International Journal of Number Theory
Vol. 3, No. 2 (2007) 217–229

World Scientific
www.worldscientific.com

UNE MINORATION POUR L'EXPOSANT DU GROUPE DES CLASSES D'UN CORPS ENGENDRÉ PAR UN NOMBRE DE SALEM

FRANCESCO AMOROSO

Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen, Campus II, BP 5186
14032 Caen Cédex, France
francesco.amoroso@math.unicaen.fr

Received 11 April 2006
Accepted 14 June 2006

In this article we extend the main result of [2] concerning lower bounds for the exponent of the class group of CM-fields. We consider a number field K generated by a Salem number α. If k denotes the field fixed by $\alpha \mapsto \alpha^{-1}$ we prove, under the generalized Riemann hypothesis for the Dedekind zeta function of K, lower bounds for the relative exponent $e_{K/k}$ and the relative size $h_{K/k}$ of the class group of K with respect to the class group of k.

Keywords: Salem numbers; class group.

Mathematics Subject Classification 2000: 11R29, 11G50

1. Introduction

Soit K un corps CM. Dans [3] nous avons montré (sous GRH) que l'exposant du groupe de classe de K tend vers l'infini avec le discriminant. Nous nous proposons ici de généraliser ce résultat à des corps engendrés par un nombre algébrique α ayant la plupart de ses conjugués sur le cercle unité.

Soit α un nombre algébrique réciproque; donc α^{-1} est un conjugué de α et l'application $\alpha \mapsto \alpha^{-1}$ s'étend à une $\mathbb{Q}$-involution τ du corps $K = \mathbb{Q}(\alpha)$; soit k le sous-corps de K fixé par τ. Soient E_K, d, (r_1, r_2) et Δ respectivement le groupe des unités, le degré $[K : \mathbb{Q}]$, la signature et le discriminant de K. Notons s le nombre de places archimédiennes v de K tels que $|\alpha|_v = 1$ et posons

$$r' = (r_1 + r_2 + 1 - s)/2.$$

Soit enfin[a]

$$\delta = \min\{h(u_1) + \cdots + h(u_{r'})\}$$

où $h(\cdot)$ est la hauteur de Weil (logarithmique et absolue) et où le minimum est pris sur le sous-groupe

$$E'_K = \{u^{1-\tau} \text{ t.q. } u \in E_K\}$$

de rang r' (cf. proposition 2.3). Le théorème principal de cet article donne (sous GRH) une minoration pour l'exposant relatif $e_{K/k}$ du groupe des classes de K par rapport à celui de k, i.e. pour le plus petit entier e tel que pour tout idéal fractionnaire I de K, il existe $\alpha \in K$ tel que $(\alpha)I^e$ soit l'extension d'un idéal fractionnaire de k. Ce théorème donne également une minoration pour le quotient h_K/h_k du nombre de classes de K et de celui de k.

Théorème 1.1. *Soit $\varepsilon > 0$; il existe alors une constante $C > 0$ et deux réels $C_\varepsilon > 0$ et $H_\varepsilon > 1$, dépendants de ε, tels que, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K,*

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

et:

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

Il est facile de voir qu'un corps CM peut être engendré par un nombre algébrique α ayant tous ses conjugués sur le cercle unité (cf. par exemple [5, proposition 1]). Le résultat principal de [3] est donc un corollaire de ce théorème (avec $r' = \delta = 0$).

Un autre cas remarquable est celui d'un nombre de Salem α, i.e. un nombre algébrique réel $\alpha > 1$ réciproque et tel que tous ses conjugués, à l'exception de $\alpha^{\pm 1}$, soient de module 1. En effet dans ce cas E'_K est engendré par $\alpha^2 = \alpha/\alpha^{-1}$ et donc $r' = 1$ et $\delta \leq 2h(\alpha) = 2(\log\alpha)/d$. On obtient donc du théorème 1.1 :

Corollaire 1.2. *Soit α un nombre de Salem, $K = \mathbb{Q}(\alpha)$ et $k = \mathbb{Q}(\alpha + \alpha^{-1})$. Soit $\varepsilon > 0$; il existe alors une constante absolue $C > 0$ et deux réels $C_\varepsilon > 0$ et $H_\varepsilon > 1$ dépendants de ε tels que, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K,*

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

[a]Avec la convention: $\delta = 0$ si $r' = 0$.

Chimburg [5] a montré une minoration pour le quotient h_K/h_k ; le théorème 1.1 donne :

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

minoration légèrement plus faible que celle obtenue dans *op. cit.* avec des méthodes entièrement différentes. Aucun résultat sur l'exposant du groupe des classes d'un corps engendré par un nombre de Salem n'était apparemment connu.

2. Notations et Préliminaires

Nous étudions dans ce paragraphe des corps engendrés par un nombre réciproque ayant beaucoup de ses conjugués sur le cercle unité. Les corps CM et les corps engendrés par un nombre de Salem en sont un exemple.

Soit K un corps de nombres muni d'une $\mathbb{Q}$-involution τ (i.e. un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\alpha)$ d'ordre 2) et soit k le sous-corps de K fixé par τ. Soient (r_1, r_2) et (r_1^τ, r_2^τ) les signatures de K et k respectivement. Notons E_K le groupe des unités de K et M_K l'ensemble des places de K ; pour toute $v \in M_K$ 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 :

$$\prod_{v \in M_K} |\alpha|_v^{d_v} = 1, \quad \alpha \in K^*$$

soit satisfaite.

Définition 2.1. On note s le nombre des places archimédiennes imaginaires de K qui sont au dessus d'une place réelle de k. On pose également $r' = (r_1 + r_2 - s)/2$.

En particulier, si K est un corps CM et τ est la conjugaison complexe on a $r' = 0$, tandis que si α est un nombre de Salem et si τ est la $\mathbb{Q}$-involution de $K = \mathbb{Q}(\alpha)$ qui envoie α dans α^{-1}, alors $r' = 1$.

Au dessus d'une place réelle de k il y a ou bien deux places réelles de K, ou bien une place imaginaire; par ailleurs au dessus d'une place imaginaire il y a une place imaginaire. Donc :

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

Soit σ un plongement imaginaire de K ; alors $\sigma\tau = \overline{\sigma}$ si et seulement si σ prolonge un plongement réel de k. On peut donc numéroter les places de K de la façon suivante[b] :

$$v_1, \ldots, v_{r'}, v_1\tau, \ldots, v_{r'}\tau, w_1, \ldots, w_s$$

où $w_j\tau = w_j$ pour $j = 1, \ldots, s$. Les places w_j sont précisément les places associées aux plongements σ qui satisfont $\sigma\tau = \overline{\sigma}$. De plus $d_{v_j} = d_{v_j\tau}$ et $d_{w_j} = 2$.

[b]Pour une place archimédienne v associée au plongement σ on note $v\tau$ la place associée à $\sigma\tau$.

Proposition 2.2. *Soit α un générateur de K. Alors*:

(i) *Supposons $\exists i \in \{1,\dots,s\}$ tel que $|\alpha|_{w_i} = 1$. Alors, $\alpha^\tau = \alpha^{-1}$ et $\forall j \in \{1,\dots,s\}$ on a $|\alpha|_{w_j} = 1$.*

(ii) *Supposons $\alpha^\tau = \alpha^{-1}$ et $|\alpha|_v = 1$ pour une place archimédienne v. Alors $v \in \{w_1,\dots,w_s\}$ et $\forall j \in \{1,\dots,s\}$ on a $|\alpha|_{w_j} = 1$.*

Démonstration. Montrons (i). Soient σ_j $(j = 1,\dots,s)$ les plongements imaginaires du corps K, deux à deux non conjugués, qui prolongent des plongements réels de k. Par hypothèse $\exists i \in \{1,\dots,s\}$ tel que $\sigma_i(\alpha)\overline{\sigma_i}(\alpha) = 1$ et donc $\sigma_i(\alpha^{-1}) = \overline{\sigma_i}(\alpha) = \sigma_i\tau(\alpha)$, ce qui implique $\alpha^{-1} = \alpha^\tau$. Soit maintenant

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

le polynôme minimal de α sur k; P^{σ_i} est à coefficients réels et ses racines sont de module 1: donc son terme constant vaut 1 et $c = 1$. Mais alors, si $j \in \{1,\dots,s\}$, on a que $\sigma_j(b) \in \mathbb{R}$ et $\sigma_j(\alpha) \notin \mathbb{R}$, d'où $|\sigma_j(\alpha)| = 1$.

Montrons maintenant (ii). Supposons donc $\alpha^\tau = \alpha^{-1}$ et $|\alpha|_v = 1$ pour une place archimédienne v. Soit σ le plongement associée à v. Alors, $\overline{\sigma}(\alpha) = \sigma(\alpha^{-1}) = \sigma\tau(\alpha)$ et donc $\overline{\sigma} = \sigma\tau$, d'où $v \in \{w_1,\dots,w_s\}$. Le point (i) montre alors que $|\alpha|_{w_j} = 1$ pour $j \in \{1,\dots,s\}$. □

Soit $w \in \{w_1,\dots,w_s\}$. Il existe alors un générateur α de $K/\mathbb{Q}$ tel que $|\alpha|_w = 1$ (voir par exemple [4, proposition 1]). La proposition précédente montre en particulier que pour tout ces α on a :

$$v \mid \infty,\ |\alpha|_v = 1 \Leftrightarrow v \in \{w_1,\dots,w_s\}.$$

Proposition 2.3. *Pour $j = 1,\dots,s$ et pour $\alpha \in K^*$ on a $|\alpha^{1-\tau}|_{w_j} = 1$. De plus,*

$$E'_K = \{u^{1-\tau} t.q. u \in E_K\}$$

est un sous-groupe du groupe des unités de rang r'.

Démonstration. La première affirmation est clair. Pour montrer la deuxième, soit

$$H = \{\mathbf{x} \in \mathbb{R}^{r_1+r_2} \text{ t.q. } x_1 + \cdots + x_{r_1+r_2} = 0\}$$

et $\mathcal{L} : E_K \to H$ le plongement logarithmique défini par

$$\begin{aligned}\mathcal{L}(\alpha) = (&d_{v_1} \log|\alpha|_{v_1}, \dots, d_{v_{r'}} \log|\alpha|_{v_{r'}},\\ &d_{v_1} \log|\alpha|_{v_1\tau}, \dots, d_{v_{r'}} \log|\alpha|_{v_{r'}\tau},\\ &2\log|\alpha|_{w_1}, \dots, 2\log|\alpha|_{w_s}).\end{aligned}$$

Soit également

$$\begin{aligned}H' = \{\mathbf{y} \in \mathbb{R}^{r_1+r_2} \text{t.q. } &y_1 + y_{1+r'} = \cdots = y_{r'} + y_{2r'} = 0,\\ &y_{2r'+1} = \cdots = y_{r_1+r_2} = 0\}\end{aligned}$$

et f l'endomorphisme de $\mathbb{R}^{r_1+r_2}$ défini par

$$\begin{aligned} f(\mathbf{x}) = (&x_1 - x_{1+r'}, \ldots, x_{r'} - x_{2r'}, \\ &- x_1 + x_{1+r'}, \ldots, -x_{r'} + x_{2r'}, 0, \ldots, 0). \end{aligned}$$

On vérifie alors que $f(H) = H'$ et $(f \circ \mathcal{L})(u) = \mathcal{L}(u^{1-\tau})$. Par le théorème de Dirichlet $\mathcal{L}(E'_K) = f(\mathcal{L}(E_K))$ est un réseau dans H' et donc E'_K est de rang $\dim(H') = r'$. □

Nous terminons ce paragraphe avec le lemme suivant qui permet de minorer h_K/h_k en fonction de l'ordre de $\mathcal{C}l(K)/j\mathcal{C}l(k)$.

Lemme 2.4. *Notons $j : \mathcal{C}l(k) \to \mathcal{C}l(K)$ le morphisme d'extension d'idéaux. Alors,*

$$|\ker j| \leq 2^{1+r'}.$$

Démonstration. Nous suivons la preuve du théorème 10.3 de [8]. Soit I un idéal de k et supposons $j(I)$ principal dans K, disons $j(I) = (\alpha)$. On a $I^{1-\tau} = \mathcal{O}_K$, et donc $\alpha^{1-\tau} \in E_K$. De plus, $\alpha^{1-\tau}$ ne dépend pas du représentant de la classe de I dans $\mathcal{C}l(k)$. Notons

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

et supposons $\alpha^{1-\tau} \in G^2$, où $G^2 = \{g^2 \text{ t.q. } g \in G\}$. Il existe donc $v \in E_k$ et $\beta \in K^*$ tels 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 $\alpha v^{-1} \in k$ et $I = (\alpha v^{-1})$ est principal dans k. On a montré que l'application $\ker j \to G/G^2$ qui envoie la classe de I dans la classe de $\alpha^{1-\tau}$ est injective. Le groupe G/G_{tors} est libre de rang $\leq r'$ (en effet, dans le notation de la proposition 2.3, $\mathcal{L}(G) \subseteq H'$ et donc G est de rang $\leq r'$) et donc

$$|\ker j| \leq [G : G^2] \leq 2^{1+r'}.$$

□

Nous terminons ce paragraphe avec le lemme suivant :

Lemme 2.5. *Soit K un corps de nombres et soit τ une $\mathbb{Q}$-involution de K. Soit ensuite P un idéal premier de $\mathcal{O}_K$ de degré 1 sur $\mathbb{Q}$ et non ramifié. Alors, $P^\tau \neq P$.*

Démonstration. Analogue à celle du lemme 3.2 de [3]. □

3. Géométrie des Nombres

Soit, comme dans le paragraphe qui précède, K un corps de nombres muni d'une $\mathbb{Q}$-involution τ et $E'_K = \{u^{1-\tau} \text{ t.q. } u \in E_K\}$ le sous-groupe de rang r' du groupe des unités de K.

Définition 3.1. On note[c]

$$\delta = \min\{h(u_1) + \cdots + h(u_{r'})\}$$

où $h(\cdot)$ est la hauteur de Weil (logarithmique et absolue) et où le minimum est pris sur les familles d'unités de E'_K multiplicativement indépendantes.

Soit I un idéal fractionnaire de K et v une place non-archimédienne de K, associé à un idéal premier P de l'anneau des entiers $\mathcal{O}_K$. On pose :

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

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

$$\prod_{v \nmid \infty} |I|_v^{d_v} = (N_{\mathbb{Q}}^K I)^{-1}$$

et, pour $\alpha \in K$,

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

La proposition suivante permet de construire des nombre algébrique de petite hauteur.

Proposition 3.2. *Supposons qu'il existe $\gamma_1, \ldots, \gamma_t \in K^*$ et des idéaux*

$$I_1, \ldots, I_t \subseteq \mathcal{O}_K$$

de norme $\leq x$ tels que les $(\gamma_j)^{-1} I_j$ soient des extensions d'idéaux fractionnaires de k. Soient ensuite m et N deux entiers strictement positifs et tels que :

$$mN^{r'} < t.$$

Alors il existe $m+1$ indices $j_0, j_1, \ldots, j_m \in \{1, \ldots, t\}$ deux à deux distincts et des unités $u_1, \ldots, u_m \in E'_K$ tels que :

$$h(u_i \gamma_{j_i}^{1-\tau} \gamma_{j_0}^{\tau-1}) \leq \frac{2 \log x}{[K : \mathbb{Q}]} + \frac{\delta}{N}$$

pour $i = 1, \ldots, m$.

Démonstration. Soient $u_1, \ldots, u_{r'}$ des unités multiplicativement indépendantes de E'_K telles que :

$$h(u_1) + \cdots + h(u_{r'}) = \delta$$

[c] Avec la convention: $\delta = 0$ si $r' = 0$.

et soient $v_1, \ldots, v_{r'}$ les places définie dans la discussion qui suit la définition 2.1. Notons $\mathcal{L}' : K^* \to \mathbb{R}^{r'}$ l'application définie par

$$\mathcal{L}'(\alpha) = (d_{v_j} \log |\alpha|_{v_j})_{j=1,\ldots,r'}.$$

Les vecteurs $\mathcal{L}'(u_1), \ldots, \mathcal{L}'(u_{r'})$ sont alors linéairement indépendants. Notons également :

$$P = \{\lambda_1 \mathcal{L}'(u_1) + \cdots + \lambda_{r'} \mathcal{L}'(u_{r'}) \text{ t.q. } 0 \leq \lambda_1, \ldots, \lambda_{r'} < 1\}.$$

Quitte à remplacer les $\gamma_1, \ldots, \gamma_t$ par $w_1\gamma_1, \ldots, w_t\gamma_t$ avec $w_1, \ldots w_t \in E_K$, on peut supposer que

$$\mathcal{L}'(\gamma_1^{1-\tau}), \ldots, \mathcal{L}'(\gamma_t^{1-\tau}) \in P.$$

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

$$\mathcal{L}'(\gamma_{j_0}^{1-\tau}), \mathcal{L}'(\gamma_{j_1}^{1-\tau}), \ldots, \mathcal{L}'(\gamma_{j_m}^{1-\tau}) \in \underline{a} + N^{-1}P.$$

Remarquons que si $\alpha \in K^*$ et $\beta = \alpha^{1-\tau}$, alors :

$$\sum_{v|\infty} d_v \log^+ |\beta|_v = \|\mathcal{L}'(\beta)\|_1$$

où $\| \cdot \|_1$ est la norme L_1. Soit $i \in \{1, \ldots, m\}$; on a donc :

$$\begin{aligned}\sum_{v|\infty} d_v \log^+ |\gamma_{j_i}^{1-\tau}\gamma_{j_0}^{\tau-1}|_v &= \|\mathcal{L}'(\gamma_{j_i}^{1-\tau}\gamma_{j_0}^{\tau-1})\|_1 \\ &\leq \frac{1}{N}(\|\mathcal{L}'(u_1)\|_1 + \cdots + \|\mathcal{L}'(u_{r'})\|_1) \\ &= \frac{[K:\mathbb{Q}]}{N}(h(u_1) + \cdots + h(u_{r'}))\ ,\end{aligned}$$

d'où

$$\sum_{v|\infty} d_v \log^+ |\gamma_{j_i}^{1-\tau}\gamma_{j_0}^{\tau-1}|_v \leq \frac{[K:\mathbb{Q}]}{N}\delta. \tag{3.1}$$

Remarquons maintenant que, pour $v \nmid \infty$, on a $|\gamma_j^{1-\tau}|_v = |I_j^{1-\tau}|_v$ car

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

Donc

$$\begin{aligned}\log |\gamma_{j_i}^{1-\tau}\gamma_{j_0}^{\tau-1}|_v &= (\log |I_{j_i}|_v - \log |I_{j_0}|_v) - (\log |I_{j_i}^{\tau}|_v - \log |I_{j_0}^{\tau}|_v) \\ &\leq -\log |I_{j_0}|_v - \log |I_{j_i}^{\tau}|_v\end{aligned}$$

car les I_j sont des idéaux entiers. Soit $i \in \{1, \ldots, m\}$; on a alors,

$$\begin{aligned}\sum_{v\nmid\infty} d_v \log^+ |\gamma_{j_i}^{1-\tau}\gamma_{j_0}^{\tau-1}|_v &\leq \sum_{v\nmid\infty} d_v(-\log |I_{j_0}|_v - \log |I_{j_i}^{\tau}|_v) \\ &\leq 2 \log x\end{aligned}$$

qui donne, avec la majoration (3.1),

$$h(\gamma_{j_i}^{1-\tau}\gamma_{j_0}^{\tau-1}) \leq \frac{2\log x}{[K:\mathbb{Q}]} + \frac{\delta}{N}.$$

□

Remarque 3.3. Si K est un corps CM et τ est la conjugaison complexe, alors $r' = 0$. Dans ce cas limite, la proposition 3.2 reste valable trivialement. Plus précisément, on obtient :

$$h\big(\gamma_j^{1-\tau}\big) \leq \frac{\log x}{[K:\mathbb{Q}]}$$

pour $j = 1, \ldots, t$.

4. Taille de Certains Groupes des Classes

Soit G un groupe abélien fini; rappelons la définition suivante (cf. [3]). Pour l entier strictement positif notons $\mathcal{M}_G(l)$ le plus petit entier A tel que pour tout $g_1, \ldots, g_l \in G$ il existe $\rho_1, \ldots, \rho_l \in \mathbb{Z}$ tels que :

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

On déduit d'une minoration de la fonction $\mathcal{M}_G(l)$ des renseignements sur l'exposant

$$e_G = \min\{e \in \mathbb{N}^* \text{ t.q. } \forall g \in G,\ g^e = 1\}$$

du groupe G et sur son cardinal $|G|$. En effet,

$$\mathcal{M}_G(1) = e_G \quad \text{et} \quad \mathcal{M}_G(|G|) \leq 2 \tag{4.2}$$

(cf. [3, lemma 5.1]).

Proposition 4.1. *Soit K un corps de nombre de degré $d = [K:\mathbb{Q}]$ et discriminant Δ. Soit τ une $\mathbb{Q}$-involution de K. Soient r' et δ comme dans la définition* 3.1, *et soit $\varepsilon > 0$. Il existe alors une constante absolue $C > 0$ et un réel $C_\varepsilon > 0$ dépendant de ε tels que, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K,*

$$\mathcal{M}_{\mathcal{C}l(K)/j\mathcal{C}l(k)}(l) \geq \frac{\max(Cd^{-1}\log|\Delta|, C_\varepsilon d^{1-\varepsilon})}{\log l + \log\log|\Delta| + r'\log(2 + d\delta/(r'+1))} \tag{4.3}$$

où $j\colon \mathcal{C}l(k) \to \mathcal{C}l(K)$ est le morphisme d'extension. De plus, si $K/\mathbb{Q}$ est abélienne, alors on peut choisir $\varepsilon = 0$ dans (4.3).

Démonstration. Nous reprenons largement les arguments de la preuve du théorème 1.1 de [3]. Posons $G = \mathcal{C}l(K)/j\mathcal{C}l(k)$. On peut évidemment supposer $\varepsilon < 1/2$. Remarquons également qu'il suffit de montrer qu'il existe une constante $C' > 0$ et un réel $C_\varepsilon > 0$ tels que,

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

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) Montrons l'inégalité :

$$\mathcal{M}_G(l) \geq \frac{C'(d^{-1}\log|\Delta| - \log d)}{\log l + \log\log|\Delta| + r'\log(2 + d\delta/(r'+1))}.$$

Une application standard de la version effective du théorème des nombres premiers dans un corps de nombres (voir [6] 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 $\subset \mathcal{O}_K$ de norme $\leq x$, de degré 1 sur $\mathbb{Q}$ et non ramifiés (voir [2, lemme 2.1]). Notons

$$t = 1 + (1 + [d\delta/(r'+1)])^{r'}$$

et soit $c_3 \geq 1$ tel que $\frac{c_3}{\log c_3 + 2} \geq c_2$. Chosissons

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

on a en particulier $x \geq c_3 y\log y \geq e$, où l'on a noté $y = ltd \geq 3$, et donc :

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

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

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

avec $\rho_{ij} \in \mathbb{Z}$. Soit $A = \max_j \sum_i |\rho_{ij}|$; donc pour $j = 1,\ldots,t$ il existe $\gamma_j \in K^*$ tel que

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

soit l'extension d'un idéal fractionnaire de norme $\leq x^A$ de k.

Choisissons $m = 1$ et $N = 1 + [d\delta/(r'+1)]$ dans la proposition 3.2; cette dernière nous assure l'existence d'une unité $u \in E'_K$ et de deux indices j_0, $j_1 \in \{1,\ldots,t\}$ avec $j_0 \neq j_1$ tels que la hauteur de $\alpha = u\gamma_{j_1}^{1-\tau}\gamma_{j_0}^{\tau-1}$ satisfasse :

$$h(\alpha) \leq \frac{2A\log x + r' + 1}{d}.$$

Remarquons que :

$$\log x \leq c_4(\log(ltd) + \log\log|\Delta|)$$

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

$$\begin{aligned}\log x &\leq c_6(\log(lt) + \log\log|\Delta|)\\ &\leq c_7(\log l + \log\log|\Delta| + r'\log(2 + d\delta/(r'+1))).\end{aligned}$$

On a donc :

$$h(\alpha) \leq c_8 A\,\frac{\log l + \log\log|\Delta| + r'\log(2 + d\delta/(r'+1))}{d}. \tag{4.4}$$

Montrons maintenant :

Sour-Lemme 4.2. *α est un générateur de K.*

Démonstration. Il est suffisant de montrer que $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq d$. Quitte à renuméroter les indices, on peut supposer $\rho = \rho_{1,j_1} \neq 0$. Soit L la clôture galoisienne de K dans $\overline{\mathbb{Q}}$ et notons $P = P_{1,j_1}$. Le lemme 3.1 de [3] nous assure que $P\mathcal{O}_L$ possède au moins d conjugués distincts

$$\sigma_1(P\mathcal{O}_L), \ldots, \sigma_d(P\mathcal{O}_L).$$

Supposons que pour certains $\iota, \kappa \in \{1, \ldots, d\}$ on ait $\alpha^{\sigma_\iota} = \alpha^{\sigma_\kappa}$. Alors :

$$\begin{aligned}&\prod_{i=1}^{l} \sigma_\iota\big(P_{i,j_1}^{1-\tau}\mathcal{O}_L\big)^{\rho_{i,j_1}} \sigma_\iota\big(P_{i,j_0}^{\tau-1}\mathcal{O}_L\big)^{\rho_{i,j_0}}\\ &\qquad = \prod_{i=1}^{l} \sigma_\kappa\big(P_{i,j_1}^{1-\tau}\mathcal{O}_L\big)^{\rho_{i,j_1}} \sigma_\kappa\big(P_{i,j_0}^{\tau-1}\mathcal{O}_L\big)^{\rho_{i,j_0}}.\end{aligned}$$

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

$$\sigma_\iota\big(P^{1-\tau}\mathcal{O}_L\big)^{\rho} = \sigma_\kappa\big(P^{1-\tau}\mathcal{O}_L\big)^{\rho}.$$

Donc :

$$\sigma_\iota\big(P\mathcal{O}_L\big)^{\rho}\sigma_\kappa\big(P^{\tau}\mathcal{O}_L\big)^{\rho} = \sigma_\iota\big(P^{\tau}\mathcal{O}_L\big)^{\rho}\sigma_\kappa\big(P\mathcal{O}_L\big)^{\rho}.$$

Par le lemme 2.5, $P \neq P^\tau$ et donc $P\mathcal{O}_L$ et $P^\tau\mathcal{O}_L$ sont premiers entre eux. On en déduit que :

$$\sigma_\iota(P\mathcal{O}_L) = \sigma_\kappa(P\mathcal{O}_L),$$

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

Nous avons montré que α est un générateur de K ; un résultat de J. Silverman (voir [7, theorem 2, p. 397] avec $F = \mathbb{Q}$, $n = 1$, $\alpha_0 = 1$ et $\alpha_1 = \alpha$) donne alors la minoration :

$$h(\alpha) \geq \frac{d^{-1}\log|\Delta| - \log d}{2(d-1)}. \tag{4.5}$$

Le résultat désiré découle de 4.4 et 4.5.

(II) Montrons maintenant l'inégalité :

$$\mathcal{M}_G(l) \geq \frac{C_\varepsilon d^{1-\varepsilon}}{\log l + \log\log|\Delta| + r'\log\big(2 + d\delta/(r'+1)\big)}.$$

Pour ce faire, rappelons d'abord le résultat principal de [1] : si $\alpha_1, \ldots, \alpha_m \in K^*$ sont multiplicativement indépendants,

$$\max_{s=1,\ldots,m} h(\alpha_s) \geq c_9(m)^{-1} d^{-1/m} \log(3d)^{-k(m)}$$

où $k(m) > 0$. Posons maintenant $m = [1/\varepsilon] + 1$. Donc :

$$c_9(m) d^{1/m} \log(3d)^{k(m)} \leq c_{10}(\varepsilon) d^{\varepsilon}.$$

Posons aussi $N = 1 + [d\delta/(r'+1)]$, $t = 1 + mN^{r'}$ et

$$x = 2c_3 lmt \log(lm) + c_1(\log|\Delta|)^2(\log\log|\Delta|)^4.$$

Le résultat de [6] déjà utilisé dans la partie I de la preuve, montre qu'il existe $2lmt$ idéaux premiers distincts $P_{ij} \subseteq \mathcal{O}_K$ $(i = 1, \ldots, l;\ j = 1, \ldots, 2mt)$ de norme $\leq x$, de degré 1 sur $\mathbb{Q}$ et non ramifiés. Nous pouvons supposer $P_{ij} \neq P_{i'j'}^{\tau}$ pour $(i,j) \neq (i,j)$ et $1 \leq j, j' \leq mt$. De plus $P_{ij} \neq P_{ij}^{\tau}$ par le lemme 2.5 et donc

$$P_{ij} \neq P_{i'j'}^{\tau} \quad (i, i' = 1, \ldots, l;\ j, j' = 1, \ldots, mt). \tag{4.6}$$

Soit g_{ij} la classe de P_{ij} dans G et supposons qu'il existe des relations multiplicatives

$$g_{1j}^{\rho_{1j}} \cdots g_{lj}^{\rho_{lj}} = 1 \quad (j = 1, \ldots, mt)$$

avec $\rho_{ij} \in \mathbb{Z}$ et $(\rho_{1j}, \ldots, \rho_{lj}) \neq (0, \ldots, 0)$ pour $j = 1, \ldots, mt$. Soit $A = \max_j \sum_i |\rho_{ij}|$; donc pour $j = 1, \ldots, mt$ il existe $\gamma_j \in K^*$ tel que

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

soit l'extension d'un idéal fractionnaire de norme $\leq x^A$ de k.

La proposition 3.2 nous assure l'existence de $m+1$ indices $j_0, j_1, \ldots, j_m \in \{1, \ldots, t\}$ deux à deux distincts et de certaines unités $u_1, \ldots, u_m \in E'_K$ tels que les hauteurs des $\alpha_s = u_s \gamma_{j_s}^{1-\tau} \gamma_{j_0}^{\tau-1}$ satisfassent :

$$h(\alpha_s) \leq \frac{2A\log x + r' + 1}{d}$$

pour $s = 1, \ldots, m$. Comme dans la première partie de la preuve,

$$\begin{aligned} \log x &\leq c_{11}(\log(lmt) + \log\log|\Delta|) \\ &\leq c_{12}(\varepsilon)(\log l + \log\log|\Delta| + r'\log(2 + d\delta/(r'+1))). \end{aligned}$$

On a donc :

$$\begin{aligned} &\max_{s=1,\ldots,m} h(\alpha_s) \\ &\quad \leq 2c_{12}(\varepsilon) A \,\frac{\log l + \log\log|\Delta| + r'\log(2 + d\delta/(r'+1))}{d}. \end{aligned} \tag{4.7}$$

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

$$\prod_{s=1}^{m} \left(u_s \gamma_{j_s}^{1-\tau} \gamma_{j_0}^{\tau-1}\right)^{e_s} = 1.$$

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

$$\prod_{s=1}^{m} \left(P_{1j_s}^{\rho_{1j_s}(1-\tau)} \cdots P_{lj_s}^{\rho_{lj_s}(1-\tau)}\right)^{e_s} = \left(P_{1j_0}^{\rho_{1j_0}(1-\tau)} \cdots P_{lj_0}^{\rho_{lj_0}(1-\tau)}\right)^{e_1+\cdots+e_m}.$$

La condition (4.6) nous assure que $e_1 = \cdots = e_m = 0$. Le résultat principal de [1] donne alors :

$$\max_{s=1,\dots,m} h(\alpha_s) \geq c_{10}(\varepsilon)^{-1} d^{-\varepsilon}. \tag{4.8}$$

Le résultat désiré découle de (4.7) et (4.8).

(III) Enfin, si $K/\mathbb{Q}$ est abélienne, on peut utiliser la minoration de la hauteur montrée dans [2] à la place du résultat principal de [1], ce qui permet, comme dans la preuve du théorème principal de [3], de pouvoir choisir $\varepsilon = 0$. □

Remarque 4.3. Soit Γ le groupe des $\mathbb{Q}$-automorphismes de K et soit $\phi = \sum_{\tau\in\Gamma} \phi_\tau \tau \in \mathbb{Z}[\Gamma]$. Notons

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

Soit r' le rang du sous-groupe $\phi(E_K)$ de E_K et $\delta = \min\left\{h(u_1) + \cdots + h(u_{r'})\right\}$, le minimum étant pris sur les familles d'unités de $\phi(E_K)$ multiplicativement indépendantes. Les résultats de la proposition 4.1 se généralisent à des familles de corps K tels qu'il existe $\phi \in \mathbb{Z}[\Gamma]$ qui satisfait

$$\|\phi\|_1 r' \log\big(d\delta/(r'+1) + 2\big) = o(d). \tag{4.9}$$

En particulier (4.9) implique

$$\|\phi\|_1 r' < d.$$

Il serait intéressant d'exhiber des exemples de familles des corps (autres que les corps considérés dans cet article) satisfaisants cette dernière inégalité.

5. Preuves du Théorème 1.1

On applique la proposition 4.1 en tenant compte des relations (4.2). On obtient donc :

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

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

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

Le lemme 2.4 montre que $\log(h_K/h_k) \geq \log l - (r'+1)\log 2$; donc :

$$\begin{aligned}\log(h_K/h_k) \;&\geq \frac{1}{2}\max(Cd^{-1}\log|\Delta|, C_\varepsilon d^{1-\varepsilon}) - \log\log|\Delta| \\ &\quad - r'\log(2 + d\delta/(r'+1)) - (r'+1)\log 2 \\ &\geq c_{13}\max(Cd^{-1}\log|\Delta|, C_\varepsilon d^{1-\varepsilon}) - r'\log(4 + 2d\delta/(r'+1))\ ,\end{aligned}$$

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

Remerciements. Je tiens à remercier B. Anglès et J. Boxall pour les discussions que nous avons pu avoir au sujet de cet article. C'est également un plaisir de remercier F. Nuccio, C. Pontreau et G. Ranieri qui ont bien voulu me faire part de leurs commentaires sur une version initiale de ce travail.

Références

[1] F. Amoroso and S. David, Le problème de Lehmer en dimension supérieure, *J. Reine Angew. Math.* **513** (1999) 145–179.
[2] F. Amoroso and R. Dvornicich, A lower bound for the height in Abelian extensions, *J. Number Theory* **80**(2) (2000) 260–272.
[3] F. Amoroso and R. Dvornicich, Lower bounds for the height and size of the ideal class group in CM fields, *Monatsh. Math.* **138**(2) (2003) 85–94.
[4] F. Amoroso and F. Nuccio, Algebraic numbers of small Weil's height in CM-fields: On a theorem of Schinzel, *J. Number Theory*, À paraître.
[5] T. Chinburg, On the arithmetic of two constructions of Salem numbers, *J. Reine Angew. Math.* **348** (1984) 166–179.
[6] J. C. Lagarias and A. M. Odlyzko, Effective versions of the Čebotarev density theorem, in *Algebraic Number Fields*, Durham Symposium, ed. A. Frolich (Academic Press, 1977), pp. 409–464.
[7] J. H. Silverman, Lower bounds for height functions, *Duke Math. J.* **51** (1984) 395–403.
[8] L. C. Washington, *Introduction to Cyclotomic Fields* (Springer-Verlag, New York, 1982).