If $d = 1$ or 2, then there is an integer m with $r < 2^m < s$, and so $2^m d$ is a power of 2 that can be written as the sum of at most 30960 distinct elements of A.

If $d = 3$, then each term of the arithmetic progression

$$\{rd, (r+1)d, \ldots, sd\} + \{a^*\} = \{3r+a^*, 3(r+1)+a^*, \ldots, 3s+a^*\}$$

is a sum of at most 30961 distinct elements of A. The quotient of the greatest and least elements of this set is

$$(3s+a^*)/(3r+a^*) > (3s+a^*)/(3(s/5)+a^*) = (15s+5a^*)/(3s+5a^*)$$
$$= 4+(3s-15a^*)/(3s+5a^*) > 4+(720n-45n)/(3s+5a^*) > 4.$$

It follows that there exists an integer m such that

$$3r+a^* \leqslant 2^m < 2^{m+1} \leqslant 3s+a^*.$$

Since $3 \nmid a^*$, either 2^m or 2^{m+1} is congruent to a^* modulo 3, hence belongs to the arithmetic progression above, and so can be written as the sum of at most 30961 distinct elements of A. This completes the proof.

References

[1] F. Dyson, *A theorem on the densities of sets of integers*, J. London Math. Soc. 20 (1945), 8–14.

[2] P. Erdös, *Some problems and results on combinatorial number theory*, in: *Proc. First China–U.S.A. Conference on Graph Theory and its Applications (Jinan, 1986)*, Annals New York Acad. Sci., to appear.

[3] P. Erdös and G. Freiman, *On two additive problems*, J. Number Theory, to appear.

[4] P. Erdös, M. B. Nathanson, and A. Sárközy, *Sumsets containing infinite arithmetic progressions*, J. Number Theory 28 (1988), 159–166.

[5] M. Filaseta, *Sets with elements summing to square-free numbers*, C. R. Math. Rep. Acad. Sci. Canada 9 (1987), 243–246.

[6] H. Halberstam and K. F. Roth, *Sequences*, Springer-Verlag, Berlin 1983.

[7] M. Kneser, *Abschätzungen der asymptotischen Dichte von Summenmengen*, Math. Z. 58 (1953), 459–484.

[8] H. B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. Math. 43 (1942), 523–527.

[9] M. B. Nathanson, *Sumsets containing k-free integers*, to appear.

[10] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. 27 (1975), 199–245.

OFFICE OF THE PROVOST AND
VICE PRESIDENT FOR ACADEMIC AFFAIRS
LEHMAN COLLEGE (CUNY)
Bronx, New York 10468 USA

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
Budapest, Hungary

Received on 11.2.1988
and in revised form on 6.7.1988 (1788)

ACTA ARITHMETICA
LIV (1989)

Notions relatives de régulateurs et de hauteurs

par

A.-M. BERGÉ et J. MARTINET (Talence)

1. Introduction. Soit L/K une extension de corps de nombres. L'étude faite dans [1] des minorations géométriques de régulateurs suggère la définition suivante du régulateur de L/K :

(1.1) DÉFINITION. Le *régulateur relatif* de L/K est: $R_{L/K} = Q_{L/K} R_L / R_K$, où $Q_{L/K}$ ("l'indice de Hasse" de L/K) est l'ordre du sous-groupe de torsion du quotient $E_L/\mu_L E_K$, les notations R_M, μ_M, E_M désignant respectivement le régulateur, le groupe des racines de l'unité et le groupe des unités d'un corps de nombres M.

Dans le cas d'une extension L/K primitive (c'est-à-dire sans sous-extension intermédiaire), on trouve dans [1] une démonstration d'une inégalité de la forme

$$R_{L/K} \geqslant \frac{1}{C_2}\left[\operatorname{Log}\frac{N_{K/\mathbf{Q}}(\mathfrak{d}_{L/K})}{C_3}\right]^{C_1} \qquad (\mathfrak{d}_{L/K} \text{ est le discriminant relatif}),$$

où C_1, C_2, C_3 sont des constantes dépendant seulement des signatures de K et L; comme constante C_1, on peut prendre la différence $r_L - r_K$ des rangs des groupes d'unités de L et de K (on suppose implicitement que la norme du discriminant relatif est $> C_3$). Cette inégalité est une généralisation du résultat classique de Remak [9] sur les corps primitifs, résultat que l'on retrouve en faisant $K = \mathbf{Q}$ et qui est basé sur une minoration de la norme euclidienne, dans le réseau des unités de L, en fonction du discriminant.

Dans le cas d'une extension $L/\mathbf{Q}$ imprimitive, la recherche d'une bonne constante C_1 nécessite en outre un argument de géométrie diophantienne sur la minoration de la hauteur d'un nombre algébrique en fonction de son seul degré: la hauteur logarithmique est en effet une norme dans le réseau des unités de L. Rappelons à ce propos une définition des hauteurs (c'est bien celle que donne Lang dans [7], ch. 3, §1, même si les degrés locaux n'y figurent pas explicitement).

(1.2) DÉFINITION. Soit d un entier > 0 et soit $x = (x_0, \ldots, x_d)$ un point de l'espace projectif $\boldsymbol{P}^d(\bar{\mathbf{Q}})$. La *hauteur* de x est

$$H(x) = \Big(\prod_w \operatorname{Max}_i |x_i|_w\Big)^{1/[L:\mathbf{Q}]},$$

où L est un sous-corps de degré fini de $\bar{\mathbf{Q}}$ contenant les x_i, et où w parcourt tous les $\mathbf{Q}$-isomorphismes de L dans les clôtures algébriques $\bar{\mathbf{Q}}_v$ des différents complétés $\mathbf{Q}_v$ de $\mathbf{Q}$ (pour chaque v, il y a $[L:\mathbf{Q}]$ choix pour w). La *hauteur logarithmique* de x est $h(x) = \operatorname{Log} H(x)$.

C'est ainsi que Silverman [10] a obtenu pour constante C_1 (vraisemblablement optimale) $C_1 = r_L - \max r_M$, où M parcourt les sous-corps stricts de L. (L'estimation antérieure de C_1, $C_1 \geqslant 1$ sauf pour les corps C.M., était due à Remak.)

Lors d'une visite à Bordeaux, en octobre 1987, E. Friedman nous a suggéré d'adapter au cas relatif la démonstration de Silverman, et pour cela d'introduire une notion de hauteur relative au corps K. En fait, la notion usuelle de hauteur s'est avérée suffisante pour une version relative de l'inégalité de Silverman (où $C_1 = r_L - \max r_M$, M parcourant les sous-corps stricts de L contenant K), qui est donc démontrée dès le §2. Toutefois, la notion de K-hauteur que nous introduisons, qui fait jouer aux racines des unités du corps K le rôle joué par les racines de l'unité pour la hauteur usuelle, nous est apparue intéressante en elle-même, ne serait-ce qu'à cause des généralisations de notions et problèmes classiques qu'elle suggère: nombres de Pisot et de Salem, problème de Lehmer, ... A ce propos, Joseph Silverman nous a suggéré, après la rédaction de cet article, une plus vaste généralisation de la notion de hauteur, attachée à un sous-groupe G arbitraire de $\bar{\mathbf{Q}}^*$ (au lieu d'un groupe d'unités E_K comme pour nos K-hauteurs). Il est à noter qu'une telle généralisation permettrait en particulier de considérer les groupes de S-unités. Cette notion de K-hauteur est introduite au §3 (noter qu'il ne s'agit pas de la "hauteur relative" d'un point de $\mathbf{P}^d(K)$, i.e. $H(x)^{[K:\mathbf{Q}]}$, comme par exemple dans [7], ch. 3, §1); on trouve dans le §3 quelques résultats techniques. Nous démontrons au §4 que les propriétés de finitude des hauteurs ont des analogues relatifs naturels. Dans le §5, nous donnons une formule explicite pour les K-hauteurs (th. 5.1), tout à fait analogue à celle de la définition 1.2 ci-dessus, et nous introduisons les notions de nombres de Pisot et de Salem pour K. Enfin, l'article s'achève par un §6 dans lequel nous étudions une version relative du problème de Lehmer. Divers compléments paraîtront dans le Séminaire de Théorie des Nombres de Bordeaux, 1987–1988. Comme nous l'avons déjà dit, c'est Edouardo Friedman qui est à l'origine de cet article. Nous l'en remercions.

2. Minoration des régulateurs relatifs. Dans ce § nous donnons une minoration du régulateur relatif $R_{L/K} = Q_{L/K} R_L / R_K$ d'une extension L/K de corps de nombres en fonction du discriminant relatif $\mathfrak{d}_{L/K}$, des degrés de L et K et des rangs des groupes des unités des sous-extensions de L/K.

(2.1) THÉORÈME. *Soient q et m des entiers positifs. Il existe des constantes $C = C(q, m)$ et $M = M(q, m)$ telles que, quels que soient les corps de nombres K et $L \supset K$ avec $[K:\mathbf{Q}] = q$ et $[L:K] = m$, on ait*

$$R_{L/K} \geqslant \frac{1}{C}\left[\operatorname{Log}\frac{N_{K/\mathbf{Q}}(\mathfrak{d}_{L/K})}{M}\right]^{r-\varrho}$$

chaque fois que $N_{K/\mathbf{Q}}(\mathfrak{d}_{L/K}) \geqslant M$, où r désigne le rang du groupe des unités E_L de L, et ϱ le maximum des rangs des groupes $E_{L'}$ pour $K \subset L' \subsetneq L$.

Plus précisément, si l'on note $n = mq$ le degré du corps L, r_K le rang du groupe des unités de K, r_2 et $r_2(K)$ le nombre de places imaginaires de L et K, et si l'on pose

$$S = m^{\log_2(4m)}, \quad d = r - r_K, \quad d_2 = r_2 - r_2(K),$$

on peut prendre m^{nS} et C telle que

$$C^2 = m^{1-r_K} 2^{-d_2} (3/4)^{d(d-1)/2} (S^2 n(m^2-1)/3)^{r-\varrho} \times \left(2\sqrt{n}\operatorname{Log}\left(1+\frac{1}{52n\operatorname{Log}6n}\right)\right)^{-2(\varrho-r_K)}$$

Lorsque $K = \mathbf{Q}$, ce théorème se réduit bien au résultat de Silverman cité au §1. Les constantes C et M qui y figurent sont très mauvaises en comparaison de celles que nous avons obtenues dans le cas primitif, cf. [1], et auxquels elles ne se réduisent pas lorsque $\varrho = r_K$ (on trouve par exemple $M = m^{nS}$ au lieu de $M = m^n$). L'exposant $r - \varrho$ nous paraît par contre optimal: voir à ce sujet les commentaires de Silverman (loc. cit.) et les exemples de [4] (Cusick) ainsi que ceux de [1].

Démonstration. Le cas où $r = \varrho$, c'est-à-dire où L est une extension (quadratique) de type C.M. d'un corps $K' \supset K$ se ramène à la remarque 2.7 ci-dessous appliquée au corps K'; nous supposons donc désormais $r > \varrho$. Soit $\mathscr{L}$ le plongement logarithmique de L^* dans $\mathbf{R}^n$: pour $\alpha \in L^*$, $\mathscr{L}(\alpha)$ est le vecteur de composantes $\operatorname{Log}|\sigma_i \alpha|$, σ_i parcourant l'ensemble des n plongements de L dans $\mathbf{C}$. Notons p la projection orthognale dans $\mathbf{R}\mathscr{L}(L^*)$ parallèlement au sous-espace $\mathbf{R}\mathscr{L}(E_K)$, et soit Λ le réseau $p\mathscr{L}(E_L)$; sa dimension est $d = r - r_K$ et son discriminant pour la structure euclidienne induite par $\mathbf{R}^n$ est lié au régulateur relatif par la formule

$$\Delta(\Lambda) = C_1 R_{L/K}, \quad \text{avec } C_1^{-2} = m^{r_K - 1} 2^{r_2(L) - r_2(K)} \tag{2.2}$$

(cf. [1], §3). Notons $\|\cdot\|$ la norme euclidienne dans $\mathbf{R}^n$. Par un résultat classique d'Hermite, il existe une base $e_1, \ldots, e_d$ de Λ et une constante $C_2 = C_2(d)$ telle que, pour tout $k \leqslant d$ on a

$$\|e_1\| \ldots \|e_k\| \leqslant C_2^k \Delta(\Lambda)^{k/d}.$$

(Hermite donne $C_2 = [\frac{3}{4}]^{(d-1)/4}$; on peut utiliser une constante de Remak cf. [12], formule (46).) Donc, on a en particulier

$$\Delta(\Lambda) \geqslant C_2^{-d} \cdot \|e_1\| \ldots \|e_d\|. \tag{2.3}$$

La base $(e_1, \ldots, e_d)$ de Λ étant choisie comme ci-dessus, on note $\varepsilon_1, \ldots, \varepsilon_d$ des unités de L telles que, pour tout i, $e_i = p\mathscr{L}(\varepsilon_i)$. Posons, pour tout i, $\varepsilon_i' = \varepsilon_i (N_{L/K}(\varepsilon_i))^{-1/m}$ (le choix de la racine $m^{\text{ième}}$ n'importe pas). On a

$$p\mathscr{L}(\varepsilon_i) = \frac{1}{m}\mathscr{L}(\varepsilon_i'^m).$$

On montre comme dans [10], p. 439 (voir aussi §3) l'inégalité

$$\|p\mathscr{L}(\varepsilon_i)\| \geqslant 2\sqrt{n}h(\varepsilon_i') \tag{2.4}$$

(h désigne la hauteur logarithmique).

Du fait que e_i est non nul, ε_i' n'est pas une racine de l'unité (théorème de Kronecker). Comme ε_i' est de degré $\leqslant nm$, il existe une constante $C_3 = C_3(n) > 0$ telle que

$$h(\varepsilon_i') \geqslant C_3 \quad \text{pour tout } i: \tag{2.5}$$

cela résulte par exemple du théorème de finitude ; la meilleure borne connue est celle de Dobrowolski ([5]).

A côté de cette minoration utilisant les hauteurs, nous en utilisons une seconde fondée sur des idées de Remak et mettant en jeu les discriminants relatifs : il existe des constantes $C_4 = C_4(n, q)$ et $M_1 = M_1(n, q)$ telles que pour tout $\varepsilon \in E_L$:

$$\|p\mathscr{L}(\varepsilon)\| \geqslant C_4 \operatorname{Log}\frac{N_{K/\mathbf{Q}}(\mathfrak{d}_{K(\varepsilon)/K})}{M_1}. \tag{2.6}$$

Il résulte de [1], prop. 4.10 et 5.2, que l'on peut prendre $M_1 = m^n$ et $C_4 = \big(n(m^2-1)/3\big)^{-1/2}$.

En reprenant les calculs de Silverman ([10], de la page 439 après (1) à la page 441 avant la proposition), on montre qu'il existe au moins $r-\varrho$ unités ε_i vérifiant

$$N_{K/\mathbf{Q}}(\mathfrak{d}_{K(\varepsilon_i)/K}) \geqslant (N_{K/\mathbf{Q}}\mathfrak{d}_{L/K})^{C_5}, \tag{2.7}$$

avec $C_5 = m^{-\log_2(4m)}$.

(L'adaptation au cas relatif de la démonstration de Silverman consiste simplement à se limiter à des corps k_i intermédiaires entre K et L et à remplacer les discriminants absolus par les normes des discriminants relatifs; par ailleurs, la première formule de la page 440 doit être lue $\alpha(j) = (2[K:k_j])^{j-n}$.)

Pour $d-(r-\varrho) = \varrho - r_K$ unités ε_i parmi lesquelles toutes celles qui ne vérifient pas (2.7), on minore $\|p\mathscr{L}(\varepsilon_i)\|$ par (2.4) et (2.5). En minorant enfin $R_{L/K}$ par (2.2) et (2.3), une obtient l'inégalité annoncée avec $M = M_1^{1/C_5}$, et $C^{-1} = (C_4C_5)^{r-\varrho}C_1^{-1}C_2^{-d}(2C_3\sqrt{n})^{\varrho-r_K}$. ∎

La valeur numérique donnée après (2.1) correspond (pour des raisons de simplicité) à l'estimation de C_2 due à Hermite, et à celle de C_3 due à Blanksby et Montgomery: $C_3 \geqslant \operatorname{Log}(1+(52n\operatorname{Log}6n)^{-1})$.

Le théorème ci-dessus ne s'applique que lorsque $\mathfrak{d}_{L/K}$ a une norme assez grande. Toutefois, il résulte des assertions (2.2) à (2.5) qu'il existe une constante $k > 0$ ne dépendant que du degré de L telle que l'on ait $R_{L/K} \geqslant k$ quel que soit $K \subset L$. Lorsque $K = \mathbf{Q}$, Friedman ([6]) a trouvé, par des méthodes analytiques, le corps réalisant le minimum du régulateur. L'existence d'une minoration de $R_{L/K}$ lorsque K est fixé en résulte. En revanche, nous ignorons si $R_{L/K}$ est minoré lorsque seul le degré de K est fixé. Les mêmes commentaires s'appliquent à $\frac{w_K}{w_L}R_{L/K}$ (w: nombre de racines de l'unité).

3. K-Hauteurs. Dans ce § et les suivants, on se donne une clôture algébrique $\bar{\mathbf{Q}}$ de $\mathbf{Q}$; les corps de nombres sont toujours supposés contenus dans $\bar{\mathbf{Q}}$. Soit K un corps de nombres, soit x un point de l'espace projectif $\boldsymbol{P}^d(\bar{\mathbf{Q}})$ et soit $(x_0, \ldots, x_d)$ un système de coordonnées de x. Pour $\varepsilon_0, \ldots, \varepsilon_d \in E_K$ et pour i entier > 0, la hauteur d'un point de coordonnées $(\varepsilon_0^{1/i}x_0, \ldots, \varepsilon_d^{1/i}x_d)$ ne dépend ni du choix dans $\bar{\mathbf{Q}}^*$ des racines i-èmes des ε_j, ni de celui des coordonnées de x. Cela justifie la définition suivante (qui redonne les notions usuelles de hauteurs lorsque $K = \mathbf{Q}$) :

(3.1) DÉFINITION. La *K-hauteur du point x* est

$$H(K; x) = \inf_{i,\varepsilon_j} H\big((\varepsilon_0^{1/i}x_0, \ldots, \varepsilon_d^{1/i}x_d)\big)$$

où i est un entier > 0 et les $\varepsilon_j \in E_K$. La *K-hauteur logarithmique de x* est $h(K; x) = \operatorname{Log} H(K; x)$.

Les hauteurs $H(K; \alpha)$ et $h(K; \alpha)$ d'un élément $\alpha \in \bar{\mathbf{Q}}^*$ sont celles de $(1, \alpha) \in \boldsymbol{P}^1(\bar{\mathbf{Q}})$; on a donc $H(K; \alpha) = \inf_{i,\varepsilon} H(\varepsilon^{1/i}\alpha)$.

Si $x \in \boldsymbol{P}^d(L)$, où $L \subset \bar{\mathbf{Q}}$ est un corps de nombres contenant K, on peut définir une *K-hauteur de x relative à L* :

$$H_L(K; x) = H^{[L:\mathbf{Q}]}(K; x).$$

(Le cas des corps de fonctions n'est pas intéressant: le rôle des unités y est joué par les constantes, si bien que les hauteurs absolues et relatives sont les mêmes.)

La démonstration de la proposition suivante est laissée au lecteur.

(3.2) PROPOSITION. *Soit $x \in \boldsymbol{P}^d(\bar{\mathbf{Q}})$.*

(i) *Pour toute extension K/K_0, on a*

$$1 \leqslant H(K; x) \leqslant H(K_0; x) \leqslant H(\mathbf{Q}; x) = H(x).$$

(ii) *Quels que soient $y_0, \ldots, y_d \in \bar{\mathbf{Q}}$ dont une puissance est dans E_K, on a*

$$H\big(K; (y_0x_0, \ldots, y_dx_d)\big) = H(K; x).$$

(iii) *Soit $y = (x_{i_0}, \ldots, x_{i_e}) \in \boldsymbol{P}^e(\bar{\mathbf{Q}})$ une projection de x (on suppose les x_{i_j} non tous nuls). Alors on a*

$$H(K; y) \leqslant H(K; x).$$

Nous reviendrons plus loin sur les cas d'égalité dans (i) ; on peut toutefois noter que si K/K_0 est une extension (quadratique) de type C.M., on a $H(K; x) = H(K_0; x)$ pour tout x. L'assertion (iii) permet souvent de se

ramener aux nombres algébriques non nuls, auxquels la suite du § est consacrée.

Nous donnons tout d'abord une version relative facile de résultats bien connus lorsque $K = \boldsymbol{Q}$:

(3.3) PROPOSITION. *Soient* α, $\beta \in \bar{\boldsymbol{Q}}^*$ *et* $j \in \boldsymbol{Z}$. *On a*:

(i) $$H(K;\alpha\beta) \leqslant H(K;\alpha)H(K;\beta),$$

(ii) $$H(K;\alpha^j) = H(K;\alpha)^{|j|}.$$

Pour aller plus loin, précisons les notations: étant donnés un corps de nombres $L \subset \bar{\boldsymbol{Q}}$ de degré n, et $\alpha \in L^*$, écrivons $(\alpha) = \mathfrak{A}\mathfrak{B}^{-1}$ la décomposition de l'idéal fractionnaire (α) comme quotient de deux idéaux entiers premiers entre eux de L. Alors, on a (cf. [7], p. 53), en notant N la norme $N_{L/\boldsymbol{Q}}$:

$$H^n(\alpha) = N(\mathfrak{B}) \prod_{|\sigma\alpha| \geqslant 1} |\sigma\alpha|$$

où σ décrit l'ensemble S des plongements de L dans $\boldsymbol{C}$, d'où l'on déduit une formule plus symétrique:

$$H^n(\alpha) = N(\mathfrak{B}) \prod_{|\sigma\alpha| \geqslant 1} |\sigma\alpha| = N(\mathfrak{A}) \prod_{|\sigma\alpha| < 1} |\sigma\alpha|^{-1}$$
$$= \left[N(\mathfrak{A}\mathfrak{B}) \prod_{\sigma \in S} (\max|\sigma\alpha|, |\sigma\alpha|^{-1})\right]^{1/2}.$$

Notons que, lorsque α est entier, on a $H(\alpha)^n \geqslant |N\alpha|$, d'où l'on déduit aisément $H(K;\alpha)^n \geqslant |N\alpha|$.

Pour interpréter géométriquement le quotient $H(K;\alpha)^{2n} N(\mathfrak{A}\mathfrak{B})^{-1}$, nous utilisons le plongement logarithmique déjà introduit au §2: $\mathscr{L}_L$ (ou $\mathscr{L}$) désigne l'homomorphisme $\alpha \to (\mathrm{Log}|\sigma\alpha|)$ de L^* dans $\boldsymbol{R}^n$, où $\sigma \in S$. Par ailleurs, pour $x = (x_1, \ldots, x_n) \in \boldsymbol{R}^n$, on pose

$$\|x\| = \Big(\sum_i x_i^2\Big)^{1/2} \quad \text{et} \quad \|x\|' = \sum_i |x_i|.$$

On a

$$\|x\| \leqslant \|x\|' \leqslant \sqrt{n}\,\|x\|.$$

(3.4) PROPOSITION. *Soit* $\alpha \in \bar{\boldsymbol{Q}}^*$ *et soit* $L \supset K(\alpha)$. *Alors, avec les notations ci-dessus et* p *désignant la projection orthogonale de* $\boldsymbol{R}\mathscr{L}(L^*)$ *parallèlement à* $\boldsymbol{R}\mathscr{L}(E_K)$, *on a*:

(i) $$2nh(\alpha) = \mathrm{Log}\,N(\mathfrak{A}\mathfrak{B}) + \|\mathscr{L}(\alpha)\|',$$

(ii) $$2nh(K;\alpha) = \mathrm{Log}\,N(\mathfrak{A}\mathfrak{B}) + \inf_{x \in \boldsymbol{R}\mathscr{L}(E_K)} \|\mathscr{L}(\alpha) + x\|',$$

(iii) $$\mathrm{Log}\,N(\mathfrak{A}\mathfrak{B}) + \|p\mathscr{L}(\alpha)\| \leqslant 2nh(K;\alpha) \leqslant \mathrm{Log}\,N(\mathfrak{A}\mathfrak{B}) + \|p\mathscr{L}(\alpha)\|'.$$

Démonstration. Pour (i), on utilise les remarques précédant (3.4), où

$$\mathrm{Log} \prod_{\sigma \in S} \max(|\sigma\alpha|, |\sigma\alpha|^{-1}) = \|\mathscr{L}(\alpha)\|'.$$

(ii) Soient $\varepsilon \in E_K$ et $i > 0$. On a $(\varepsilon\alpha^i) = \mathfrak{A}^i\mathfrak{B}^{-i}$ et $\mathscr{L}(\varepsilon\alpha^i) = \mathscr{L}(\varepsilon) + i\mathscr{L}(\alpha)$, d'où, par (i) (appliqué à $\varepsilon\alpha^i$) et (3.3) (ii),

$$2n\,h(\varepsilon^{1/i}\alpha) = \mathrm{Log}\,N(\mathfrak{A}\mathfrak{B}) + \left\|\mathscr{L}(\alpha) + \frac{1}{i}\mathscr{L}(\varepsilon)\right\|'.$$

On conclut en remarquant que les bornes inférieures sur $\boldsymbol{Q}\mathscr{L}(E_K)$ et $\boldsymbol{R}\mathscr{L}(E_K)$ sont identiques.

(iii) La seconde inégalité est évidente, car $p\mathscr{L}(\alpha)$ est de la forme $\mathscr{L}(\alpha) + x$, $x \in \boldsymbol{R}\mathscr{L}(E_K)$. Pour la première, on utilise l'égalité $\|p\mathscr{L}(\alpha)\| = \inf_x \|\mathscr{L}(\alpha) + x\|$ et l'inégalité $\|y\|' \geqslant \|y\|$. ∎

Soit maintenant K_0 un sous-corps de K. Nous allons associer à tout $\alpha \in \bar{\boldsymbol{Q}}^*$ un élément $\alpha'_{K/K_0} = \alpha' \in \bar{\boldsymbol{Q}}^*$ tel que $h(K;\alpha)h(K_0;\alpha')^{-1}$ soit borné lorsque α est une unité.

(3.5) NOTATIONS. (i) On note E_{K/K_0} le sous-groupe de E_K formé des unités dont la norme sur K_0 est une racine de l'unité, et p, p_0 et p' les projections orthogonales respectives de $\boldsymbol{R}\mathscr{L}(L^*)$ parallèlement à $\boldsymbol{R}\mathscr{L}(E_K)$, $\boldsymbol{R}\mathscr{L}(E_{K_0})$ et $\boldsymbol{R}\mathscr{L}(E_{K/K_0})$ (on a $p = p_0 \circ p'$).

(ii) Soit $\alpha \in \bar{\boldsymbol{Q}}^*$ et soit L un corps de nombres contenant $K(\alpha)$. On pose $q = [K:K_0]$, $n_0 = [L:K_0]$, $n = [L:\boldsymbol{Q}]$ et

$$\alpha'_{K/K_0} = \alpha[N_{L/K}(\alpha)^q \cdot N_{L/K_0}(\alpha)^{-1}]^{-1/n_0}.$$

On écrit simplement α'_K lorsque $K_0 = \boldsymbol{Q}$.

(Noter que α' n'est défini qu'à une racine de l'unité près, et que, modulo une telle racine, il ne dépend pas du choix de L contenant $K(\alpha)$. On a $[K(\alpha'):K] \leqslant [K(\alpha):K]^2$.)

(3.6) PROPOSITION. *Avec les notations ci-dessus, on a*:

(i) $$\frac{1}{n_0}\mathscr{L}(\alpha'^{n_0}_{K/K_0}) = p'\mathscr{L}(\alpha).$$

(ii) $$\frac{1}{\sqrt{n}}\left(h(K_0;\alpha'_{K/K_0}) + \frac{\sqrt{n}-3}{2n}\mathrm{Log}\,N(\mathfrak{A}\mathfrak{B})\right)$$
$$\leqslant h(K;\alpha) \leqslant h(K_0;\alpha'_{K/K_0}) + \frac{1}{2n}\mathrm{Log}\,N(\mathfrak{A}\mathfrak{B})$$

où $\mathfrak{A}$ *et* $\mathfrak{B}$ *sont des idéaux entiers et premiers entre eux de* L *tels que* $(\alpha) = \mathfrak{A}\mathfrak{B}^{-1}$.

(iii) *Si* α *est une unité,*

$$(1 - \mathrm{Log}\,2)\,h(K_0;\alpha'_{K/K_0}) \leqslant h(K;\alpha) \leqslant h(K_0;\alpha'_{K/K_0}).$$

Démonstration. (i) On remarque que $R\mathcal{L}(E_{K/K_0})$ est le sous-espace de $R\mathcal{L}(L^*)$ formé des vecteurs (y_σ) tels que $y_\sigma = y_{\sigma'}$ si σ et σ' ont même restriction à K et $\sum_{\sigma|\tau_0} y_\sigma = 0$ quel que soit le plongement τ_0 de K_0 dans C. Donc l'image par $\mathcal{L}$ de $\beta = N_{L/K}(\alpha)^q \cdot N_{L/K_0}(\alpha)^{-1}$ appartient à $R\mathcal{L}(E_{K/K_0})$. Comme $N_{L/K}(\alpha^n\beta^{-1})$ appartient à K_0, $\mathcal{L}(\alpha)-(1/n)\mathcal{L}(\beta)$ est dans son orthogonal. Pour (ii) et (iii), nous utiliserons le résultat géométrique suivant :

(3.7) Lemme. *Soit $y \in R\mathcal{L}(L^*)$. Alors on a:*

(1) $$\frac{1}{\sqrt{n}} \operatorname*{Inf}_{x_0} \|p'y+x_0\|' \leqslant \operatorname*{Inf}_{x} \|y+x\|' \leqslant \operatorname*{Inf}_{x_0} \|p'y+x_0\|' ;$$

(2) *Si de plus $y \in R\mathcal{L}(E_L)$,*

$$(1-\operatorname{Log}2) \operatorname*{Inf}_{x_0} \|p'y+x_0\|' \leqslant \operatorname*{Inf}_{x} \|y+x\|'.$$

(Dans cet énoncé, x parcourt $R\mathcal{L}(E_K)$ et x_0 $R\mathcal{L}(E_{K_0})$.)

Démonstration du lemme. On a $\operatorname*{Inf}_x \|y+x\|' = \operatorname*{Inf}_x \|py+x\|'$, et aussi, comme $p = p_0 \circ p'$,

$$\operatorname*{Inf}_{x_0} \|p'y+x_0\|' = \operatorname*{Inf}_{x_0} \|py+x_0\|'.$$

On peut donc supposer désormais $y = py$. On a alors

$$\operatorname*{Inf}_x \|y+x\| = \|y\| \quad \text{et} \quad \operatorname*{Inf}_{x_0} \|y+x_0\| = \|p_0 y\| = \|y\|,$$

d'où (1) grâce aux inégalités d'équivalence des normes $\|\cdot\|$ et $\|\cdot\|'$. Nous allons montrer un résultat plus précis que (2) pour tout $y \in R\mathcal{L}(E_L)$ tel que $y = py$, et pour tout $x \in R\mathcal{L}(E_K)$, on a

$$\|y-x\|' \geqslant (1-\operatorname{Log}2)\|y\|'.$$

On a

$$\|y-x\|' = \sum_\tau \sum_{\sigma|\tau} |x_\sigma - y_\sigma|,$$

où τ parcourt l'ensemble des plongements de K dans C, et σ l'ensemble des plongements de L dans C. Comme l'on a $x_\sigma = x_{\sigma'}$ si σ et σ' ont même restriction à K, et $\sum_{\sigma|\tau} y_\sigma = 0$ pour tout τ, il nous suffit de vérifier la propriété suivante :

Soient $y_1 \leqslant \ldots \leqslant y_m$ des réels tels que $\sum_{i=1}^m y_i = 0$, et soit, pour $\lambda \in R$,

$$f(\lambda) = \sum_{i=1}^m |\lambda - y_i|.$$

Alors on a

$$f(\lambda) \geqslant (1-\operatorname{Log}2) f(0).$$

La fonction f est linéaire par morceaux, et est minimum pour $\lambda = y_j$, avec $j = m/2$ (resp. $(m+1)/2$) si m est pair (resp. impair). On a donc

$$\min f(\lambda) = f(y_j) = \sum_1^j (y_j - y_i) + \sum_{j+1}^m (y_i - y_j) = 2\sum_{j+1}^m y_i + (2j-m)y_j$$

(puisque $\sum y_i = 0$). Quitte à changer tous les y_i en leurs opposés et λ en $-\lambda$, on peut supposer $y_j \geqslant 0$, d'où $\min f(\lambda) \geqslant 2\sum_{j+1}^m y_i$. Soit $2 \leqslant k \leqslant j$ tel que $y_{k-1} \leqslant 0$ et $y_k \geqslant 0$. On peut alors écrire

$$f(0) = \sum_k^m y_i - \sum_1^{k-1} y_i = 2\sum_k^m y_i = 2\sum_k^j y_i + 2\sum_{j+1}^m y_i,$$

d'où $f(0) \leqslant \min f(\lambda) + 2\sum_k^j y_i$. Par ailleurs, pour tout $i \geqslant k$, on a les inégalités suivantes:

$$(m+1-i)y_i \leqslant \sum_{l=i}^m y_l \leqslant \sum_{l=k}^m y_l = \tfrac{1}{2} f(0),$$

d'où finalement

$$f(0) \leqslant \min f(\lambda) + f(0) \sum_{k \leqslant i \leqslant j} \frac{1}{m+1-i} \leqslant \min f(\lambda) + f(0) \operatorname{Log} \frac{m+1-k}{m-j}$$

où

$$\frac{m+1-k}{m-j} \leqslant \frac{m-1}{m/2-1/2} = 2.$$

Ceci achève la démonstration de (3.7).

Revenons à la démonstration de (3.6). Ecrivons $(\alpha'^{n_0}) = \mathfrak{A}'\mathfrak{B}'^{-1}$, où $\mathfrak{A}'$ et $\mathfrak{B}'$ sont des idéaux entiers et premiers entre eux de L. Par (3.4) (ii), on a

$$2nh(K;\alpha) = \operatorname{Log} N(\mathfrak{A}\mathfrak{B}) + \operatorname*{Inf}_x \|\mathcal{L}(\alpha)+x\|'$$

et

$$2nh(K_0;\alpha') = \frac{1}{n_0} \operatorname{Log} N(\mathfrak{A}'\mathfrak{B}') + \operatorname*{Inf}_{x_0} \left\| \frac{1}{n_0} \mathcal{L}(\alpha'^{n_0}) + x_0 \right\|'.$$

Lorsque α est une unité, il en est de même de α'^{n_0}, de sorte que (3.6) (iii) est équivalente à (3.7) (2) appliquée à $y = \mathcal{L}(\alpha)$ (d'où $p'y = \frac{1}{n_0}\mathcal{L}(\alpha'^{n_0})$. Dans le cas général, on a

$$0 \leqslant \frac{1}{n_0} \operatorname{Log} N(\mathfrak{A}'\mathfrak{B}') \leqslant 3 \operatorname{Log} N(\mathfrak{A}\mathfrak{B}):$$

en effet, (3.5) (ii) donne

$$\mathfrak{A}'\mathfrak{B}'^{-1} = \mathfrak{A}^{n_0} N_{L/K_0}(\mathfrak{A}) N_{L/K}(\mathfrak{B}^q)\mathfrak{B}^{-n_0} N_{L/K_0}(\mathfrak{B})^{-1} N_{L/K_0}(\mathfrak{A})^{-q},$$

donc (puisque $\mathfrak{A}'$ et $\mathfrak{B}'$ sont premiers entre eux), $\mathfrak{A}'\mathfrak{B}'$ divise l'idéal $(\mathfrak{A}\mathfrak{B})^{n_0} N_{L/K_0}(\mathfrak{A}\mathfrak{B}) N_{L/K}(\mathfrak{A}\mathfrak{B})^q$; il s'ensuit que $N_{L/K_0}(\mathfrak{A}'\mathfrak{B}')$ divise $N_{L/K_0}(\mathfrak{A}\mathfrak{B})^{3n_0}$, et *a fortiori* $\operatorname{Log} N(\mathfrak{A}'\mathfrak{B}') \leqslant 3n_0 \operatorname{Log} N(\mathfrak{A}\mathfrak{B})$. Cette inégalité, jointe à (3.7) (1) appliquée à $y = \mathscr{L}(\alpha)$, donne, par les expressions de $h(K;\alpha)$ et $h(K_0;\alpha')$ rappelées ci-dessus, l'assertion (3.6) (ii). ∎

4. Un théorème de finitude. On conserve les notations des § antérieurs; $K \subset \bar{\mathbf{Q}}$ est un corps de nombres et d un entier > 0. Appelons degré d'un point $x \in \mathbf{P}^d(\bar{\mathbf{Q}})$ le minimum des degrés des corps $\mathbf{Q}(x_0, \ldots, x_d)$ engendrés par les systèmes de coordonnées de x. Par ailleurs, faisons opérer E_K^{d+1} sur $\mathbf{P}^d(\bar{\mathbf{Q}})$ par $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_d)\cdot(x_0, x_1, \ldots, x_d) = (\varepsilon_0 x_0, \varepsilon_1 x_1, \ldots, \varepsilon_d x_d)$.

(4.1) THÉORÈME. (i) *Soit $x \in \mathbf{P}^d(\bar{\mathbf{Q}})$. Alors, on a $H(K;x) = 1$ si et seulement si x possède un système de coordonnées $x_0, \ldots, x_d$ tel que, pour tout i, x_i ait une puissance dans E_K ou soit nul.*

(ii) *L'ensemble des points de $\mathbf{P}^d(\bar{\mathbf{Q}})$ ayant un degré et une K-hauteur bornés est fini modulo l'action de E_K^{d+1}.*

La démonstration utilise les théorèmes de Kronecker et de Northcott, auxquels l'énoncé précédent se réduit lorsque $K = \mathbf{Q}$.

Démonstration. Quitte à permuter les coordonnées de x, on peut supposer la première coordonnée non nulle, et même égale à 1. Si x_i est alors une coordonnée non nulle de x, on a $1 \leqslant H(K;x_i) \leqslant H(K;x)$ et $dg(x_i) \leqslant dg(x)$. On est donc ramené au cas d'un élément $\alpha \in \bar{\mathbf{Q}}^*$.

(i) Soit L contenant $K(\alpha)$, et supposons $H(K;\alpha) = 1$. Par (3.4) (iii) on a $\operatorname{Log} N(\mathfrak{A}\mathfrak{B}) = \|p\mathscr{L}(\alpha)\| = 0$. De $N(\mathfrak{A}\mathfrak{B}) = 1$, on déduit que $\alpha \in E_L$. De $p\mathscr{L}(\alpha) = 0$, on déduit que $\mathscr{L}(\alpha) \in \mathbf{R}\mathscr{L}(E_K)$. Comme $\mathscr{L}(\alpha)$ est dans le réseau $\mathscr{L}(E_L)$, on a $\mathscr{L}(\alpha) \in \mathbf{Q}\mathscr{L}(E_K)$. Si $\mathscr{L}(\alpha) = \mathscr{L}\left(\frac{a}{b}\varepsilon\right)$, $a, b \in \mathbf{Z}$ et $\varepsilon \in E_L$, on a $\alpha^b \varepsilon^{-a} \in \operatorname{Ker}\mathscr{L}$, égal à μ_L par le théorème de Kronecker.

(ii) Soient n_0 et $h_0 > 0$, et soit $\mathscr{E}$ l'ensemble des $\alpha \in \bar{\mathbf{Q}}^*$ tels que $dg(\alpha) \leqslant n_0$ et $h(K;\alpha) \leqslant h_0$. Nous montrons d'abord que l'ensemble des $\alpha'_K \in \bar{\mathbf{Q}}^*$ que l'on peut associer aux $\alpha \in \mathscr{E}$ par (3.5) (ii) est fini. Pour $\alpha \in \mathscr{E}$, soit $L = K(\alpha)$; son degré n est $\leqslant n_0 q$ ($q = [K:\mathbf{Q}]$). Le degré de α' est $\leqslant n^2$, donc borné. En appliquant (3.4) (iii), dont on conserve les notations, on en déduit que pour $\alpha \in \mathscr{E}$, $\operatorname{Log} N(\mathfrak{A}\mathfrak{B})$ est majoré. Par (3.6) (ii), α' est de hauteur bornée ; le théorème de Northcott ([7]), p. 59) montre alors la finitude de l'ensemble des α' pour $\alpha \in \mathscr{E}$.

Restreignons-nous maintenant aux $\alpha \in \mathscr{E}$ correspondant à un α' donné, et ayant en outre un degré n fixé. Dans l'écriture $(\alpha) = \mathfrak{A}\mathfrak{B}^{-1}$, les idéaux $N(\mathfrak{A})$ et $N(\mathfrak{B})$ ne prennent qu'un nombre fini de valeurs (puisque $\operatorname{Log} N(\mathfrak{A}\mathfrak{B})$ est majoré) ; il en est de même des idéaux $N_{L/K}(\mathfrak{A})$ et $N_{L/K}(\mathfrak{B})$ de K. On en déduit

que les idéaux fractionnaires principaux de K engendrés par $N_{L/K}(\alpha)^q N(\alpha)^{-1}$ sont en nombre fini. Il s'en suit que α lui-même ne prend qu'un nombre fini de valeurs modulo $E_K^{1/n}$ (cf. (3.5)), donc aussi modulo E_K, puisque E_K/E_K^n est un groupe fini. ∎

5. Quelques calculs de hauteurs relatives. Dans ce paragraphe, $K \subset \bar{\mathbf{Q}}$ désigne un corps de nombres donné. Nous donnons d'abord une formule explicite générale pour la K-hauteur d'un nombre algébrique :

(5.1) THÉORÈME. *Soit $\theta \in \bar{\mathbf{Q}}^*$ un nombre algébrique, et soit $L \subset \bar{\mathbf{Q}}$ un corps de nombres contenant $K(\theta)$. On note $\mathfrak{A}$ et $\mathfrak{B}$ les idéaux entiers et premiers entre eux de L tels que $(\theta) = \mathfrak{A}\mathfrak{B}^{-1}$. Pour tout plongement τ de K dans $\mathbf{C}$, on ordonne les m ($m = [L:K]$) plongements $\sigma_{i,\tau}$ de L dans $\mathbf{C}$ au-dessus de τ de façon que l'on ait*

$$|\sigma_{1,\tau}\theta| \leqslant |\sigma_{2,\tau}\theta| \leqslant \ldots \leqslant |\sigma_{m,\tau}\theta|$$

(avec, si τ est imaginaire, $\overline{\sigma_{i,\tau}} = \sigma_{i,\bar{\tau}}$). La hauteur relative $H_L(K;\theta) = H(K;\theta)^{[L:\mathbf{Q}]}$ est donnée par la formule

$$H_L(K;\theta) = N_{L/K}(\mathfrak{B}) \prod_{1 \leqslant i \leqslant m} \max\left(1, \prod_\tau |\sigma_{i,\tau}\theta|\right).$$

Remarquons que cette expression, qui redonne le résultat classique lorsque $K = \mathbf{Q}$, peut être, comme dans ce cas (cf. §3), formulée de façon plus symétrique :

$$H_L(K;\theta) = N(\mathfrak{B}) \prod_i \max\left(1, \prod_\tau |\sigma_{i,\tau}\theta|\right) = N(\mathfrak{A}) \prod_i \left[\min\left(1, \prod_\tau |\sigma_{i,\tau}\theta|\right)\right]^{-1}$$

$$= N(\mathfrak{A}\mathfrak{B})^{1/2} \prod_i \max\left(\left|\prod_\tau \sigma_{i,\tau}\theta\right|, \left|\prod_\tau \sigma_{i,\tau}\theta\right|^{-1}\right)^{1/2}.$$

(On écrit N pour $N_{L/\mathbf{Q}}$.)

Démonstration de (5.1). Posons $a_{i,\tau} = \operatorname{Log}|\sigma_{i,\tau}\theta|$, et soit $\mathscr{L} : \theta \mapsto (a_{i,\tau})_{i,\tau}$ le plongement de L^* dans $\mathbf{R}^n$. D'après (3.4) (ii), il s'agit de montrer que l'on a

$$\operatorname*{Inf}_x \|\mathscr{L}(\theta) - x\|' = \sum_{1 \leqslant i \leqslant m} \left|\sum_\tau a_{i,\tau}\right|,$$

où $x = (x_{i,\tau})$ parcourt le sous-espace $\mathbf{R}\mathscr{L}(E_K)$ défini par les équations $x_{i,\tau} = x_{1,\tau}$ noté x_τ, $i = 2, \ldots, m$, $x_\tau = x_{\bar{\tau}}$, et $\sum_\tau x_\tau = 0$. On pose $f(x) = \|\mathscr{L}(\theta) - x\|'$:

$$f(x) = \sum_\tau \sum_i |a_{i,\tau} - x_\tau|.$$

On définit l'entier $p \in \{0, 1, \ldots, m\}$ par $\sum_\tau a_{p,\tau} \leqslant 0 \leqslant \sum_\tau a_{p+1,\tau}$; soit X l'ensemble des $x \in \mathbf{R}\mathscr{L}(E_K)$ tels que, pour tout τ, l'on ait $a_{p,\tau} \leqslant x_\tau \leqslant a_{p+1,\tau}$. (Par exemple,

X contient le vecteur x défini par $x_\tau = a_{p,\tau} - s_p(s_{p+1}-s_p)^{-1}(a_{p+1,\tau}-a_{p,\tau})$, où l'on a posé $s_i = \sum_\tau a_{i,\tau}$.) Pour tout $x \in X$, on a :

$$f(x) = \sum_\tau \Big[\sum_{i\leqslant p}(x_\tau - a_{i,p}) + \sum_{i\geqslant p+1}(a_{i,p}-x_\tau)\Big]$$
$$= (2p-m)\sum_\tau x_\tau + \sum_i \Big|\sum_\tau a_{i,\tau}\Big| = \sum_i \Big|\sum_\tau a_{i,\tau}\Big|.$$

Comme f est convexe (c'est-à-dire que l'ensemble des $x \in \boldsymbol{R}\mathscr{L}(E_K)$ tels que $f(x) > 0$ est une partie convexe de $\boldsymbol{R}\mathscr{L}(E_K)$), il suffit de montrer que la valeur de f sur X est un minimum local ; cela est clair si X est d'intérieur non vide ; la démonstration suivante est générale: soit x l'élément de X exhibé ci-dessus, et soit $x' \in \boldsymbol{R}\mathscr{L}(E_K)$. On a

$$f(x') = f(x) + \sum_\tau A_\tau(x'_\tau - x_\tau),$$

où, pour $|x'_\tau - x_\tau|$ assez petit, A_τ ne dépend que du signe de $x'_\tau - x_\tau$. On montre, en examinant successivement les cas $x_\tau = a_{p,\tau} = a_{p+1,\tau}$, $x_\tau = a_{p,\tau} < a_{p+1,\tau}$, et $a_{p,\tau} < x_\tau < a_{p+1,\tau}$, que l'on a toujours $A_\tau \leqslant 2p-m$ si $x'_\tau - x_\tau < 0$, et $A_\tau \geqslant 2p-m$ si $x'_\tau - x_\tau > 0$, d'où, pour x' assez voisin de x,

$$\sum_\tau A_\tau(x'_\tau - x_\tau) \geqslant (2p-m)\sum_\tau (x'_\tau - x_\tau) = 0,$$

et finalement $f(x') \geqslant f(x)$. ∎

(5.2) Exemple. Si $\theta \in K^*$, on a, avec les notations de (5.1),

$$H(K;\theta)^{[K:\mathbb{Q}]} = \max(N_{K/\mathbb{Q}}(\mathfrak{A}), N_{K/\mathbb{Q}}(\mathfrak{B})).$$

(5.3) Exemple. Si θ est une unité de degré 2 sur K, on a

$$H(K;\theta)^{[K(\theta):\mathbb{Q}]} = \prod_\tau |\sigma_{2,\tau}\theta|,$$

où $\sigma_{2,\tau}(\theta)$ est le conjugué de θ au-dessus de τ de plus grand module.

Cette formule permet de déterminer facilement les $\theta \in \bar{\boldsymbol{Q}}^*$ de degré 2 sur un corps quadratique K et dont la hauteur sur K est inférieure à une borne donnée. Ainsi l'inégalité $1 < H(K;\theta)^4 < (1+\sqrt{5})/2$ possède exactement 14 solutions (à conjugaison près): ce sont les nombres θ définis par les polynômes $X^2 - aX + b$ suivants:

$a = 1$, $b = -(3+\sqrt{13})/2$,
$$H(K;\theta)^4 = 1{,}3122\ldots \quad (H(\theta)^4 = 3{,}3028\ldots),$$

$a = 1$, $b = -1-\sqrt{2}$,
$$H(K;\theta)^4 = 1{,}3722\ldots \quad (H(\theta)^4 = 2{,}4142\ldots),$$

$a = 1$, $b = -(1+\sqrt{5})/2$,
$$H(K;\theta)^4 = 1{,}4675\ldots \quad (H(\theta)^4 = 1{,}4675\ldots),$$

$a = (5+\sqrt{21})/2$, $b = a$,
$$H(K;\theta)^4 = 1{,}5392\ldots \quad (H(\theta)^4 = 4{,}7913\ldots).$$

On constate que les 4 corps $\boldsymbol{Q}(\theta)$ sont de signature mixte, de sorte que la K-hauteur est donnée par la formule

$$H(K;\theta)^4 = \frac{|a| + \sqrt{a^2-4b}}{2\sqrt{|b|}}.$$

Le théorème (5.1) permet de comparer la K-hauteur à la hauteur usuelle dans quelques cas particuliers :

(5.4) Corollaire. *Soient $\theta \in \bar{\boldsymbol{Q}}^*$ et L un corps de nombres contenant $K(\theta)$. Si au-dessus de chaque plongement τ de K dans $\boldsymbol{C}$ il y a le même nombre de plongements σ de L dans $\boldsymbol{C}$ tels que $|\sigma\theta| > 1$, on a $H(K;\theta) = H(\theta)$. C'est notamment le cas si K et $\boldsymbol{Q}(\theta)$ sont linéairement disjoints sur $\boldsymbol{Q}$ (ou sur un corps quadratique imaginaire).*

Démonstration. La place de 1 dans les suites $|\sigma_{i,\tau}\theta|$ de (5.1) ne dépendant pas du choix de τ par hypothèse, on a pour tout i :

$$\max\Big(1, \prod_\tau |\sigma_{i,\tau}\theta|\Big) = \prod_\tau \max(1, |\sigma_{i,\tau}\theta|),$$

d'où par (5.1),

$$H(K;\theta)^{[L:\mathbb{Q}]} = N_{L/\boldsymbol{Q}}(\mathfrak{B}) \prod_\sigma \max(1, |\sigma\theta|). \ ∎$$

(5.5) Remarque. On peut démontrer aisément, à partir de (5.1), le résultat plus général suivant : soient K_0 un corps de nombres, K et K_1 deux corps de nombres contenant K_0 et linéairement disjoints sur K_0 (ou sur une extension quadratique de type C.M. de K_0). Alors, on a $H(K;\theta) = H(K_0;\theta)$ pour tout $\theta \in K_1^*$. En fait, la conclusion reste valable sous une hypothèse moins restrictive que la linéaire disjonction: il suffit que le groupe E_{K/K_0} soit contenu dans E_{K_1K/K_1} (rappelons que, pour une extension K_2/K_1 de corps de nombres, nous avons noté (dans (3.5) (i)) E_{K_2/K_1} le groupe des unités de K_2 dont la norme sur K_1 est une racine de l'unité). Les conditions $H(K;\theta) = H(K_0;\theta)$ pour tout $\theta \in K_1^*$ et $E_{K/K_0} \subset E_{K_1K/K_1}$ sont probablement équivalentes, mais nous ne l'avons prouvé que pour $K_0 = \boldsymbol{Q}$.

Nous introduisons maintenant deux classes de nombres algébriques θ pour lesquels, d'après (5.4), on a encore $H(K;\theta) = H(\theta)$.

(5.6) Définition. Un entier θ de $\bar{\boldsymbol{Q}}^*$ est un *K-nombre de Salem* (resp. *K-nombre de Pisot*) si, au-dessus de tout plongement τ de K dans $\boldsymbol{C}$, il existe un unique conjugué de θ de module > 1, et au moins un (resp. aucun) conjugué de module 1.

Si $\theta \in \bar{\mathbf{Q}}^*$ est un tel nombre, notons, pour tout plongement τ de K dans $\mathbf{C}$, θ_τ le conjugué de θ au-dessus de τ dont le module est > 1. On déduit immédiatement de (5.1) (ou (5.4)):

$$H(K;\theta)^{[K(\theta):\mathbf{Q}]} = H(\theta)^{[K(\theta):\mathbf{Q}]} = \prod_\tau |\theta_\tau| > 1.$$

Afin de nous rapprocher de la définition classique des nombres de Salem ou de Pisot, nous identifions l'algèbre $\mathbf{R}\otimes_{\mathbf{Q}} K$ au produit $A = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, où (r_1, r_2) désigne la signature du corps K : un élément $\alpha \in K$ est représenté par une suite $(\tau\alpha)_\tau$ de ses conjugués, τ parcourant l'ensemble des places infinies de K dans un ordre fixé (mais non canonique). Nous pouvons aussi représenter dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ un K-nombre de Salem ou de Pisot θ: nous lui associons la suite $(\theta_\tau)_\tau$ de ses conjugués de module > 1 (en effet, si τ est réel, l'unicité de θ_τ implique qu'il est réel, même si τ est ramifiée dans $K(\theta)$). Cette identification permet de voir qu'un $\mathbf{Q}$-nombre de Salem (resp. Pisot) est, au signe près, un nombre de Salem (resp. Pisot) au sens usuel (cf. [2]). Elle permet en outre de formuler une version relative des propriétés modulo 1 des nombres de Pisot, dont nous laissons la démonstration au lecteur:

(5.7) Proposition. *Soit Λ le réseau image dans $A = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ de l'anneau des entiers de K, et soit θ un K-nombre de Pisot (identifié à son image dans A). Alors, quand $n \to \infty$, la suite θ^n tend vers 0 modulo Λ. Plus précisément si $\alpha_n \in \Lambda$ est l'image de $\mathrm{Tr}_{K(\theta)/K}(\theta^n)$, on a*

$$\lim_{n\to\infty} (\theta^n - \alpha_n) = 0.$$

Nous laissons également au lecteur le soin de démontrer le résultat suivant relatif aux changements de corps de base :

(5.8) Proposition. *Soient $K_0 \subset K$ deux corps de nombres, et soit θ un K_0-nombre de Salem (resp. Pisot). Pour que θ soit un K-nombre de Salem (resp. Pisot), il faut et il suffit que K et $K_0(\theta)$ soient linéairement disjoints sur K_0.*

(5.9) Remarque. Pourvu qu'on puisse le représenter dans l'algèbre A, un nombre algébrique θ dont tous les conjugués ont un module $\neq 1$ et dont un au plus au-dessus de chaque plongement τ de K dans $\mathbf{C}$ est de module > 1, vérifie la propriété de (5.7). C'est le cas en particulier des K_0-nombres de Pisot, $K_0 \subset K$.

(5.10) Question. L'ensemble des K-nombres de Pisot est-il fermé dans A?

Noter qu'une réponse affirmative à (5.10) entraîne l'existence de nombres de Pisot pour K ayant une K-hauteur minimale, qu'il serait intéressant de déterminer pour certains corps K. Signalons que lorsque K est un corps quadratique imaginaire, les nombres de Pisot pour K font partie de l'ensemble des nombres considérés par C. Chamfy dans [3].

6. Autour du problème de Lehmer. Rappelons, en termes de hauteurs, le problème classique de Lehmer, que nous proposons, comme c'est l'usage, sous forme de conjecture ([8], p. 476).

(6.1) Conjecture de Lehmer (forme faible). *Il existe une constante $C > 1$ telle que, pour tout entier algébrique θ différent de 0 et d'une racine de l'unité, on ait, n désignant le degré de θ, $H(\theta)^n \geqslant C$.*

Une forme forte de la conjecture est que le minimum de $H(\theta)^n$ est atteint lorsque θ est le plus petit nombre de Salem connu ($\theta = 1{,}17628\ldots$), et même qu'il existe des minima successifs donnés par les petits nombres de Salem (voir Boyd [2], p. 326, table).

Il résulte du §3 (3.6) que la conjecture de Lehmer (6.1) est équivalente à la conjecture suivante :

(6.2) Conjecture. *Il existe une constante $C > 1$ telle que, pour tout corps de nombres $K \subset \bar{\mathbf{Q}}$ et tout entier algébrique $\theta \in \bar{\mathbf{Q}}^*$ dont aucune puissance n'est une unité de K, on ait $H(K;\theta)^{n'} \geqslant C$, avec $n' = [K(\theta'):\mathbf{Q}]$, où θ' désigne l'élément introduit dans* (3.2).

(On a $n' \leqslant [K(\theta):\mathbf{Q}]^2$, et $n' = [K(\theta):\mathbf{Q}]$ si $N_{K(\theta)/K}(\theta) \in \mu_K$; noter que, si θ n'est pas une unité, on a $H(K;\theta)^n \geqslant 2$.)

(6.3) Question. *Peut-on, dans l'inégalité de* (6.2), *remplacer n' par $[K(\theta):\mathbf{Q}]$ même lorsque θ est une unité dont la norme relative n'est pas racine de l'unité?*

(6.4) Problème. *Trouver, pour un corps K donné, une valeur au moins conjecturale du minimum de $H(K;\theta)^{n'}$ sur les $\theta \in \bar{\mathbf{Q}}^*$ dont aucune puissance n'est une unité de K.*

En liaison avec (6.4), il convient de signaler le résultat de Smyth ([11]), selon lequel la hauteur minimale d'un nombre algébrique qui n'est pas racine d'un polynôme réciproque est atteinte sur le plus petit nombre de Pisot (la racine réelle du polynôme $X^3 - X - 1$). Il serait intéressant de démontrer des énoncés généralisant celui de Smyth à d'autres corps de base que le corps $\mathbf{Q}$. Notons que, lorsque θ est un K-nombre de Pisot, il ne peut être racine d'un polynôme reciproque que lorsque $K(\theta)$ est un corps totalement réel de degré 2 sur K, ce qui répond partiellement à la question (5.10).

Bibliographie

[1] A.-M. Bergé et J. Martinet, *Sur les minorations géométriques des régulateurs*, Sém. Théorie des Nombres de Paris, exposé du 12 octobre 1987, Birkhäuser, à paraître.
[2] D. W. Boyd, *Small Salem numbers*, Duke Math. J. 44 (1977), 315–327.
[3] C. Chamfy, *Fonctions méromorphes dans le cercle-unité et leurs séries de Taylor*, Ann. Inst. Fourier 8 (1958), 211–262.
[4] T. W. Cusick, *Lower bounds for regulators*, Journées Arithmétiques de 1983, Lecture Notes nº 1068, Springer-Verlag, 1984, 63–73.

[5] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.
[6] E. Friedman, *Analytic formulas for the regulator of a number field*, à paraître.
[7] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.
[8] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. 34 (1933), 461–479.
[9] R. Remak, *Über Grössenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers*, Comp. Math. 10 (1952), 245–285.
[10] J. H. Silverman, *An inequality relating the regulator and the discriminant of a number field*, J. Number Theory 19 (1984), 437–442.
[11] C. J. Smyth, *On the product of conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), 169–175.
[12] B. L. van der Waerden, *Die Reduktionstheorie der positiven quadratischen Formen*, Acta Math. 96 (1956), 265–293.

Ajouté aux épreuves. A Schinzel nous signale les deux références suivantes qui améliorent des résultats que nous citons ([5], [11]):

R. Louboutin, *Sur la mesure de Mahler d'un nombre algébrique*, Comptes Rendus Acad. Sc. Paris I, 296 (1983), 707–708.

A. Bazylewicz, *On the product of the conjugates outside the unit circle of an algebraic integer*, Acta Arith. 30 (1976), 43–61.

Reçu le 21.3.1988
et dans la forme modifiée le 13.6.1988 (1800)
