



HAL
open science

Groupes de classes de corps de type CM

Francesco Amoroso

► **To cite this version:**

| Francesco Amoroso. Groupes de classes de corps de type CM. 2005. hal-00004664

HAL Id: hal-00004664

<https://hal.science/hal-00004664>

Preprint submitted on 11 Apr 2005

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Groupes de classes de corps « de type CM »

Francesco AMOROSO

*Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen, Campus II, BP 5186
14032 Caen Cédex, France*

1 Introduction.

Soit K un corps CM de degré d ; notons $|\Delta|$ la valeur absolue de son discriminant et k le sous-corps de K fixé par la conjugation complexe J . Soient aussi h_K et h_k les nombres de classes de K et k respectivement; notons également $e_{K/k}$ l'exposant relatif du groupe de classes de K par rapport à celui de k , *i. e.* le plus petit entier e tel que pour tout idéal I de K , il existe $\alpha \in K$ tel que $(\alpha)I^e$ soit l'extension d'un idéal fractionnaire de k . Dans [Am-Dv] nous avons obtenu¹ les minoration suivantes pour $e_{K/k}$ et h_K/h_k :

Théorème 1.1 *Soit K un corps CM et $\varepsilon > 0$; ils existent alors trois constantes $C, C_\varepsilon > 0$ et $H_\varepsilon > 1$ telles que, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K ,*

$$e_{K/k} \geq \max \left(\frac{C \log |\Delta|}{d \log \log |\Delta|}, C_\varepsilon d^{1-\varepsilon} \right)$$

et

$$\frac{h_K}{h_k} \geq \max (|\Delta|^{C/d}, H_\varepsilon^{d^{1-\varepsilon}}) .$$

Nous nous proposons de généraliser ce théorème dans deux directions différentes. D'abord, les techniques de [Am-Dv] s'appliquent également à l'étude de l'anneau du groupe de classes. Notons Γ le groupe de \mathbb{Q} -automorphismes de K et

$$\mathbb{Z}[\Gamma]^\pm = \{\psi \in \mathbb{Z}[\Gamma] \text{ t.q. } \psi(1 \mp J) = 0\}$$

¹les résultats dans op.cit sont légèrement moins précis : on trouvera une preuve du théorème 1.1 dans le paragraphe 5. Signalons également que la minoration pour h_K/h_k est légèrement plus faible de celle obtenue dans [Od].

Notons également $\mathcal{Cl}^-(K)$ le groupe de classe relatif de $\mathcal{Cl}(K)/j\mathcal{Cl}(k)$, où j est le morphisme d'extension, et

$$\text{Ann}(\mathcal{Cl}^-(K))^- = \text{Ann}(\mathcal{Cl}^-(K)) \cap \mathbb{Z}[\Gamma]^-$$

l'ensemble des $\psi \in \mathbb{Z}[\Gamma]^-$ tels que pour tout idéal I de K , il existe $\alpha \in K$ tel que $(\alpha)I^\psi$ soit l'extension d'un idéal fractionnaire de k .

On montre alors :

Théorème 1.2 *Soit K un corps CM et $\varepsilon > 0$; ils existent alors deux constantes $C > 0$ et $H_\varepsilon > 1$ telle que, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K ,*

$$[\mathbb{Z}[\Gamma]^- : \text{Ann}(\mathcal{Cl}^-(K))^-] \geq \max \left(\left(\frac{C \log |\Delta|}{dd_0 \log \log |\Delta|} \right)^{d_0/2}, H_\varepsilon^{d_0^{1-\varepsilon}} \right),$$

où $d_0 = \text{Card}(\Gamma)$.

Ensuite, nous nous proposons d'élargir la famille des corps auxquels nos méthodes s'appliquent. Par exemple, soit α un nombre de Salem; notons $K = \mathbb{Q}(\alpha)$ et $k = \mathbb{Q}(\alpha + \alpha^{-1})$. Alors, en conservant les notations introduites précédemment,

Théorème 1.3 *Soit $\varepsilon > 0$; ils existent trois constantes $C, C_\varepsilon > 0$ et $H_\varepsilon > 1$ telles que, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K ,*

$$e_{K/k} \geq \frac{\max(C \log |\Delta|, C_\varepsilon d^{1-\varepsilon})}{\log \log |\Delta| + \log(2 + \log \alpha)}$$

et :

$$\frac{h_K}{h_k} \geq \frac{\max(|\Delta|^{C/d}, H_\varepsilon^{d^{1-\varepsilon}})}{2 + \log \alpha}.$$

Signalons que la minoration pour h_K/h_k est légèrement plus faible de celle obtenue dans [Ch] avec des méthodes différentes.

Notons comme auparavant Γ le groupe des \mathbb{Q} -automorphismes de K et soit E_K le groupe des unités. Plus généralement, nous montrerons dans la proposition technique 3.1 que nos résultats s'appliquent dès qu'il existe $\phi \in \mathbb{Z}[\Gamma]$ tel que

$$\|\phi\|_1 \times \text{rang}(E_K^\phi) = o(d),$$

où $\|\phi\|_1$ est la somme des modules des coefficients de ϕ .

Remerciements. *Je tiens à remercier Bruno Anglès et John Boxall pour plusieurs discussions au sujet de cet article. C'est également un plaisir de remercier Corentin Pontreau qui a bien voulu me faire part de ses commentaires sur une version initiale de ce travail.*

2 Géométrie des nombres.

Soit K un corps de nombres; pour toute place $v \in M_K$ de K on note $d_v = [K_v : \mathbb{Q}_v]$ et $|\cdot|_v$ la valeur absolue v -adique, normalisée de telle sorte que la formule du produit :

$$\prod_v |\alpha|^{d_v} = 1, \quad \alpha \in K^*$$

soit satisfaite. Soit Γ le groupe des \mathbb{Q} -automorphismes de K . Pour $\phi = \sum_{\tau \in \Gamma} \phi_\tau \tau \in \mathbb{Z}[\Gamma]$, on note

$$\|\phi\|_1 = \sum_{\tau \in \Gamma} |\phi_\tau|$$

et, si $\alpha \in K$,

$$\alpha^\phi = \prod_{\tau \in \Gamma} (\tau\alpha)^{\phi_\tau}.$$

On note également r_ϕ le rang du sous-groupe E_K^ϕ de E_K et

$$\delta_\phi = \min_{v_1, \dots, v_r \in E_K^\phi} \{h(v_1) + \dots + h(v_r)\}$$

où le minimum est pris sur les familles d'unités de E_K^ϕ multiplicativement indépendantes.

La proposition suivante généralise la proposition 2.3 de [Am]; sa preuve est une généralisation de la preuve de cette dernière.

Proposition 2.1 *Soient K, Γ comme auparavant. Soit $\phi \in \mathbb{Z}[\Gamma]$, $\phi \neq 0$ et notons $r = r_\phi$ et $\delta = \delta_\phi$. Soient ensuite $x \geq 1$ un réel et $t \geq 2$ un entier. Supposons qu'il existe des entiers algébriques non nuls $\gamma_1, \dots, \gamma_t$ de K tels que $|N_{\mathbb{Q}}^K \gamma_j| \leq x$ ($j = 1, \dots, t$). Soient ensuite m et N deux entiers strictement positifs et tels que :*

$$mN^r < t.$$

Alors il existe $m+1$ indices $j_0, j_1, \dots, j_m \in \{1, \dots, t\}$ deux à deux distincts et des unités $v_1, \dots, v_m \in E_K^\phi$ tels que :

$$h(v_s \gamma_{j_s}^\phi \gamma_{j_0}^{-\phi}) \leq \frac{\|\phi\|_1 \log x}{[K : \mathbb{Q}]} + \frac{\delta}{N}$$

pour $s = 1, \dots, m$.

Démonstration. Notons $\mathcal{L} : K^* \rightarrow \mathbb{R}^{r_1+r_2}$ le plongement logarithmique :

$$\mathcal{L}(\alpha) = (d_v \log |\alpha|_v)_{v|_\infty}$$

(où l'on a choisit un ordre sur l'ensemble des places archimédiennes de K). Soit $V = \mathcal{L}((K^*)^\phi) \otimes \mathbb{R}$ et $H = \mathcal{L}(E_K^\phi) \otimes \mathbb{R}$; remarquons que

$$H = \left\{ \underline{x} \in V \text{ t.q. } \sum_{v|\infty} x_v = 0 \right\}$$

et donc ou bien $H = V$ ou bien H est un hyperplan de V (plus précisément, $H = V$ si et seulement si $\sum \phi_\tau = 0$). Posons $\underline{e}_0 = \underline{0}$ dans le premier cas et choisissons dans le deuxième un vecteur $\underline{e}_0 \in V \setminus H$ tel que $\|\underline{e}_0\|_1 = 1$.

Soient v_1, \dots, v_r des unités multiplicativement indépendantes de E_K^ϕ tels que :

$$h(v_1) + \dots + h(v_r) = \delta$$

et notons :

$$P = \{ \lambda_1 \mathcal{L}(v_1) + \dots + \lambda_r \mathcal{L}(v_r) \text{ t.q. } 0 \leq \lambda_1, \dots, \lambda_r < 1 \} \subseteq H .$$

Quitte à remplacer les $\gamma_1, \dots, \gamma_t$ par $u_1 \gamma_1, \dots, u_t \gamma_t$ avec $u_1, \dots, u_r \in E_K$, on peut supposer que

$$(\pi \circ \mathcal{L})(\gamma_1^\phi), \dots, (\pi \circ \mathcal{L})(\gamma_t^\phi) \in P ,$$

où $\pi : \mathbb{R}^{r_1+r_2} \rightarrow H$ est définie par :

$$\pi(\underline{a}) = \underline{a} - \left(\sum_{s=0}^r a_s \right) \underline{e}_0 \quad (\underline{a} \in \mathbb{R}^{r_1+r_2}).$$

Par le principe des tiroirs, il existe $m+1$ indices $j_0, j_1, \dots, j_m \in \{1, \dots, t\}$ deux à deux distincts et un vecteur $\underline{a} \in P$, tels que :

$$(\pi \circ \mathcal{L})(\gamma_{j_0}^\phi), (\pi \circ \mathcal{L})(\gamma_{j_1}^\phi), \dots, (\pi \circ \mathcal{L})(\gamma_{j_m}^\phi) \in \underline{a} + N^{-1}P .$$

Remarquons que si $u \in E_K$, alors (*voir* par exemple [Am] lemme 2.1)

$$[K : \mathbb{Q}]h(u) = \frac{1}{2} \|\mathcal{L}(u)\|_1 .$$

Soit $s \in \{1, \dots, m\}$; on a donc :

$$\begin{aligned} \frac{1}{2} \|(\pi \circ \mathcal{L})(\gamma_{j_s}^\phi \gamma_{j_0}^{-\phi})\|_1 &\leq \frac{1}{2N} (\|\mathcal{L}(v_1)\|_1 + \dots + \|\mathcal{L}(v_r)\|_1) \\ &= [K : \mathbb{Q}]N^{-1} (h(v_1) + \dots + h(v_r)) \\ &= [K : \mathbb{Q}]N^{-1}\delta . \end{aligned}$$

Pour $x \in \mathbb{R}$ notons $x^+ = \max(x, 0)$ et $x^- = \max(-x, 0)$; notons aussi, pour $\phi = \sum_{\tau \in \Gamma} \phi_\tau \tau$,

$$\phi^+ = \sum_{\tau \in \Gamma} \phi_\tau^+ \tau, \quad \text{et} \quad \phi^- = \sum_{\tau \in \Gamma} \phi_\tau^- \tau .$$

Posons $\theta_1 = \gamma_{j_s}^{\phi^+} \gamma_{j_0}^{\phi^-}$ et $\theta_2 = \gamma_{j_s}^{\phi^-} \gamma_{j_0}^{\phi^+}$; donc $\theta_1, \theta_2 \in \mathcal{O}_K$ et $\gamma_{j_s}^{\phi} \gamma_{j_0}^{-\phi} = \theta_1 \theta_2^{-1}$.
On a alors facilement (voir [Am] lemme 2.1 pour les détails) :

$$[K : \mathbb{Q}]h(\theta_1 \theta_2^{-1}) \leq \max\{\log |N_{\mathbb{Q}}^K \theta_1|, \log |N_{\mathbb{Q}}^K \theta_2|\} + \frac{1}{2} \|(\pi \circ \mathcal{L})(\theta_1 \theta_2^{-1})\|_1.$$

Par ailleurs,

$$\log |N_{\mathbb{Q}}^K \theta_1| = \left(\sum_{\tau \in \Gamma} \phi_{\tau}^+ \right) \log |N_{\mathbb{Q}}^K \gamma_{j_s}| + \left(\sum_{\tau \in \Gamma} \phi_{\tau}^- \right) \log |N_{\mathbb{Q}}^K \gamma_{j_0}| \leq \|\phi\|_1 \log x$$

et, de même, $\log |N_{\mathbb{Q}}^K \theta_2| \leq \|\phi\|_1 \log x$. On déduit des inégalités précédentes que :

$$h(\gamma_{j_s}^{\phi} \gamma_{j_0}^{-\phi}) \leq \frac{\|\phi\|_1 \log x}{[K : \mathbb{Q}]} + \frac{\delta}{N}.$$

□

Si $\sum_{\tau} \phi_{\tau} = 0$, nous pouvons affaiblir l'hypothèse sur la norme des γ_j dans la proposition 2.1. Pour ce faire, introduisons d'abord quelques notations. Soit I un idéal fractionnaire de K et $v \nmid \infty$ une place non-archimédienne de K , associé à un idéal premier $\wp \subset \mathcal{O}_K$. On pose :

$$|I|_v = p^{-\lambda/e(\wp, p)}$$

où $(p) = \wp \cap \mathbb{Z}$ et où $\lambda \in \mathbb{Z}$ est l'exposant de \wp dans la décomposition de I en produit d'idéaux premiers de \mathcal{O}_K . On a donc

$$\prod_{v \nmid \infty} |I|_v^{n_v} = (NI)^{-1}$$

et, pour $\alpha \in K$,

$$|\alpha|_v = |(\alpha)|_v.$$

Proposition 2.2 *Soient $K, \Gamma, \phi, r, \delta, x$ et t comme dans la proposition 2.1 et supposons $\sum_{\tau} \phi_{\tau} = 0$. Supposons aussi qu'il existe des entiers algébriques non nuls $\gamma_1, \dots, \gamma_t \in \mathcal{O}_K$ et des idéaux $I_1, \dots, I_t \subseteq \mathcal{O}_K$ de norme $\leq x$ tels que les $(\gamma_j)^{-1} I_j$ soient des extensions d'idéaux fractionnaires de K^{Γ} . Soient ensuite m et N deux entiers strictement positifs et tels que :*

$$mN^r < t.$$

Alors il existent $m+1$ indices $j_0, j_1, \dots, j_m \in \{1, \dots, t\}$ deux à deux distincts et des unités $v_1, \dots, v_m \in E_K^{\phi}$ tels que :

$$h(v_j \gamma_{j_s}^{\phi} \gamma_{j_0}^{-\phi}) \leq \frac{\|\phi\|_1 \log x}{[K : \mathbb{Q}]} + \frac{\delta}{N}$$

pour $s = 1, \dots, m$.

Démonstration. Remarquons d'abord que, pour $v \nmid \infty$, $|\gamma_j^\phi|_v = |I_j^\phi|_v$ car

$$(\gamma_j)^{-\phi} I_j^\phi = ((\gamma_j)^{-1} I_j)^{\sum \tau \phi_\tau} = \mathcal{O}_K.$$

Donc

$$\begin{aligned} \log |\gamma_{j_s}^\phi \gamma_{j_0}^{-\phi}|_v &= \sum_{\tau \in \Gamma} \phi_\tau (\log |I_{j_s}^\phi|_v - \log |I_{j_0}^\phi|_v) \\ &\leq \sum_{\tau \in \Gamma} (\phi_\tau^+ (-\log |I_{j_s}|_v) + \phi_\tau^- (-\log |I_{j_0}|_v)) \end{aligned} \quad (2.1)$$

car les I_j sont des idéaux entiers. La preuve de la proposition 2.1 montre qu'il existe $m+1$ indices $j_0, j_1, \dots, j_m \in \{1, \dots, t\}$ deux à deux distincts et des unités $v_1, \dots, v_m \in E_K^\phi$ tels que :

$$\frac{1}{2} \|\mathcal{L}(v_j \gamma_{j_s}^\phi \gamma_{j_0}^{-\phi})\|_1 \leq [K : \mathbb{Q}] N^{-1} \delta$$

pour $s = 1, \dots, m$.

Soit $s \in \{1, \dots, m\}$; on a alors :

$$\sum_{v \nmid \infty} n_v \log^+ |v_j \gamma_{j_s}^\phi \gamma_{j_0}^{-\phi}|_v \leq [K : \mathbb{Q}] N^{-1} \delta$$

(car $|N_{\mathbb{Q}}^K v_j \gamma_{j_s}^\phi \gamma_{j_0}^{-\phi}| = 1$) et, grâce à (2.1),

$$\begin{aligned} \sum_{v \nmid \infty} n_v \log^+ |v_j \gamma_{j_s}^\phi \gamma_{j_0}^{-\phi}|_v &\leq \sum_{\tau \in \Gamma} (\phi_\tau^+ (-\log |I_{j_s}|_v) + \phi_\tau^- (-\log |I_{j_0}|_v)) \\ &\leq \|\phi\|_1 \log x. \end{aligned}$$

□

Nous terminons ce paragraphe avec un résultat galoisien élémentaire, qui généralise le lemme 3.2 de [Am-Dv] :

Lemme 2.3 *Soit K un corps de nombres et Γ le groupe des \mathbb{Q} -automorphismes de K . Soit ensuite P un idéal premier de \mathcal{O}_K de degré 1 sur \mathbb{Q} et non ramifié. Alors, les idéaux premiers P^σ ($\sigma \in \Gamma$) sont deux à deux distincts.*

Démonstration. Soit K^Γ le sous-corps de K fixé par Γ ; par le lemme d'Artin K/K^Γ est une extension de Galois de groupe de Galois Γ . Soit $P_0 = P \cap \mathcal{O}_{K_0}$; par hypothèse $P_0 \mathcal{O}_K = P_1 \dots P_r$ avec $P_1 = P$, $r = |\Gamma|$ et les P_j deux-à-deux distincts. Par ailleurs Γ agit transitivement sur $\{P_1, \dots, P_r\}$, et donc $\{P^\sigma \text{ t.q. } \sigma \in \Gamma\} = \{P_1, \dots, P_r\}$. □

3 Taille de certains groupes de classes.

Soit K un corps de nombres de degré d et discriminant Δ , notons Γ le groupe des \mathbb{Q} -automorphismes de K . Soit ensuite $\phi \in \mathbb{Z}[\Gamma]$ et posons $r = r_\phi$ et $\delta = \delta_\phi$. Nous nous proposons d'étudier la structure de $\mathbb{Z}[\Gamma]$ -module de

$$Cl(K)/jCl(K^\Gamma),$$

où $j: Cl(K^\Gamma) \rightarrow Cl(K)$ est le morphisme d'extension. Pour ce faire considérons la fonction $\mathcal{M}_{\mathcal{C},\phi}: \mathbb{N}^* \rightarrow \mathbb{N}^*$ suivante attachée au $\mathbb{Z}[\Gamma]$ -module \mathcal{C} . Pour l entier strictement positif notons $\mathcal{M}_{\mathcal{C},\phi}(l)$ le plus petit entier A tel que pour tout $g_1, \dots, g_l \in \mathcal{C}$ ils existent $\rho_1, \dots, \rho_l \in \mathbb{Z}[\Gamma]$ tels que :

- i) $(\rho_1, \dots, \rho_l)\phi \neq (0)$;
- ii) $g_1^{\rho_1} \cdots g_l^{\rho_l} = 1$;
- iii) $\sum_j \|\rho_j\|_1 \leq A$.

Cette définition généralise celle de la fonction $\mathcal{M}_G(l)$ attachée à un groupe fini G (cf [Am-Dv]).

Proposition 3.1 *Soit $\varepsilon > 0$; ils existent alors deux constantes C et $C_\varepsilon > 0$ telles que, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K ,*

$$\mathcal{M}_{Cl(K),\phi}(l) \geq \frac{\max(Cd^{-1} \log |\Delta|, C_\varepsilon d^{1-\varepsilon})}{\|\phi\|_1 (\log l + \log \log |\Delta| + r \log (d\delta/r + 2))}.$$

De plus, si $\sum_\tau \phi_\tau = 0$, l'inégalité précédente reste vraie si l'on remplace $Cl(K)$ par $Cl(K)/jCl(K^\Gamma)$.

Démonstration. On peut évidemment supposer $\varepsilon < 1/2$. Remarquons également qu'il suffit de montrer qu'il existe deux constantes C' et $C_\varepsilon > 0$ telles que,

$$\mathcal{M}_{Cl(K),\phi}(l) \geq \frac{\max(C'(d^{-1} \log |\Delta| - \log d), C(\varepsilon)d^{1-\varepsilon})}{\|\phi\|_1 (\log l + \log \log |\Delta| + r \log (d\delta/r + 2))}$$

et de même pour $\mathcal{M}_{Cl(K)/jCl(K^\Gamma),\phi}(l)$ si $\sum_\tau \phi_\tau = 0$. En effet, si $\log |\Delta| > 2d \log d$, alors

$$C'(d^{-1} \log |\Delta| - \log d) > \frac{1}{2}C'd^{-1} \log |\Delta|$$

tandis que, si $\log |\Delta| \leq 2d \log d$,

$$d^{-1} \log |\Delta| \leq 2 \log d \leq \frac{4}{e}d^{1-\varepsilon}.$$

I) La preuve de l'inégalité :

$$\mathcal{M}_{Cl(K),\phi}(l) \geq \frac{C(d^{-1} \log |\Delta| - \log d)}{\|\phi\|_1 (\log l + \log \log |\Delta| + r \log (d\delta/r + 2))},$$

généralise celle de la proposition 3.1 de [Am]. Une application standard de la version effective du théorème des nombres premiers dans un corps de nombres (voir [Lag-Odl] avec $L = K$), montre que, sous GRH, il existe des constantes absolues et effectives $c_1, c_2 > 0$ telles que pour tout K et tout réel x avec

$$x \geq c_1 (\log |\Delta|)^2 (\log \log |\Delta|)^4$$

il existe au moins $c_2^{-1} x (\log x)^{-1}$ idéaux premiers de norme $\leq x$, de degré 1 sur \mathbb{Q} et non ramifiés (voir [Am-Dv], lemme 2.1). Notons $t = ([d\delta/r] + 2)^r$ et soit $c_3 \geq 1$ tel que $\frac{c_3}{\log c_3 + 2} \geq c_2$. Choisissons

$$x = c_3 l t d \log(l t d) + c_1 (\log |\Delta|)^2 (\log \log |\Delta|)^4;$$

on a en particulier $x \geq c_3 y \log y \geq e$, où l'on a noté $y = l t d \geq 3$, et donc :

$$x (\log x)^{-1} \geq \frac{c_3 y \log y}{\log(c_3 y \log y)} \geq \frac{c_3 y \log y}{\log c_3 + 2 \log y} \geq c_2 y = c_2 l t d.$$

Remarquons qu'il y a au plus d premiers distincts dans \mathcal{O}_K au dessus d'un premier rationnel ; il existe donc $l t$ premiers rationnels distincts $p_{ij} \leq x$ et $l t$ idéaux premiers $P_{ij} \subseteq \mathcal{O}_K$ ($i = 1, \dots, l; j = 1, \dots, t$) tels que $P_{ij} \cap \mathbb{Z} = (p_{ij})$ et $e(P_{ij}|p_{ij}) = f(P_{ij}|p_{ij}) = 1$ pour $i = 1, \dots, l$ et $j = 1, \dots, t$. Soit g_{ij} la classe de P_{ij} dans G et supposons qu'il existe des relations

$$g_1^{\rho_{1j}} \cdots g_t^{\rho_{lj}} = e \quad (j = 1, \dots, t)$$

avec $\rho_{ij} \in \mathbb{Z}[\Gamma]$ tels que $(\rho_{1j}, \dots, \rho_{lj})\phi \neq (0)$ ($j = 1, \dots, t$). Soit $A = \max_j \sum_i \|\rho_{ij}\|_1$; donc, pour $j = 1, \dots, t$,

$$P_{1j}^{\rho_{1j}} \cdots P_{lj}^{\rho_{lj}} = (\gamma_j)$$

est un idéal principal de norme $\leq x^A$. Choisissons $m = 1$ et $N = [d\delta/r] + 1$ dans la proposition 2.1 ; cette dernière nous assure l'existence d'une unité $v \in E_K^\phi$ et de deux indices $j_0, j_1 \in \{1, \dots, t\}$ avec $j_0 \neq j_1$ tels que la hauteur de $\alpha = v \gamma_{j_1}^\phi \gamma_{j_0}^{-\phi}$ satisfasse :

$$h(\alpha) \leq \frac{A \|\phi\|_1 \log x + r}{d}.$$

Remarquons que :

$$\log x \leq c_4 (\log(l t d) + \log \log |\Delta|)$$

d'où, en utilisant la minoration $\log |\Delta| \geq c_5 d$ et en remplaçant t par sa valeur,

$$\begin{aligned} \log x &\leq c_6(\log(lt) + \log \log |\Delta|) \\ &\leq c_7(\log l + \log \log |\Delta| + r \log(d\delta/r + 2)). \end{aligned}$$

On a donc :

$$h(\alpha) \leq c_5 A \|\phi\|_1 \left(\frac{\log l + \log \log |\Delta| + r \log(d\delta/r + 2)}{d} \right). \quad (3.2)$$

Montrons maintenant que α est un générateur de K . Pour cela, il est suffisant de montrer que $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq d$. Quitte à renuméroter les indices, on peut supposer $\rho_{1,j_1} \phi \neq 0$. Soit L la clôture galoisienne de K dans $\overline{\mathbb{Q}}$ et notons $Q_{i,j} := P_{i,j} \mathcal{O}_L$. Le lemme 3.1 de [Am-Dv] nous assure que Q_{1,j_1} a au moins d conjugués distincts $Q_{1,j_1}^{\sigma_1}, \dots, Q_{1,j_1}^{\sigma_d}$. Supposons que pour certains $\iota, \kappa \in \{1, \dots, d\}$ on ait $\alpha^{\sigma_\iota} = \alpha^{\sigma_\kappa}$. Alors :

$$\prod_{i=1}^l Q_{i,j_1}^{\rho_{i,j_1} \phi^{\sigma_\iota}} Q_{i,j_0}^{-\rho_{i,j_0} \phi^{\sigma_\iota}} = \prod_{i=1}^l Q_{i,j_1}^{\rho_{i,j_1} \phi^{\sigma_\kappa}} Q_{i,j_0}^{-\rho_{i,j_0} \phi^{\sigma_\kappa}}.$$

Les $P_{ij} \cap \mathbb{Z}$ sont distincts et donc la relation précédente donne en particulier :

$$Q_{1,j_1}^{\rho_{1,j_1} \phi^{\sigma_\iota - \sigma_\kappa}} = \mathcal{O}_L.$$

Par le lemme 2.3, les premiers P_{1,j_1}^τ ($\tau \in \Gamma$) sont deux à deux distincts et donc les idéaux $(\sigma_\tau)Q_{1,j_1}$ sont deux à deux premiers entre eux ; par ailleurs $\rho_{1,j_1} \phi \neq 0$. On en déduit facilement que :

$$Q_{1,j_1}^{\sigma_\iota} = Q_{1,j_1}^{\sigma_\kappa},$$

d'où $\iota = \kappa$. Donc α a au moins d conjugués distincts et $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq d$.

Un résultat de J. Silverman (voir [Si], Theorem 2, p. 397 avec $F = \mathbb{Q}$, $n = 1$, $\alpha_0 = 1$ et $\alpha_1 = \alpha$) donne alors :

$$h(\alpha) \geq \frac{d^{-1} \log |\Delta| - \log d}{2(d-1)}. \quad (3.3)$$

Le résultat désiré découle de 3.2 et 3.3.

II) Montrons maintenant l'inégalité :

$$\mathcal{M}_{Cl(K), \phi}(l) \geq \frac{C(\varepsilon) d^{1-\varepsilon}}{\|\phi\|_1 (\log l + \log \log |\Delta| + r \log(d\delta/r + 2))}.$$

Pour ce faire, nous reprenons l'argument de la preuve de l'inégalité correspondante de [Am-Dv] (inégalité (6), p. 92). Rappelons d'abord le résultat principal de [Am-Da] : si $\alpha_1, \dots, \alpha_m \in K$ sont multiplicativement indépendants,

$$\max_{s=1, \dots, m} h(\alpha_s) \geq c_8(m)^{-1} d^{-1/m} \log(3d)^{-k(m)}$$

où $k(m) > 0$.

Posons maintenant $m = [1/\varepsilon] + 1$. Donc :

$$c_8(m) d^{1/m} \log(3d)^{k(m)} \leq c_9(\varepsilon) d^\varepsilon.$$

Posons aussi $N = [d\delta/r] + 1$, $t = mN^r + 1$ et

$$x = c_3 l m t d \log(lm) + c_1 (\log |\Delta|)^2 (\log \log |\Delta|)^4.$$

Le résultat de [Lag-Od] déjà utilisé dans la partie I de la preuve, montre qu'ils existent $l m t d$ idéaux premiers $P_{ij} \subseteq \mathcal{O}_K$ ($i = 1, \dots, l$; $j = 1, \dots, m t d$) de norme $\leq x$, de degré 1 sur \mathbb{Q} et non ramifiés. Par l'inégalité $|\Gamma| \leq d$, nous pouvons supposer

$$\forall \tau \in \Gamma, \quad P_{ij} \neq P_{i'j'}^\tau \quad (3.4)$$

pour $(i, j) \neq (i', j')$ avec $1 \leq j, j' \leq l m t$. Soit g_{ij} la classe de P_{ij} dans G et supposons qu'il existe des relations multiplicatives

$$g_{1j}^{\rho_{1j}} \cdots g_{lj}^{\rho_{lj}} = e \quad (j = 1, \dots, m t)$$

avec $\rho_{ij} \in \mathbb{Z}[\Gamma]$ et $(\rho_{1j}, \dots, \rho_{lj})\phi \neq (0)$ pour $j = 1, \dots, m t$. Soit $A = \max_j \sum_i \|\rho_{ij}\|_1$; donc, pour $j = 1, \dots, m t$,

$$P_{1j}^{\rho_{1j}} \cdots P_{lj}^{\rho_{lj}} = (\gamma_j)$$

est un idéal principal de norme $\leq x^A$. La proposition 2.1 nous assure l'existence de $m + 1$ indices $j_0, j_1, \dots, j_m \in \{1, \dots, t\}$ deux à deux distincts et de certaines unités $v_1, \dots, v_m \in \phi E_K$ tels que les hauteurs des $\alpha_s = v_j \gamma_{j_s}^\phi \gamma_{j_0}^{-\phi}$ satisfassent :

$$h(\alpha_s) \leq \frac{A \|\phi\|_1 \log x + r}{d}$$

pour $s = 1, \dots, m$.

Comme dans la première partie de la preuve,

$$\begin{aligned} \log x &\leq c_6 (\log(lm t) + \log \log |\Delta|) \\ &\leq c_{10}(\varepsilon) \left(\log l + \log \log |\Delta| + r \log(d\delta/r + 2) \right). \end{aligned}$$

On a donc :

$$\begin{aligned} & \max_{s=1, \dots, m} h(\alpha_s) \\ & \leq c_{10}(\varepsilon) A \|\phi\|_1 \left(\frac{\log l + \log \log |\Delta| + r \log (d\delta/r + 2)}{d} \right). \end{aligned} \quad (3.5)$$

Montrons que $\alpha_1, \dots, \alpha_m$ sont multiplicativement indépendants. En effet supposons $\alpha_1^{e_1} \cdots \alpha_m^{e_m} = 1$ avec $e_1, \dots, e_m \in \mathbb{Z}$. Donc :

$$\prod_{s=1}^m (v_j \gamma_{j_s}^\phi \gamma_{j_0}^{-\phi})^{e_s} = 1.$$

En utilisant la définition des γ_j , on en déduit une relation multiplicative dans $\text{Spec}(\mathcal{O}_K)$:

$$\prod_{s=1}^m (P_{1j_s}^{\rho_{1j_s}\phi} \cdots P_{lj_s}^{\rho_{lj_s}\phi})^{e_s} = (P_{1j_0}^{\rho_{1j_0}\phi} \cdots P_{lj_0}^{\rho_{lj_0}\phi})^{e_1 + \cdots + e_s}.$$

La condition (3.4) et le lemme 2.3 nous assurent que $e_1 = \cdots = e_s = 0$. Le résultat principal de [Am-Da] donne alors :

$$\max_{s=1, \dots, m} h(\alpha_s) \geq c_9(\varepsilon)^{-1} d^{-\varepsilon}. \quad (3.6)$$

Le résultat désiré découle de (3.5) et (3.6).

III) Supposons enfin $\sum_\tau \phi_\tau = 0$. Soient P_1, \dots, P_m des idéaux premiers de \mathcal{O}_k , notons g_i la classe de P_i dans G et supposons qu'il existe une relation multiplicative non triviale

$$g_1^{\rho_1} \cdots g_m^{\rho_m} = e$$

avec les $\rho_i \in \mathbb{Z}[\Gamma]$. Alors, il existe $\gamma \in \mathcal{O}_K$ tel que

$$(\gamma^{-1}) P_1^{\rho_1} \cdots P_m^{\rho_m}$$

soit l'extension d'un idéal fractionnaire de K^Γ . Pour montrer la dernière assertion de la proposition 3.1 il suffit alors d'utiliser la proposition 2.2 à la place de la proposition 2.1 dans les parties I) et II) de la preuve. \square

Remarque 3.2 *On déduit en particulier de la proposition 3.1 des renseignements sur le nombre de classes h_K et sur l'exposant e_K du groupe de classes : en effet $\mathcal{M}_{\mathcal{C}, \phi}(1) \leq e_K$ et $\mathcal{M}_{\mathcal{C}, \phi}(h_K) \leq 2$ (cf [Am-Dv], lemma 5.1).*

4 Corps « de type CM » et nombres de Salem.

Nous étudions dans ce paragraphe des corps auxquels nos résultats principaux s'appliquent. Il s'agit de certaines généralisations des corps CM : des corps engendrés par un nombre réciproque ayant « beaucoup » des conjugués sur le cercle unité. Le corps engendrés par un nombre de Salem en sont un exemple.

Définition 4.1 Soit $\alpha \in \overline{\mathbb{Q}}$; on note $l(\alpha)$ le nombre de places archimédiennes $v \in M_{\mathbb{Q}(\alpha)}$ tels que $|\alpha|_v = 1$.

Remarquons que si $\alpha \neq \pm 1$ et si $l(\alpha) > 1$, alors α n'est pas totalement réel. De plus, α est réciproque : en effet, il existe un plongement imaginaire $\sigma : \mathbb{Q}(\alpha) \hookrightarrow \mathcal{C}$ tel que $\sigma(\alpha)\overline{\sigma(\alpha)} = 1$ et donc $\sigma(\alpha^{-1}) = \overline{\sigma(\alpha)}$, ce qui implique que α^{-1} est un conjugué de α . L'application $\alpha \mapsto \alpha^{-1}$ s'étend donc à une \mathbb{Q} -involution τ de $\mathbb{Q}(\alpha)$ (i. e. un \mathbb{Q} -automorphisme τ de $\mathbb{Q}(\alpha)$ d'ordre 2).

Définition 4.2 Soit K un corps de nombres, τ une \mathbb{Q} -involution de K et K^τ le sous corps d'indice 2 fixé par K . On note l_τ le nombre des places archimédiennes imaginaires de K au dessus d'une place réel de K^τ .

Notons (r_1, r_2) et (r_1^τ, r_2^τ) les signatures de K et K^τ respectivement. On vérifie immédiatement que

$$l_\tau = r_1^\tau - r_1/2.$$

Remarquons aussi que si $K = \mathbb{Q}(\alpha)$ avec $\alpha^\tau = \alpha^{-1}$, alors :

$$K^\tau = \mathbb{Q}(\alpha + \alpha^{-1}).$$

On a :

Lemme 4.3 Soit τ une \mathbb{Q} -involution de K . Alors :

$$l_\tau = \max\{l(\alpha) \text{ t.q. } K = \mathbb{Q}(\alpha), \alpha^\tau = \alpha^{-1}\}.$$

Démonstration. Soient σ_j ($j = 1, \dots, l$) des plongements imaginaires du corps K , deux à deux non conjugués, qui prolongent des plongements réels de K^τ . Il existe un générateur α de K/\mathbb{Q} tel que $|\sigma_1(\alpha)| = 1$ (voir par exemple [Am-Nu], proposition 1). Soit

$$P(x) = x^2 - bx + c,$$

le polynôme minimal de α sur K^τ ; P^{σ_1} est à coefficients réels et admet une racine de module 1 : donc son terme constante vaut 1 et $c = 1$. Mais alors, si $j \in \{1, \dots, l\}$,

$$\sigma_j(b) \in \mathbb{R}, \quad \sigma_j(\alpha) \notin \mathbb{R} \implies |\sigma_j(\alpha)| = 1$$

et $l_\tau(\alpha) \geq l$. Nous avons prouvé que :

$$\max\{l(\alpha) \text{ t.q. } K = \mathbb{Q}(\alpha), \alpha^\tau = \alpha^{-1}\} \geq l_\tau .$$

Soit maintenant α un générateur de K/\mathbb{Q} tel que $\alpha^\tau = \alpha^{-1}$ et soient σ_j ($j = 1, \dots, l$) des plongements imaginaires du corps K , deux à deux non conjugués et tels que $|\sigma_j(\alpha)| = 1$. Alors, $\alpha^2 - b\alpha + 1 = 0$ avec $b = \alpha + \alpha^{-1}$. Par la remarque qui précède ce lemme, $K^\tau = \mathbb{Q}(b)$. Par ailleurs, si $j \in \{1, \dots, l\}$, on a $\sigma_j(\alpha^{-1}) = \overline{\sigma_j(\alpha)}$, d'où $\sigma_j(b) \in \mathbb{R}$ et $\sigma_j(K^\tau) = K^\tau$. Donc $l \geq l_\tau(\alpha)$. Nous avons prouvé que :

$$l_\tau \geq \max\{l(\alpha) \text{ t.q. } K = \mathbb{Q}(\alpha), \alpha^\tau = \alpha^{-1}\} .$$

□

Les corps de nombres engendrés par un nombre algébrique ayant beaucoup des conjugués sur le cercle unité donnent des exemples d'applications du théorème 3.1, comme la proposition suivante le montre.

Proposition 4.4 *Soit K un corps de nombres de signature (r_1, r_2) munit d'une \mathbb{Q} -involution τ . Alors*

$$r_{1-\tau} \leq r_1 + r_2 - l_\tau .$$

Démonstration. Soit α un générateur de K/\mathbb{Q} tel que $\alpha^\tau = \alpha^{-1}$ et tel qu'ils existent $l = l_\tau$ plongements imaginaires $\sigma_j: K \rightarrow \mathcal{C}$ deux à deux non conjugués avec $|\sigma_j(\alpha)| = 1$. Soit $P \in \mathbb{Q}[x]$ et $j \in \{1, \dots, l\}$. Alors :

$$\overline{\sigma_j(P(\alpha))} = P(\overline{\sigma_j(\alpha)}) = P(\sigma_j(\alpha)^{-1}) = P(\sigma_j(\alpha^\tau)) = \sigma_j(P(\alpha)^\tau)$$

et de même

$$\overline{\sigma_j(P(\alpha)^\tau)} = \sigma_j(P(\alpha)) .$$

Donc $|\sigma_j(P(\alpha)^{1-\tau})|^2 = 1$. On en déduit que $\dim \mathcal{L}((K^*)^{1-\tau}) \otimes \mathbb{R} \leq r_1 + r_2 - l_\tau$. □

En particulier, cette proposition s'applique dès que K est un corps CM : pour ces corps on a $r_{1-J} = 0$, où J est la conjugation complexe. De même, la proposition 4.4 montre que si K est engendré par un nombre de Salem α et si τ est le \mathbb{Q} -automorphisme de K qui envoie α dans α^{-1} , alors $r_{1-\tau} = 1$. Par ailleurs $E_K^{1-\tau}$ est engendré par $\alpha^2 = \alpha/\alpha^{-1}$ et donc $\delta_{1-\tau} \leq 2h(\alpha) = 2(\log \alpha)/d$, où $d = [K : \mathbb{Q}]$.

Nous terminons ce paragraphe avec le lemme suivant qui permet de minorer h_K/h_{K^τ} en fonction de l'ordre de $\mathcal{Cl}(K)/j\mathcal{Cl}(K^\tau)$.

Lemme 4.5 Soit τ une \mathbb{Q} -involution d'un corps de nombres K et notons $j: Cl(K^\tau) \rightarrow Cl(K)$ le morphisme d'extension d'idéaux. Alors,

$$|\ker j| \leq 2^{1+r_{1-\tau}}.$$

Démonstration.

Nous suivons la preuve du théorème 10.3 de [Wa]. Soit I un idéal de K^τ et supposons $j(I)$ principal dans K , disons $j(I) = (\alpha)$. On a $I^{1-\tau} = I/I^\tau = \mathcal{O}_K$, et donc $\alpha^{1-\tau} \in E_K$. De plus, α ne dépend pas du représentant de la classe de I dans $Cl(K^\tau)$. Notons

$$G = \{u \in E_K \text{ t.q. } \exists \alpha \in K, \alpha^{1-\tau} = u\}$$

et supposons $\alpha^{1-\tau} \in G^2$. Il existe donc $v \in E_k$ et $\beta \in K$ tel que $v = \beta^{1-\tau}$ et $\alpha^{1-\tau} = v^2$. On en déduit :

$$\begin{aligned} (\alpha v^{-1})^{1-\tau} &= \alpha^{1-\tau} \beta^{-(1-\tau)^2} = \alpha^{1-\tau} \beta^{-2(1-\tau)} \\ &= \alpha^{1-\tau} v^{-2} = 1 \end{aligned}$$

et donc $\alpha v^{-1} \in K^\tau$ et $I = (\alpha v^{-1})$ est principal dans K^τ . On a montré que l'application $\ker j \rightarrow G/G^2$ qu'envoie la classe de I dans la classe de $\alpha^{1-\tau}$ est injective et donc $|\ker j| \leq [G : G^2] \leq 2^{1+r_{1-\tau}}$, car G est de rang $r_{1-\tau} + 1$. \square

5 Taille des groupes de classes de corps « de type CM ».

Soit K un corps de nombres de signature (r_1, r_2) munit d'une \mathbb{Q} -involution τ et notons $r = r_1 + r_2 - l_\tau$ et $\delta = \delta_{1-\tau}$. $k = \mathbb{Q}(\alpha + \alpha^{-1})$. Le théorème suivant résume les renseignements principaux que l'on peut obtenir sur la structure du groupe de classes de K .

Corollaire 5.1 Soit $\varepsilon > 0$; il existe alors trois constantes $C, C_\varepsilon > 0$ et $H_\varepsilon > 1$ telles que, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K ,

$$e_{K/k} \geq \frac{\max(Cd^{-1} \log |\Delta|, C_\varepsilon d^{1-\varepsilon})}{\log \log |\Delta| + r \log (d\delta/r + 2)}$$

et :

$$\frac{h_K}{h_k} \geq \frac{\max(|\Delta|^{C/d}, H_\varepsilon^{d^{1-\varepsilon}})}{(2d\delta/r + 4)^r}.$$

Démonstration. On applique la proposition 3.1 en tenant compte de la majoration de $r_{1-\tau} \leq r$ fournit par la proposition 4.4 et de la remarque 3.2. On obtient donc :

$$e_{K/k} \geq \frac{\max(Cd^{-1} \log |\Delta|, C_\varepsilon d^{1-\varepsilon})}{\log \log \Delta + r \log (d\delta/r + 2)} .$$

et, en prenant $l = |\mathcal{Cl}(K)/j\mathcal{Cl}(k)|$,

$$2 \geq \frac{\max(Cd^{-1} \log |\Delta|, C_\varepsilon d^{1-\varepsilon})}{2(\log l + \log \log |\Delta| + r \log (d\delta/r + 2))} .$$

Le lemme 4.5 montre que $\log(h_K/h_k) \geq \log l - (r+1) \log 2$; donc :

$$\begin{aligned} \log(h_K/h_k) &\geq \frac{1}{4} \max(Cd^{-1} \log |\Delta|, C_\varepsilon d^{1-\varepsilon}) - \log \log |\Delta| \\ &\quad - r \log (2d\delta/r + 4) - (r+1) \log 2 \\ &\geq c_{11} \max(Cd^{-1} \log |\Delta|, C_\varepsilon d^{1-\varepsilon}) - r \log (2d\delta/r + 4) , \end{aligned}$$

d'où la minoration annoncée pour h_K/h_k . □

On peut également déduire de la proposition 3.1 des renseignements sur l'annulateur du groupe de classes de K , comme on l'a fait dans [Am2] pour le cas d'un corps cyclotomique. Notons $\mathcal{Cl}^-(K) = \mathcal{Cl}(K)/j\mathcal{Cl}(K^\tau)$,

$$\mathbb{Z}[\Gamma]^\pm = \{\psi \in \mathbb{Z}[\Gamma] \text{ t.q. } \psi(1 \mp \tau) = 0\}$$

et

$$\text{Ann}(\mathcal{Cl}^-(K))^- = \text{Ann}(\mathcal{Cl}^-(K)) \cap \mathbb{Z}[\Gamma]^-$$

l'ensemble des $\psi \in \mathbb{Z}[\Gamma]^-$ tel que pour tout idéal I de K , il existe $\alpha \in K$ tel que $(\alpha)I^\psi$ soit l'extension d'un idéal fractionnaire de K^τ . On a alors :

Corollaire 5.2 *Soit $\varepsilon > 0$; il existe alors deux constantes C et $C_\varepsilon > 0$ telles que, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K et pour tout $\psi \in \text{Ann}(\mathcal{Cl}^-(K)) \setminus \mathbb{Z}[\Gamma]^+$, on a $\|\psi\|_1 \geq B$, où*

$$B := \frac{\max(Cd^{-1} \log |\Delta|, C_\varepsilon d^{1-\varepsilon})}{\log \log |\Delta| + r \log (d\delta/r + 2)} .$$

*En particulier,*²

$$[\mathbb{Z}[\Gamma]^- : \text{Ann}(\mathcal{Cl}^-(K))^-] \geq \binom{\lfloor B/4 \rfloor + \text{Card}(\Gamma)/2}{\text{Card}(\Gamma)/2} .$$

²pour $x \in \mathbb{R}$ on note $\lfloor x \rfloor$ l'entier n défini par les inégalités : $n - 1 \leq x < n$.

Démonstration. La minoration pour la taille des éléments de l'annulateur découle immédiatement de la proposition 3.1 (avec $l = 1$), en tenant compte de la majoration $r_{1-\tau} \leq r$ fournie par la proposition 4.4.

Montrons la minoration de l'indice. Pour ce faire on reprend l'argument de la preuve du théorème 2 de [Am2]. Soit $\Gamma' \subset \Gamma$ tel que $\Gamma' \cap \Gamma'\tau = \emptyset$ et $\Gamma = \Gamma' \cup \Gamma'\tau$. L'ensemble

$$\Lambda = \left\{ \sum_{\sigma \in \Gamma'} \psi_\sigma \sigma (1-\tau) \text{ t.q. } \psi_\sigma \geq 0, \text{ et } \sum_{\sigma \in \Gamma'} |\psi_\sigma| < B/4 \right\} \subseteq \mathbb{Z}[\Gamma]^-$$

est de cardinalité

$$\text{Card}(\Lambda) = \binom{\lfloor B/4 \rfloor + \text{Card}(\Gamma)/2}{\text{Card}(\Gamma)/2}. \quad (5.7)$$

Soient $\psi, \psi' \in \Lambda$ avec $\psi \neq \psi'$. Alors $(\psi - \psi')(1-\tau) \neq 0$ et

$$\|\psi - \psi'\|_1 < B.$$

La première partie du corollaire 5.2 nous assure que $\psi - \psi' \notin \text{Ann}(\mathcal{C}l(K)^-)$, ce qui montre :

$$[\mathbb{Z}[\Gamma]^- : \text{Ann}(\mathcal{C}l(K)^-)] \geq \text{Card}(\Lambda). \quad (5.8)$$

Les relations (5.7) et (5.8) montrent la minoration annoncée pour l'indice de l'annulateur. \square

Les résultats annoncés dans l'introduction se déduisent facilement à partir des corollaires 5.1 et 5.2.

Démonstration du théorème 1.1. On applique le corollaire 5.1 avec $r = 0$ et on remarque que

$$\frac{\max(Cd^{-1} \log |\Delta|, C_\varepsilon d^{1-\varepsilon})}{\log \log |\Delta|} \geq \max\left(\frac{C \log |\Delta|}{d \log \log |\Delta|}, C'_\varepsilon d^{1-2\varepsilon}\right).$$

\square

Démonstration du théorème 1.2. Soit $\varepsilon > 0$; le corollaire 5.2 montre qu'ils existent deux constantes C et $C_\varepsilon > 0$ tels que

$$[\mathbb{Z}[\Gamma]^- : \text{Ann}(\mathcal{C}l^-(K))^-] \geq \binom{\lfloor B/4 \rfloor + d_0/2}{d_0/2},$$

où

$$B = \frac{\max(Cd^{-1} \log |\Delta|, C_{\varepsilon/2} d^{1-\varepsilon/2})}{\log \log |\Delta|} \geq \max\left(\frac{C \log |\Delta|}{d \log \log |\Delta|}, C'_\varepsilon d^{1-\varepsilon}\right).$$

L'inégalité $B \geq (C \log |\Delta|)/(d \log \log |\Delta|)$ montre que :

$$[\mathbb{Z}[\Gamma]^- : \text{Ann}(\mathcal{Cl}^-(K))^-] \geq \left(\frac{\lfloor B/4 \rfloor}{d_0/2} \right)^{d_0/2} \geq \left(\frac{C' \log |\Delta|}{dd_0 \log \log |\Delta|} \right)^{d_0/2},$$

tandis que $B \geq C'_\varepsilon d^{1-\varepsilon} \geq C'_\varepsilon d_0^{1-\varepsilon}$ donne :

$$[\mathbb{Z}[\Gamma]^- : \text{Ann}(\mathcal{Cl}^-(K))^-] \geq \left(\frac{d_0/2}{\lfloor B/4 \rfloor} \right)^{\lfloor B/4 \rfloor} \geq H_\varepsilon^{d_0^{1-\varepsilon}}.$$

□

Démonstration du théorème 1.3. On applique le corollaire 5.1 avec $r = 1$. □

Références

- [Am] F. Amoroso – « Une minoration pour l'exposant du groupe de classes d'idéaux. » *Acta Arith.* **115**, No.1, 59–69 (2004).
- [Am2] F. Amoroso – « A remark on the annihilator of the class group of a cyclotomic field. » 2005. Soumis.
- [Am-Da] F. Amoroso and S. David – « Le problème de Lehmer en dimension supérieure. » *J. reine angew. Math.* **513** (1999), 145–179.
- [Am-Dv] F. Amoroso and R. Dvornicich – « Lower bounds for the height and size of the ideal class group in CM fields. » *Monatsh. Math.* **138**, No.2, 85-94 (2003).
- [Am-Nu] F. Amoroso and F. Nuccio – « Algebraic Numbers of Small Weil's height in CM-fields : on a Theorem of Schinzel. » 2004. Rapport de Recherche LMNO 2004-19. Soumis.
- [Ch] T. Chinburg – « On the arithmetic of two constructions of Salem numbers. » *J. Reine Angew. Math.* **348**, 166-179 (1984).
- [La-Od] J. C. Lagarias and A. M. Odlyzko – « Effective versions of the Čebotarev density theorem » , *Algebraic Number Fields*, Durham Symposium, Academic Press, 1977.
- [Od] A. M. Odlyzko – « Some analytic estimates of class numbers and discriminants », *Invent. Math.* **29** (1975), 275–286.
- [Si] J. H. Silverman – « Lower bounds for height functions. » *Duke Math. J.* **51** (1984), 395-403.
- [Wa] L.C. Washington. – « Introduction to Cyclotomic Fields. » Springer–Verlag, New York (1982).