragraphe 2. Les calculs des  $\chi_-(\mathcal{Q})$  avec  $M \in \mathcal{D}_2$ , sont très simples. Soient  $q$  un nombre premier et  $\mathcal{Q}$  un idéal entier de  $L$  au-dessus de  $q$ . Nous avons :

1) Quand  $[M : \mathbb{Q}] = 4$ , soient  $L_0$  et  $L_1$  les deux sous-corps quadratiques imaginaires de  $M$ . Si  $\chi_{L_0}(q) = \chi_{L_1}(q) = 0$  alors  $\chi_-(\mathcal{Q}) = 0$ . Sinon posons  $\sigma = \chi_{L_0}(q) + \chi_{L_1}(q)$ . Si  $\sigma = 0$  alors  $\chi_-(\mathcal{Q}) = 1$  sinon  $\chi_-(\mathcal{Q}) = \text{signe}(\sigma)$ .

2) Quand  $[M : \mathbb{Q}] = 2^r \geq 8$ ,  $M$  est le 2-corps de classes de Hilbert au sens strict de  $L$ . Soit alors  $I_2$  un générateur du 2-Sylow du groupe des classes au sens strict de  $L$ . Nous avons alors  $h_L = 2^{r-2}h$  avec  $h$  impair, donc il existe  $h'$  tel que  $hh' \equiv 1 \pmod{2^{r-1}}$ . Dans ce cas il existe un unique  $v_{\mathcal{Q}} \in \{0, \dots, 2^{r-1} - 1\}$ , tel que  $\mathcal{Q}^h I_2^{v_{\mathcal{Q}}}$  soit principal au sens strict et alors  $\chi_-(\mathcal{Q}) = \exp(-2ih'v_{\mathcal{Q}}\pi/2^{r-1})$ .

## 8. Exemple.

Nous allons ici reprendre sur un exemple toutes les étapes de la détermination des corps à multiplication complexe diédraux de nombre de classes relatif un à  $M \in \mathcal{D}_2$  fixé. Dans tout ce paragraphe fixons

$$M = \mathbb{Q}\left(\sqrt{5}, \sqrt{269}, \sqrt{-(17 + 2\sqrt{5})}\right) \in \mathcal{D}_2,$$

le 2-corps de Hilbert au sens strict de  $L = \mathbb{Q}(\sqrt{1345})$ .

Alors  $h_L = 6$  et  $\varepsilon_L = 4841 + 132\sqrt{1345}$ . Nous avons donc :

$p$	3	5	7	11	13
$f_L(p)$	1	11	113	419	103
$F_L(p)$	1	11	103	103	103

Nous avons  $\mu_L \leq 1,060$  et  $L(1, \chi_L) \leq 3,004$ . Avec les notations du lemme 3.6, nous avons donc  $b_L = \log \sqrt{1345}$ . Nous trouvons que  $\alpha_L(103) = 3,86\dots > e^{1/11}$ . De plus la minoration (4) avec  $p = 7$  et  $f = F_L(7) = 103$  donne  $h_{N_p}^- > 1,1$ . Si  $N_p$  est un corps diédral à multiplication complexe de degré  $2^r p$  contenant  $M$  et si  $p \geq 7$  alors  $h_{N_p}^- > 1,1$ .

Maintenant pour  $p = 3$  ou  $5$ , cherchons tous les corps  $N_p$  diédraux à multiplication complexe de degré  $2^r p = 8p$  contenant  $M$  et de nombre de classes relatif un.

Nous avons alors, avec les notations de la minoration (5),  $f_{M/L} = 1$ ,  $w_M = 2$  et  $Q_M = 2$ . Nous trouvons ainsi que  $B(M, 3) = 125$ ,  $B(M, 5) = 43$ .

Les conducteurs possibles pour  $F_p$  inférieurs à ces bornes sont :

pour  $p = 3$ ,  $f_3 = 1$  et  $f_3 = 101$ ;

pour  $p = 5$ ,  $f_5 = 11$ .

Or  $p = 3$  ne divise pas  $w_M = 2$ . Comme 101 est inerte dans  $L$ , il est totalement décomposé dans  $M/L$  et en particulier dans  $M/M^+$ . La proposition 4.2 permet donc de dire que, si  $f_3 = 101$ , alors 3 divise  $h_{N_3}^-$  et donc  $h_{N_3}^- > 1$ .

Il ne nous reste donc que deux calculs de nombres de classes relatifs à effectuer :

pour  $p = 3$  et  $f_3 = 1$ , nous avons  $h_{N_3}^- = 1$ ;

pour  $p = 5$  et  $f_5 = 11$ , nous avons  $h_{N_5}^- = 2641^2$ .

Il n'existe donc qu'un seul corps à multiplication complexe diédral de degré  $2^r p$  contenant  $M$  et de nombre de classes relatif un : le corps de Hilbert au sens strict  $N_3$  de  $L$  qui est de degré 24. Cherchons tous les corps  $N_9$  diédraux à multiplication complexe de degré 72 contenant ce  $N_3$  et de nombre de classes relatif un.

Pour cela nous utilisons la minoration (6). Nous trouvons que la borne  $B(N_3)$  sur les conducteurs  $f_9$  est  $B(N_3) = 55$ . Le seul conducteur possible inférieur à cette borne est : 47. Nous effectuons le calcul du nombre de classes relatif (voir table 8) et nous trouvons que  $h_{N_9}^-$  est strictement supérieur à 1.

Donc il n'y a aucun corps diédral à multiplication complexe de degré 72 contenant  $N_3$  et de nombre de classes relatif un. Finalement  $N_3$  est le seul corps à multiplication complexe diédral de nombre de classes relatif un contenant  $M$ .

## 9. Tables de nombres de classes relatifs.

Dans les tables 4, 5 et 6, nous donnons la liste des corps à multiplication complexe  $N_p$  diédraux de degrés respectifs  $4p$ ,  $8p$  et  $16p$  (avec  $p$  premier impair) cycliques sur le corps quadratique réel  $L$ , pour lesquels nous avons dû calculer effectivement  $h_{N_p}^-$ . Rappelons que pour le degré 12, les tables ne sont pas données uniquement parce qu'elles sont trop longues. Ces corps  $N_p = MF_p$  sont entièrement définis par la donnée de  $M$ , de  $p$  et du conducteur  $f_p \mathcal{O}_L$  de  $F_p/L$ , où  $M = \mathbb{Q}(\sqrt{d_{L_0}}, \sqrt{d_{L_1}})$  est biquadratique bicyclique quand  $[N_p : \mathbb{Q}] = 4p$  et  $M$  est le 2-corps de classes strictes de Hilbert de  $L$  quand  $[N_p : \mathbb{Q}] = 8p$  ou  $16p$ . Ces tables permettent de finir la preuve du théorème 4.1. Remarquons que dans ces tables, seules apparaissent les situations décrites aux points 1) et 2) b du théorème 2.2. La seule fois où nous nous sommes trouvés dans la situation du point 2) a du théorème 2.2, c'est dans le cas suivant :

$$M = \mathbb{Q}(\sqrt{-19}, \sqrt{-267}), \quad p = 3 \quad \text{et} \quad f_p = 9$$

pour lequel il existe trois corps diédraux à multiplication complexe vérifiant ces conditions, de nombre de classes relatif 7, 19 et 23 respectivement.



Pour les tables suivantes  $N_p$  est un corps à multiplication complexe diédral de degré  $2^r p$  cyclique sur le corps quadratique réel  $L$  et de nombre de classes relatif un qui peut être inclus dans un corps à multiplication complexe diédral de degré  $2^r p^2$  (*i.e.*  $N_p$  est l'un des corps indicés en gras décrits dans le théorème 4.1). Notons  $\mathcal{F}_{N_p/L} = f_p \mathcal{O}_L$ . Les tables 7 et 8 donnent la borne  $B(F_p)$  sur le conducteur  $f_{p^2} \mathcal{O}_L = \mathcal{F}_{F_{p^2}/L}$  pour laquelle  $f_{p^2} > B(F_p)$  implique  $h_{N_{p^2}}^- > 1$  dans la minoration (6) et tous les conducteurs  $f_{p^2}$  inférieurs à cette borne pour lesquels nous avons du calculer effectivement  $h_{N_{p^2}}^-$ . Ces tables permettent de prouver le théorème 5.2.

$d_L$	$d_{L_0}$	$d_{L_1}$	$p$	$f_p$	$h_{N_p}^-$	$d_L$	$d_{L_0}$	$d_{L_1}$	$p$	$f_p$	$h_{N_p}^-$
12	-3	-4	5	71	$11^2$	489	-3	-163	5	25	$164^2$
21	-3	-7	5	101	$269^2$	536	-8	-67	5	25	$181^2$
28	-4	-7	5	131	$1789^2$	645	-43	-15	5	5	$11^2$
56	-7	-8	5	31	$151^2$	652	-4	-163	5	11	$44^2$
60	-3	-20	5	55	$109^2$	696	-3	-232	5	11	$16^2$
60	-3	-20	5	131	$461^2$	705	-3	-235	5	11	$31^2$
60	-3	-20	7	71	$1651^2$	705	-3	-235	7	29	$2813^2$
60	-4	-15	5	131	$3061^2$	737	-11	-67	5	41	$1616^2$
60	-4	-15	7	71	$23773^2$	817	-19	-43	5	1	1
76	-4	-19	5	31	$29^2$	861	-7	-123	7	7	$169^2$
105	-3	-35	5	41	$361^2$	940	-4	-235	5	31	$596^2$
105	-7	-15	5	41	$19^2$	988	-19	-52	5	41	$1109^2$
120	-8	-15	5	101	$6219^2$	1340	-67	-20	5	11	$49^2$
129	-3	-43	5	131	$549^2$	1720	-43	-40	5	5	$11^2$
201	-3	-67	5	41	$229^2$	1869	-7	-267	7	7	$463^2$
264	-11	-24	5	61	$539^2$	2345	-67	-35	5	5	$41^2$
264	-11	-24	7	43	$7351^2$	5705	-163	-35	7	7	$3053^2$
280	-7	-40	5	5	$31^2$	6097	-67	-91	7	1	$8^2$
280	-8	-35	5	5	1	7009	-43	-163	5	25	$6611^2$
345	-3	-115	5	55	$369^2$	7705	-67	-115	5	1	$9^2$
364	-4	-91	5	11	$11^2$	14833	-163	-91	5	11	$1829^2$
456	-19	-24	5	41	$79^2$	18361	-43	-427	7	7	$1597^2$
469	-7	-67	5	41	$891^2$	18745	-163	-115	5	11	$1844^2$
473	-11	-43	7	29	$13861^2$	28609	-67	-427	7	1	$113^2$

Table 4 :  $[N_p : \mathbb{Q}] = 4p$  avec  $p \geq 5$  premier

$d_L$	$p$	$f_p$	$h_{N_p}^-$	$d_L$	$p$	$f_p$	$h_{N_p}^-$
136	3	61	$1300^2$	1345	3	1	1
136	3	163	$8926^2$	1345	5	11	$2641^2$
136	3	277	$19702^2$	1537	3	7	$73^2$
136	3	333	$39412^2$	1537	3	19	$694^2$
136	3	379	$40996^2$	1537	3	79	$15517^2$
205	3	31	$382^2$	1537	3	117	$22453^2$
205	3	61	$1744^2$	1537	3	133	$13156^2$
205	3	63	$1417^2$	1864	3	7	$22^2$
205	3	67	$1702^2$	1864	3	43	$1300^2$
205	3	91	$3601^2$	1864	5	11	$3821^2$
205	3	97	$2950^2$	1945	3	9	$49^2$
205	3	117	$5014^2$	2041	3	63	$9661^2$
221	3	37	$472^2$	2041	3	73	$9286^2$
221	3	43	$628^2$	2248	3	13	$166^2$
305	3	7	$22^2$	2248	3	19	$421^2$
377	3	37	$793^2$	2248	3	31	$352^2$
377	3	73	$1342^2$	2248	5	11	$12841^2$
377	5	31	$161996^2$	2329	3	9	$286^2$
545	3	37	$649^2$	2329	5	31	$4517276^2$
545	3	61	$1549^2$	2353	3	63	$3352^2$
545	3	103	$4534^2$	4369	3	37	$7822^2$
712	3	61	$718^2$	4369	3	63	$2488^2$
745	3	9	$16^2$	4369	3	91	$48889^2$
745	3	193	$17656^2$	7081	3	13	$436^2$
745	3	223	$21229^2$	7081	3	61	$54424^2$
745	5	5	$281^2$	7081	3	63	$34648^2$
745	11	23	$337893598681^2$				

Table 5 :  $[N_p : \mathbb{Q}] = 8p$  avec  $p \geq 3$  premier

$d_L$	$p$	$f_p$	$h_{N_p}^-$	$d_L$	$p$	$f_p$	$h_{N_p}^-$
505	3	9	$1726^2$	793	3	31	$470062^2$
505	3	127	$80578777^2$	793	3	63	$7485838^2$
505	3	133	$70159198^2$	793	3	103	$62841169^2$
505	3	163	$187048174^2$	793	3	151	$261102046^2$
505	3	217	$611206366^2$	2056	3	31	$344358^2$
689	3	19	$40825^2$				

Table 6 :  $[N_p : \mathbb{Q}] = 16p$  avec  $p \geq 3$  premier

$d_L$	$\mu_L \leq L(1, \chi_L) \leq$	$d_{L_0}$	$d_{L_1}$	$p$	$f_p$	$B(F_p)$	$f_{p^2}$	$h_{N_{p^2}}^-$	
105	0, 531	1, 721	-7	-15	3	9	190	27	$163^2$
280	0, 857	1, 487	-8	-35	5	5	30	-	-
469	1, 090	1, 157	-7	-67	3	1	40	13	$712^2$
469	1, 090	1, 157	-7	-67	3	1	40	18	$657^2$
469	1, 090	1, 157	-7	-67	3	1	40	22	$1539^2$
469	1, 090	1, 157	-7	-67	3	1	40	34	$4833^2$
473	1, 170	1, 424	-11	-43	3	1	60	31	$11289^2$
473	1, 170	1, 424	-11	-43	3	1	60	35	$15336^2$
473	1, 170	1, 424	-11	-43	3	1	60	45	$20331^2$
817	1, 093	2, 285	-19	-43	5	1	30	-	-
940	1, 153	1, 770	-4	-235	3	1	50	23	$2943^2$
940	1, 153	1, 770	-4	-235	3	1	50	29	$5679^2$
1304	1, 634	1, 077	-8	-163	3	1	20	9	$171^2$
1304	1, 634	1, 077	-8	-163	3	1	20	13	$901^2$
1708	1, 629	1, 400	-4	-427	3	1	25	-	-

Table 7 :  $[N_{p^2} : \mathbb{Q}] = 4p^2$  avec  $p \geq 3$  premier

$d_L$	$\mu_L \leq L(1, \chi_L) \leq$	$p$	$f_p$	$B(F_p)$	$f_{p^2}$	$h_N^-$
1345	1,060      3,004	3	1	55	47	2613971736 <sup>2</sup>

Table 8 :  $[N_{p^2} : \mathbb{Q}] = 8p^2$  avec  $p \geq 3$  premier

## BIBLIOGRAPHIE

- [1] H. COHEN, F. DIAZ Y DIAZ, M. OLIVIER, Computing ray class groups, conductors and discriminants, Actes du Colloque ANTS II, Talence, 1996.
- [2] S. CHOWLA, Note on Dirichlet's  $L$ -functions, Acta Arith., 1 (1936), 113–114.
- [3] S. CHOWLA, M.J. DELEON, P. HARTUNG, On a hypothesis implying the non-vanishing of Dirichlet's  $L$ -series  $L(s, \chi)$  for  $s > 0$ , J. reine angew. Math., 262/263 (1973), 415–419.
- [4] A. FRÖHLICH, J. QUEYRUT, On the functional equation of the Artin  $L$ -function for characters of real representations, Invent. Math., 20 (1973), 125–138.
- [5] H. HIDA, Elementary theory of  $L$ -functions and Eisenstein series, London Math. Soc., Student Texts, Cambridge University Press, 26 (1993).
- [6] J. HOFFSTEIN, Some analytic bounds for zeta functions and class numbers, Invent. Math., 55 (1979), 37–47.
- [7] Y. LEFEUVRE, Corps à multiplication complexe diédraux principaux, Thèse, Univ. Caen, soutenue le 28 juin 1999.
- [8] Y. LEFEUVRE, S. LOUBOUTIN, The class number one problem for the dihedral CM-fields, to appear in the Proceedings of Conference on Algebraic Number Theory and Diophantine Analysis, Gras, 1998.
- [9] S. LOUBOUTIN, Lower bounds for relative class numbers of CM-fields, Proc. Amer. Math. Soc., 120 (1994), 425–434.
- [10] S. LOUBOUTIN, Corps quadratiques principaux à corps de classes de Hilbert principaux et à multiplication complexe, Acta Arith., 74 (1996), 121–140.
- [11] S. LOUBOUTIN, Majorations explicites du résidu au point 1 des fonctions zêta de certains corps de nombres, J. Math. Soc. Japan, 50 (1998), 57–69.
- [12] S. LOUBOUTIN, Upper bounds on  $|L(1, \chi)|$  and applications, Canad. J. Math., 50 (1998), 795–815.
- [13] S. LOUBOUTIN, Computation of relative class numbers of CM-fields by using Hecke  $L$ -functions, Math. Comp., 69 (1999), 371–393.
- [14] S. LOUBOUTIN, Computation of  $L(0, \chi)$  and of relative class numbers of CM-fields, Preprint Univ. Caen, 1998.
- [15] S. LOUBOUTIN, 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.

- [16] S. LOUBOUTIN, R. OKAZAKI, The class number one problem for some non-abelian normal CM-fields of 2-power degrees, Proc. London Math. Soc., 76 (3) (1998), 523–548.
- [17] S. LOUBOUTIN, R. OKAZAKI, M. OLIVIER, The class number one problem for some non-abelian normal CM-fields, Trans. Amer. Math. Soc., 349 (1997), 3657–3678.
- [18] S. LOUBOUTIN, Y.H. PARK, Y. LEFEUVRE, Construction of the real dihedral number fields of degree  $2p$ . Applications, Acta Arith., 89 (1999), 201–215.
- [19] J. MARTINET, Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre  $2p$ , Ann. Inst. Fourier Grenoble, 19, 1 (1969), 1–80.
- [20] A.M. ODLYZKO, Some analytic estimates of class numbers and discriminants, Invent. Math., 29 (1975), 279–286.
- [21] A.M. ODLYZKO, On conductors and discriminants, Algebraic number fields, Durham Symposium, 1975, A. Fröhlich, éd., Academic Press (1977), 377–407.
- [22] X.F. ROBLLOT, Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction des corps de classes de rayon, Thèse, Univ. Bordeaux, 1997.
- [23] L.C. WASHINGTON, Introduction to cyclotomic fields, Springer-Verlag, Graduate Texts in Mathematics 83, second edition, 1997.
- [24] K. YAMAMURA, The determination of the imaginary abelian number fields with class number one, Math. Comp., 62 (1994), 899–921.

Manuscrit reçu le 19 février 1999,  
accepté le 6 juillet 1999.

Yann LEFEUVRE,  
Université de Caen  
Département de Mathématiques  
Campus II  
BP 5186  
14032 Caen cedex (France).  
lefeuvre@math.unicaen.fr