ACTA ARITHMETICA
115.1 (2004)

Une minoration pour l'exposant du groupe de classes d'idéaux

par

Francesco Amoroso (Caen)

1. Introduction. Nous poursuivons ici l'étude amorcée dans [Amo-Dvo] des applications des minorations de la hauteur de Weil à l'étude des groupes de classes d'idéaux G des corps de nombres. Dans *op. cit.* nous avons montré, sous GRH, que l'exposant du groupe de classe d'un corps CM tends vers l'infini avec le discrimant ; plus précisement ([1]) :

Théorème 1.1. *Soit $K/\mathbb{Q}$ un corps CM et soit E_K l'exposant de son groupe de classes d'idéaux. Alors pour tout $\varepsilon > 0$ et pour tout entier $l \geq 1$, on a, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K,*

$$E_K \geq C_1(\varepsilon)\,\frac{\max\{d_K^{-1}\log|\Delta_K| - \log d_K, d_K^{1-\varepsilon}\}}{\log\log|\Delta_K|},$$

où $C_1(\varepsilon)$ est une fonction positive, effectivement calculable, de ε. De plus, si $K/\mathbb{Q}$ est abélien, alors

$$E_K \geq C_1\,\frac{\max\{d_K^{-1}\log|\Delta_K| - \log d_K, d_K^{1-\varepsilon}\}}{\log\log|\Delta_K|},$$

où C_1 est une constante positive et effectivement calculable.

Nous généralisons ici ce théorème au cas de corps de nombres quelconques. Bien évidemment on verra alors apparaître un terme responsable de la structure du groupe des unités de K ; à la différence des résultats classiques (théorème de Brauer–Siegel) le théorème principal de cet article fait apparaître une quantité δ_K (minimum de la somme des hauteurs de Weil d'un système d'unités multiplicativement indépendantes) qui semble plus

2000 *Mathematics Subject Classification*: 11R29, 11R21.

([1]) Dans cet article, on note d_K, $|\Delta_K|$, R_K respectivement le degré, la valeur absolue du discriminant et le régulateur de K. On note également h_K et E_K le nombres de classes et l'exposant du groupe de classes de K.

fine que le régulateur du corps K et vérifie

$$\mathrm{R}_K \leq (4\delta_K)^r, \quad \delta_K \leq 158 r!\, r^{3/2} (\log d_K) \mathrm{R}_K,$$

où r est le rang de $\mathcal{O}_K^*$.

Notre résultat principal est le suivant :

Théorème 1.2. *Soit K un corps de nombres et soit E_K l'exposant de son groupe de classes d'idéaux. Alors, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K, on a*

$$E_K \geq C_2 \frac{d_K^{-1} \log |\Delta_K| - \log d_K}{\log\log |\Delta_K| + d_K \log(\delta_K + 2)},$$

où C_2 est une constante positive et effectivement calculable. En particulier,

$$E_K \geq C_2(d_K) \frac{\log |\Delta_K|}{\log\log |\Delta_K| + \log \mathrm{R}_K},$$

où $C_2(d_K)$ est une fonction positive et effective.

Ce théorème peut être vu comme un analogue pour l'exposant de la célèbre minoration $h_K \mathrm{R}_K \gg |\Delta_K|^{1/2-\varepsilon}$ conjecturée par Siegel et démontrée par Brauer (cf. [Bra]).

Plusieurs auteurs ont construit des familles infinies de corps de nombres K de petit degré dont l'exposant satisfait (sous GRH)

$$E_K \gg \frac{\log |\Delta_K|}{\log\log |\Delta_K|}. \tag{1.1}$$

Par exemple, Murty (cf. [Mur, paragraphe 7]) montre que les exposants des groupes des classes des corps $K = \mathbb{Q}(\sqrt{m^2+1})$ (où m est un entier strictement positif tel que m^2+1 est sans facteurs carrés) satisfont, sous GRH, (1.1). De même, Louboutin (cf. [Lou1], [Lou2] et [Lou3]) construit trois familles infinies de corps cubiques K (non galoisiens et non totalement réels, galoisiens et totalement réels, non galoisiens et totalement réels respectivement) dont l'exposant satisfait à nouveau (toujours sous GRH) l'inégalité (1.1) (et, de plus, détermine les corps K de ces familles avec $E_K \leq 3$).

En 1956, Ankeny, Brauer et Chowla (voir [Ank-Bra-Cho]) ont montré l'existence d'une famille infinie de corps de nombres K de signature donnée et dont le nombre de classes est très grand : $h_K \gg |\Delta_K|^{1/2-\varepsilon}$. Nous généralisons ici ce résultat à l'exposant :

Corollaire 1.3. *Soient $d \geq 2$ et $r_1, r_2 \geq 0$ entiers tels que $r_1 + 2r_2 = d$. Alors, sous l'hypothèse de Riemann généralisée, il existe une infinité de corps de nombres K de signature (r_1, r_2) et tels que*

$$E_K \geq C_3(d) \frac{\log |\Delta_K|}{\log\log |\Delta_K|},$$

où $C_3(d)$ est une fonction positive et effective.

Remerciements. Je tiens à remercier Yuri F. Bilu dont la conférence au "Symposium on Diophantine Problems in honour of Wolfgang Schmidt" (Vienne 6–10 octobre 2003) a attirée mon attention sur la construction de Ankeny, Brauer et Chowla.

C'est également un plaisir de remercier B. Anglès, J. Cougnard et S. Louboutin qui ont bien voulu me faire part de leurs commentaires sur une version initiale de ce travail.

2. Géométrie des nombres. Soient K un corps de nombres de signature (r_1, r_2) et $r = r_1 + r_2 - 1$ le rang de son groupe des unités $\mathcal{O}_K^*$. Pour toute place v 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. Dans la suite on suppose que les places archimédiennes $v \mid \infty$ sont ordonnées (d'une façon arbitraire).

Notons $\mathcal{L} : K^* \to \mathbb{R}^{r+1}$ le plongement logarithmique

$$\mathcal{L}(\alpha) = (d_v \log |\alpha|_v)_{v|\infty} \quad (\alpha \in K^*),$$

H l'hyperplan $\{\underline{a} \in \mathbb{R}^{r+1} : a_0 + a_1 + \cdots + a_r = 0\}$ et $\underline{e_0} = (d_v/[K : \mathbb{Q}])_{v|\infty}$. Remarquons que pour tout $\alpha \in K^*$ on a

$$\mathcal{L}(\alpha) = (\log |N_{\mathbb{Q}}^K \alpha|)\underline{e_0} + (\pi \circ \mathcal{L})(\alpha),$$

où $\pi : \mathbb{R}^{r+1} \to H$ est la projection

$$\pi(\underline{a}) = \underline{a} - \Big(\sum_{j=0}^{r} a_j\Big)\underline{e_0} \quad (\underline{a} \in \mathbb{R}^{r+1}).$$

Notons $\|\cdot\|_1$ la norme L_1 sur $\mathbb{R}^{r+1}$ et $h(\cdot)$ la hauteur de Weil (logarithmique et absolue). On a alors :

LEMME 2.1. *Pour toute unité $u \in \mathcal{O}_K^*$ on a*

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

De plus, si $\gamma_1, \gamma_2 \in \mathcal{O}_K$ ne sont pas nuls, alors

$$[K : \mathbb{Q}]h(\gamma_1\gamma_2^{-1}) \le \max\{\log |N_{\mathbb{Q}}^K \gamma_1|, \log |N_{\mathbb{Q}}^K \gamma_2|\} + \frac{1}{2}\,\|(\pi \circ \mathcal{L})(\gamma_1\gamma_2^{-1})\|_1.$$

Démonstration. Pour montrer la première assertion, il suffit de remarquer que

$$\sum_{v|\infty} d_v \log^+ |u|_v = \frac{1}{2}\sum_{v|\infty} \big|d_v \log |u|_v\big| = \frac{1}{2}\,\|\mathcal{L}(u)\|_1.$$

Montrons la deuxième. Notons $\alpha = \gamma_1\gamma_2^{-1}$. Alors

$$\begin{aligned}\sum_{v|\infty} d_v \log^+ |\alpha|_v &= \frac{1}{2}\Big(\sum_{v|\infty} d_v \log|\alpha|_v + \sum_{v|\infty} \big|d_v \log|\alpha|_v\big|\Big)\\ &= \frac{1}{2}\left(\log|N_{\mathbb{Q}}^K\alpha| + \|\mathcal{L}(\alpha)\|_1\right)\\ &= \frac{1}{2}\left(\log|N_{\mathbb{Q}}^K\alpha| + \|(\log|N_{\mathbb{Q}}^K\alpha|)\underline{e_0} + (\pi\circ\mathcal{L})(\alpha)\|_1\right)\\ &\le \frac{1}{2}\left(\log|N_{\mathbb{Q}}^K\alpha| + \big|\log|N_{\mathbb{Q}}^K\alpha|\big| + \|(\pi\circ\mathcal{L})(\alpha)\|_1\right)\\ &= \log^+|N_{\mathbb{Q}}^K\alpha| + \frac{1}{2}\|(\pi\circ\mathcal{L})(\alpha)\|_1.\end{aligned}$$

Par ailleurs, en utilisant la formule du produit,

$$\sum_{v\nmid\infty} d_v \log^+|\alpha|_v \le \sum_{v\nmid\infty} d_v(-\log|\gamma_2|_v) = \log|N_{\mathbb{Q}}^K\gamma_2|.$$

Donc

$$\begin{aligned}[K:\mathbb{Q}]h(\alpha) &\le \log|N_{\mathbb{Q}}^K\gamma_2| + (\log|N_{\mathbb{Q}}^K\gamma_1| - \log|N_{\mathbb{Q}}^K\gamma_2|)^+ + \frac{1}{2}\|(\pi\circ\mathcal{L})(\alpha)\|_1\\ &= \max(\log|N_{\mathbb{Q}}^K\gamma_1|, \log|N_{\mathbb{Q}}^K\gamma_2|) + \frac{1}{2}\|(\pi\circ\mathcal{L})(\alpha)\|_1. \ \blacksquare\end{aligned}$$

Soit maintenant U un sous-groupe de $\mathcal{O}_K^*$ d'indice fini. La proposition 2.3, clef de notre travail, fait intervenir d'une façon naturelle la quantité

$$\delta_U = \min_{u_1,\dots,u_r\in U}\{h(u_1)+\cdots+h(u_r)\},$$

où le minimum est pris sur les familles d'unités multiplicativement indépendantes ([2]).

Remarquons que si $U \subseteq V$ sont deux sous-groupes de $\mathcal{O}_K^*$ d'indice fini alors $\delta_V \le \delta_U$; on pose $\delta_K = \delta_{\mathcal{O}_K^*}$.

LEMME 2.2. *On a* $\mathrm{R}_U \le (4\delta_U)^r$ *et*

$$\delta_U \le 158 r!\, r^{3/2}(\log d)\mathrm{R}_U,$$

où $d = [K:\mathbb{Q}]$ *et où* r *est le rang de* $\mathcal{O}_K^*$.

Démonstration. Soit $u_1,\dots,u_r$ un système de générateurs de U/U_{tors} tel que

$$h(u_1)+\cdots+h(u_r) = \delta_U.$$

On a

$$\mathrm{R}_U \le \left|\det\begin{pmatrix}(d_v\log|u_j|_v)_{v|\infty,\,j=1,\dots,r}\\ (d_v/d)_{v|\infty}\end{pmatrix}\right|.$$

([2]) On remarquera que le minimum est atteint sur un système de générateurs de $\mathcal{O}_K^*$.

En utilisant l'inégalité d'Hadamard et l'inégalité algébro-géométrique, on en déduit que

$$\mathrm{R}_U \le \Big(\sum_{v|\infty}(d_v/d)^2\Big)^{1/2}\prod_{j=1}^{r}\Big\{\sum_{v|\infty}(d_v\log|u_j|_v)^2\Big\}^{1/2}\le\prod_{j=1}^{r}\Big\{\sum_{v|\infty}d_v\big|\log|u_j|_v\big|\Big\}$$
$$=\prod_{j=1}^{r}\{2dh(u_j)\}\le\left(\frac{2d}{r}\sum_{j=1}^{r}h(u_j)\right)^r\le(4\delta_U)^r,$$

ce qui montre la première assertion. Montrons maintenant la seconde. Soit $\widetilde{\pi}:\mathbb{R}^{r+1}\to\mathbb{R}^r$ la projection sur les r premières cordonnées. On vérifie immédiatement que $\Lambda=(\widetilde{\pi}\circ\mathcal{L})(U)$ est un réseau de $\mathbb{R}^r$ et que $\mathrm{Vol}(\mathbb{R}^r/\Lambda)=\mathrm{R}_U$. Rappelons aussi que

$$\mathrm{Vol}(\{\underline{a}\in\mathbb{R}^r:\|\underline{a}\|_1\le 1\})=2^r/r!.$$

Le théorème de Minkowski assure donc l'existence de r unités multiplicativement indépendantes $u_1,\dots,u_r\in U$ telles que

$$\prod_{i=1}^{r}\|(\widetilde{\pi}\circ\mathcal{L})(u_i)\|_1\le r!\,\mathrm{R}_U.$$

Si $\underline{a}\in H$, on a $\|\underline{a}\|_1\le 2\|\widetilde{\pi}(\underline{a})\|_1$, et donc, par la première assertion du lemme 2.1,

$$\prod_{i=1}^{r}h(u_i)\le r!\,d^{-r}\mathrm{R}_U. \tag{2.1}$$

Le raffinement de T. Loher et D. Masser (cf. [Loh-Mas, Corollary 3.1]) d'un résultat de E. M. Matveev ([Mat]) donne

$$\prod_{i=1}^{r-1}h(u_i)^{-1}\le\frac{58(r-1)!\,e^r}{(r-1)^{r-1}}\,d^r\log d\le 58e\sqrt{r}\,d^r\log d.$$

Supposons $h(u_1)\le\cdots\le h(u_r)$; on a donc

$$\delta_U\le h(u_1)+\cdots+h(u_r)\le rh(u_r)\le r(58e\sqrt{r}\,d^r\log d)r!\,d^{-r}\mathrm{R}_U$$
$$\le 158r!\,r^{3/2}(\log d)\,\mathrm{R}_U.\ \blacksquare$$

Remarquons que dans certains cas on peut considérablement améliorer la majoration de δ_U du lemme précédent. Par exemple, si K est un corps totalement réel, alors

$$h(\alpha)\ge c:=\frac{1}{2}\log\frac{1+\sqrt{5}}{2}\in\,]0,1[$$

pour tout $\alpha\in K\backslash\{-1,0,1\}$, et donc l'argument du lemme 2.2 conduit à la majoration suivante :

$$\delta_U\le rc^{-(r-1)}r!\,d^{-r}\mathrm{R}_U\le(d-1)^{3/2}(1.53)^{d-2}\mathrm{R}_U,$$

où l'on a utilisé $r=d-1$ et les inégalités $r!\le r^{r+1/2}e^{-(r-1)}$ et $(ec)^{-1}\le 1.53$.

Remarquons par ailleurs que quelquefois il est plus simple de majorer directement δ_U. Par exemple, soient q une puissance d'un nombre premier, ζ_q une racine primitive q-ième de l'unité et $K = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$ le sous-corps réel maximal du q-ième corps cyclotomique. Notons U le groupe des unités cyclotomiques ; on sait alors (voir [Was, Lemma 8.1]) que U/U_{tors} est engendré par

$$\xi_a = \zeta_q^{(1-a)/2} \frac{1-\zeta_q^a}{1-\zeta_q}$$

pour $a \in]1, q/2[$ entier premier avec q. On a $h(\xi_a) \leq 2\log 2$ et donc

$$\delta_U \leq (2\log 2)r,$$

où $r = \mathrm{rang}(U) = \mathrm{rang}(\mathcal{O}_K^*) = \frac{1}{2}\phi(q) - 1$.

Nous pouvons maintenant énoncer la proposition qui nous permet de construire des nombres algébriques de petite hauteur à partir d'un nombre suffisant d'entiers algébriques de petite norme. Sa preuve repose sur une application standard du principe de tiroirs.

Proposition 2.3. *Soient $x \geq 1$ réel, $t \geq 2$ entier et U un sous-groupe de $\mathcal{O}_K^*$ de rang r. Supposons qu'il existe des entiers algébriques non nuls $\gamma_1, \ldots, \gamma_t \in \mathcal{O}_K$ tels que $|N_{\mathbb{Q}}^K \gamma_i| \leq x$ $(i = 1, \ldots, t)$. Soient ensuite m et N deux entiers strictement positifs et tels que*

$$mN^r < t.$$

Alors il existe une unité $u \in U$ et $m+1$ indices $i_0, i_1, \ldots, i_m \in \{1, \ldots, t\}$ deux-à-deux distincts et tels que

$$h(u\gamma_{i_j}\gamma_{i_0}^{-1}) \leq \frac{\log x}{[K:\mathbb{Q}]} + \frac{\delta_U}{N}$$

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

Démonstration. Soit $u_1, \ldots, u_r$ un système de générateurs de U/U_{tors} tel que

$$h(u_1) + \cdots + h(u_r) = \delta_U$$

et notons

$$P = \{\lambda_1 \mathcal{L}(u_1) + \cdots + \lambda_r \mathcal{L}(u_r) : 0 \leq \lambda_1, \ldots, \lambda_r < 1\} \subseteq H.$$

Quitte à remplacer les $\gamma_1, \ldots, \gamma_t$ par $v_1\gamma_1, \ldots, v_t\gamma_t$ avec $v_1, \ldots, v_r \in U$, on peut supposer que

$$(\pi \circ \mathcal{L})(\gamma_1), \ldots, (\pi \circ \mathcal{L})(\gamma_t) \in P.$$

Par le principe des tiroirs, il existe $m+1$ indices $i_0, i_1, \ldots, i_m \in \{1, \ldots, t\}$ deux-à-deux distincts et un vecteur $\underline{a} \in P$ tels que

$$(\pi \circ \mathcal{L})(\gamma_{i_0}), (\pi \circ \mathcal{L})(\gamma_{i_1}), \ldots, (\pi \circ \mathcal{L})(\gamma_{i_m}) \in \underline{a} + N^{-1}P.$$

On a donc, par la première partie du lemme 2.1,

$$\frac{1}{2}\,\|(\pi\circ\mathcal{L})(\gamma_{i_j}\gamma_{i_0}^{-1})\|_1 \le \frac{1}{2N}\,(\|\mathcal{L}(u_1)\|_1+\cdots+\|\mathcal{L}(u_r)\|_1)$$
$$= [K:\mathbb{Q}]N^{-1}(h(u_1)+\cdots+h(u_r)) = [K:\mathbb{Q}]N^{-1}\delta_U$$

pour $j=1,\dots,m$. En utilisant la deuxième partie du lemme 2.1, on en déduit que

$$[K:\mathbb{Q}]h(\gamma_{i_j}\gamma_{i_0}^{-1}) \le \max\{\log|N_{\mathbb{Q}}^K\gamma_{i_0}|,\log|N_{\mathbb{Q}}^K\gamma_{i_j}|\}+[K:\mathbb{Q}]N^{-1}\delta_U$$
$$\le \log x+[K:\mathbb{Q}]N^{-1}\delta_U$$

pour $j=1,\dots,m$. ∎

3. Preuve du théorème 1.2. Soit G un groupe fini ; pour l entier strictement positif notons $\mathcal{M}_G(l)$ le plus petit entier A tel que pour tout $g_1,\dots,g_l\in G$ il existe $\underline{a}\in\mathbb{Z}^l\setminus\{0\}$ tel que $g_1^{a_1}\cdots g_l^{a_l}=e$ et $\sum_j|a_j|\le A$. En particulier, $\mathcal{M}_G(1)$ est l'exposant du groupe G. Dans ce paragraphe nous démontrons la proposition suivante, dont le théorème 1.2 est un cas particulier :

PROPOSITION 3.1. *Soit K un corps de nombres et soit G son groupe de classes d'idéaux. Alors, sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K, on a*

$$\mathcal{M}_G(l)\ge C_4\,\frac{d_K^{-1}\log|\Delta_K|-\log d_K}{\log l+\log\log|\Delta_K|+d_K\log(\delta_K+2)},$$

où C_4 est une constante positive et effectivement calculable.

Démonstration. 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

$$x\ge c_1(\log|\Delta_K|)^2(\log\log|\Delta_K|)^4$$

il existe au moins $c_2^{-1}x(\log x)^{-1}$ idéaux premiers de norme $\le x$, de degré 1 sur $\mathbb{Q}$ et non ramifiés (voir [Amo-Dvo, Lemma 2.1]). Notons $t=[\delta_K+2]^r$, où r est le rang de $\mathcal{O}_K^*$, et soit $c_3\ge 1$ tel que $c_3/(\log c_3+2)\ge c_2$. Choisissons

$$x=c_3ltd_K\log(ltd_K)+c_1(\log|\Delta_K|)^2(\log\log|\Delta_K|)^4\,;$$

on a en particulier $x\ge c_3y\log y\ge e$, où l'on a noté $y=ltd_K\ge 3$, et donc

$$x(\log x)^{-1}=\frac{c_3y\log y}{\log(c_3y\log y)}\ge\frac{c_3y\log y}{\log c_3+2\log y}\ge c_2y=c_2ltd_K.$$

Remarquons qu'il y a au plus d_K premiers distincts dans $\mathcal{O}_K$ au-dessus d'un premier rationnel ; il existe donc lt premiers rationnels distincts $p_{ij}\le x$ et lt 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 multiplicatives non triviales

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

avec a_{ij} entiers. Soit $A = \max_j \sum_i |a_{ij}|$; donc, pour $j = 1, \dots, t$,

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

est un idéal principal de norme $\le x^A$. Choisissons $m = 1$, $N = [\delta_K + 1]$ et $U = \mathcal{O}_K^*$ dans la proposition 2.3 ; cette dernière nous assure l'existence d'une unité $u \in \mathcal{O}_K^*$ et de deux indices $j_0, j_1 \in \{1, \dots, t\}$ avec $j_0 \neq j_1$ tels que la hauteur de $\alpha = u\gamma_{j_1}\gamma_{j_0}^{-1}$ satisfasse

$$h(\alpha) \le \frac{A \log x}{d_K} + 1.$$

Remarquons que

$$\log x \le c_4(\log l + \log t + \log d_K + \log\log|\Delta_K|),$$

d'où, en utilisant la minoration $\log|\Delta_K| \ge c_6 d_K$ et en remplaçant t par sa valeur,

$$\log x \le c_5(\log l + d_K \log(\delta_K + 2) + \log\log|\Delta_K|).$$

On a donc

$$h(\alpha) \le c_6 A\left(\frac{\log l + \log\log|\Delta_K|}{d_K} + \log(\delta_K + 2)\right). \tag{3.1}$$

Montrons maintenant que α est un générateur de K. Pour cela, il est suffisant de montrer que $[\mathbb{Q}(\alpha) : \mathbb{Q}] \ge d_K$. Quitte à renuméroter les indices, on peut supposer $a_{1,j_1} \neq 0$. Soit L la clôture galoisienne de K dans $\overline{\mathbb{Q}}$; le lemme 3.1 de [Amo-Dvo] nous assure que $P_{1,j_1}\mathcal{O}_L$ a au moins d_K conjugués distincts $\sigma_1(P_{1,j_1}\mathcal{O}_L), \dots, \sigma_{d_K}(P_{1,j_1}\mathcal{O}_L)$. Supposons que pour certains $\iota, \kappa \in \{1, \dots, d_K\}$ on ait $\sigma_\iota(\alpha) = \sigma_\kappa(\alpha)$. Alors

$$\begin{aligned}&\sigma_\iota(P_{1,j_1}\mathcal{O}_L)^{a_{1,j_1}}\sigma_\iota(P_{1,j_0}\mathcal{O}_L)^{-a_{1,j_0}} \cdots \sigma_\iota(P_{l,j_1}\mathcal{O}_L)^{a_{l,j_1}}\sigma_\iota(P_{l,j_0}\mathcal{O}_L)^{-a_{l,j_0}}\\ &\quad = \sigma_\kappa(P_{1,j_1}\mathcal{O}_L)^{a_{1,j_1}}\sigma_\kappa(P_{1,j_0}\mathcal{O}_L)^{-a_{1,j_0}} \cdots \sigma_\kappa(P_{l,j_1}\mathcal{O}_L)^{a_{l,j_1}}\sigma_\kappa(P_{l,j_0}\mathcal{O}_L)^{-a_{l,j_0}}.\end{aligned}$$

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

$$\sigma_\iota(P_{i,j_1}\mathcal{O}_L) = \sigma_\kappa(P_{i,j_1}\mathcal{O}_L),$$

d'où $\iota = \kappa$. On en déduit que α a au moins d_K conjugués distincts et donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] \ge d_K$.

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

$$h(\alpha) \ge \frac{d_K^{-1}\log|\Delta_K| - \log d_K}{2(d_K - 1)}. \tag{3.2}$$

Le résultat désiré découle de (3.1) et (3.2). ∎

En remarquant que $\mathcal{M}_G(h_K) \leq 2$ (voir [Amo-Dvo, Lemma 5.1]), on déduit de cette proposition une minoration explicite (sous GRH) du nombre de classes ([3]) :

$$\log h_K \gg d_K^{-1} \log|\Delta_K| - d_K \log(\delta_K + 2).$$

Plus généralement, on peut déduire de la proposition 3.1 des renseignements sur les diviseurs élémentaires

$$\lambda_n \,|\, \lambda_{n-1} \,|\, \cdots \,|\, \lambda_1$$

du groupe des classes G :

COROLLAIRE 3.2. *Pour tout $j \in \{1, \ldots, n+1\}$ et sous l'hypothèse de Riemann généralisée pour la fonction zêta du corps K, on a :*

$$\lambda_j \log\left(\frac{\lambda_1 \cdots \lambda_{j-1}}{\lambda_j^{j-1}} (\delta_K + 2)^{d_K} \log|\Delta_K|\right) \gg d_K^{-1} \log|\Delta_K| - \log d_K,$$

où l'on a noté $\lambda_{n+1} = 1$.

Démonstration. Voir la preuve du corollaire 1.2 de [Amo-Dvo]. ∎

4. Minoration de l'exposant dans certaines familles infinies. Dans ce paragraphe nous démontrons le corollaire 1.3 ; sa preuve s'appuie sur la construction de Ankeny, Brauer et Chowla (voir [Ank-Bra-Cho]). La minoration du discriminant ci-dessous est inspirée à un travail récent de Bilu et Luca ([Bil-Luc]).

Soient $d \geq 2$ et $r_1, r_2 \geq 0$ entiers tels que $r_1 + 2r_2 = d$. Si $r_2 = 0$, on fixe $r_1 - 1$ entiers deux-à-deux distincts $a_1, \ldots, a_{r_1-1}$ et on considère la famille de polynômes

$$f_N(x) = 1 + \prod_{\lambda=1}^{r_1} (x - a_\lambda), \qquad a_{r_1} = N \in \mathbb{N}.$$

Si $r_2 \geq 1$, on fixe r_1 entiers deux-à-deux distincts $a_1, \ldots, a_{r_1}$ et $r_2 - 1$ entiers positifs deux-à-deux distincts $a_{r_1+1}, \ldots, a_{r_1+r_2-1}$ et on considère la famille de polynômes

$$f_N(x) = 1 + \prod_{\lambda=1}^{r_1} (x - a_\lambda) \prod_{\mu=r_1+1}^{r_1+r_2} (x^2 + a_\mu), \qquad a_{r_1+r_2} = N \in \mathbb{N}.$$

D'après [Ank-Bra-Cho] (lemme 1 et preuve du théorème 1 si $r_2 = 0$; preuve du théorème 1* si $r_2 \geq 1$) ce polynôme est irréductible, le corps des nombres K_N engendré par une de ses racines a signature (r_1, r_2) et de plus

$$\mathrm{R}_{K_N} \leq c_8(d)(\log N)^{d-1}.$$

([3]) Signalons que S. Bessassi [Bes] a récemment obtenu, avec des techniques analytiques classiques, des minorations meilleures.

Par ailleurs, un résultat de Sprindzhuk ([Spr, Lemma 8.6.4]) montre qu'il existe au moins $M/d!$ entiers N avec $M \leq N \leq 2M$ tels que les corps des nombres K_N sont deux-à-deux non isomorphes. Le nombre de corps de nombres deux-à-deux non isomorphes de degré d dont la valeur absolue du discriminant est $\leq X$ étant borné par $c_9(d)X^{(d+2)/4}$ (voir [Coh, Proposition 9.3.4]), on en déduit que pour une infinité d'entiers N on a

$$|\Delta_{K_N}| \geq c_{10}(d)N^{4/(d+2)}.$$

Le théorème 1.2 montre alors que, sous GRH,

$$E_{K_N} \geq c_{11}(d)\,\frac{\log \Delta_{K_N}}{\log\log \Delta_{K_N}}$$

pour une infinité d'entiers N.

Addendum. Signalons qu'une version faible de la Proposition 2.3 apparaît dans [Abl, lemme 2.2].

Références

[Abl] M. Ably et M. M'zari, *Interpolation polynômiale sur un ordre d'un corps de nombres*, prépublication, Lille.

[Ank-Bra-Cho] N. C. Ankeny, R. Brauer and S. Chowla, *A note on the class numbers of algebraic number fields*, Amer. J. Math. 78 (1956), 51–61.

[Amo-Dvo] F. Amoroso and R. Dvornicich, *Lower bounds for the height and size of the ideal class group in CM fields*, Monatsh. Math. 138 (2003), 85–94.

[Bes] S. Bessassi, *Bounds for the degrees of the CM-fields of class number one*, Acta Arith. 106 (2003), 213–245.

[Bil-Luc] Yu. F. Bilu and F. Luca, *Divisibility of class numbers*: *enumerative approach*, preprint, 2003, submitted.

[Bra] R. Brauer, *On the zeta-functions of algebraic number fields*, Amer. J. Math. 69 (1947), 243–250.

[Coh] H. Cohen, *Advanced Topics in Computational Number Theory*, Grad. Texts in Math. 193, Springer, 2000.

[Lag-Odl] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, dans : Algebraic Number Fields (Durham, 1975), Academic Press, 1977, 409–464.

[Loh-Mas] T. Loher and D. Masser, *Uniformly counting points of bounded height*, Acta Arith. 111 (2004), 277–297.

[Lou1] S. Louboutin, *Class-group problems for cubic number fields*, Japan. J. Math. 23 (1997), 365–378.

[Lou2] —, *The exponent three class group problem for some real cyclic cubic number fields*, Proc. Amer. Math. Soc. 130 (2002), 353–361.

[Lou3] —, *Class number and class group problems for some non-normal totally real cubic number fields*, Manuscripta Math. 106 (2001), 411–427.

[Mat] E. M. Matveev, *On the successive minima of the extended logarithmic height of algebraic numbers*, Sb. Math. 190 (1999), 407–425.

[Mur] M. R. Murty, *The ABC conjecture and exponents of class groups of quadratic fields*, dans : Number Theory (Tiruchirapalli, 1996), Contemp. Math. 210, Amer. Math. Soc., 1998, 85–95.

[Sil] J. H. Silverman, *Lower bounds for height functions*, Duke Math. J. 51 (1984), 395–403.

[Spr] V. G. Sprindžuk [V. G. Sprindzhuk], *Classical Diophantine Equations*, Lecture Notes in Math. 1559, Springer, 1993.

[Was] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

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

Reçu le 21.3.2003
et révisé le 26.4.2004 (4500)