S. Louboutin
Nagoya Math. J.
Vol. 130 (1993), 1–18

MINORATIONS D'UNITÉS FONDAMENTALES APPLICATIONS

STÉPHANE LOUBOUTIN

1. Cas des corps quadratiques réels

Un idéal entier $\mathbf{I}$ d'un corps quadratique réel $\mathbf{k}$ est dit *primitif* lorsque $n \in \mathbf{N}^*$ et (n) divise $\mathbf{I}$ impliquent $n = 1$. Un idéal entier est primitif si et seulement si il vérifie les trois conditions suivantes:
(i) il n'est divisible par aucun idéal premier inerte,
(ii) il n'est divisible par le carré d'aucun idéal premier ramifié,
(iii) si il est divisible par un idéal premier totalement décomposé, alors il n'est pas divisible par son idéal premier conjugué.

En particulier, le conjugué d'un idéal primitif est primitif, où le *conjugué* d'un idéal $\mathbf{I}$ est l'idéal noté $\tilde{\mathbf{I}}$ et défini par: $\tilde{\mathbf{I}} = \{\tau(i)\ ;\ i \in \mathbf{I}\}$, où τ est le $\mathbf{Q}$-isomorphisme non trivial de $\mathbf{k}$. De plus, si $\mathbf{I}$ est primitif et de norme première au discriminant de $\mathbf{k}$, alors toute les puissances de $\mathbf{I}$ et de son idéal conjugué son primitives, et de plus deux à deux distinctes si $\mathbf{I}$ n'est pas l'anneau des entiers de $\mathbf{k}$. D'où l'intérêt du lemme suivant:

LEMME (a). *Si* $D = B^2 \pm 4A$ *vérifie* $D \equiv 1 \pmod 4$ *et si* D *n'est pas un carré parfait, alors l'idéal principal* $\mathbf{I} = \left(\frac{B + \sqrt{D}}{2}\right)$ *est primitif et de norme* A *première au discriminant du corps quadratique réel* $\mathbf{Q}(\sqrt{D})$ *(qui n'est de discriminant* D *que si* D *est libre de facteur carré).*

Preuve. Soit $D = f^2 \Delta$ où $\Delta \equiv 1 \pmod 4$ libre de facteur carré est le discriminant du corps quadratique réel $\mathbf{k} = \mathbf{Q}(\sqrt{D})$. Si $\omega = \frac{B + \sqrt{D}}{2}$, alors l'idéal principal (ω) est de norme A première à D, donc première à Δ. Il reste à voir

Received July 8, 1992.

qu'il est primitif. Mais si (n) divise (ω) où n est un entier relatif strictement positif, alors n divise ω, donc divise sa trace B et n^2 divise sa norme A, de sorte que n divise également D. Puisque A et D sont supposés premiers entre eux, nous avons $n = 1$ et le résultat désiré. □

Soit maintenant $\mathbf{I}$ un idéal entier primitif de norme A d'un corps quadratique réel $\mathbf{k}$ de discriminant $\Delta \geq 5$. Il existe alors B, unique modulo $2A$ tel que $\mathbf{I}$ soit le $\mathbf{Z}$-module $A\mathbf{Z} + \frac{B+\sqrt{\Delta}}{2}\mathbf{Z}$ avec $4A$ divisant $\Delta - B^2$, notation que nous abrégeons en $\mathbf{I} = \left(A, \frac{B+\sqrt{\Delta}}{2}\right)_{\mathbf{Z}}$. Un tel idéal est dit *réduit* si il est possible de choisir B modulo $2A$ (de manière alors unique) de telle sorte que les inégalités suivantes soient satisfaites:

$$x_0(\mathbf{I}) > 1 > -x_0(\mathbf{I})' > 0, \tag{1}$$

où $x_0(\mathbf{I}) \overset{\text{def}}{=} \frac{B+\sqrt{\Delta}}{2A}$ et où $x_0(\mathbf{I})'$ est le conjugué de $x_0(\mathbf{I})$ dans $\mathbf{k}$. Ces inégalités sont équivalentes aux suivantes:

$$B + \sqrt{\Delta} > 2A > \sqrt{\Delta} - B > 0, \tag{2}$$

et impliquent en particulier: $B > \sqrt{\Delta} > 2A$, de sorte que l'on a alors:

$$x_0(\mathbf{I}) > \frac{\sqrt{\Delta}}{A}\left(1 - \frac{A}{\sqrt{\Delta}}\right). \tag{3}$$

De plus, il est alors aisé de voir que ces inégalités (2) sont satisfaites pour un choix convenable de B modulo $2A$ dès lors que l'on $A \leq \frac{1}{2}\sqrt{\Delta}$, i.e. un idéal primitif de norme A telle que $A \leq \frac{1}{2}\sqrt{\Delta}$ est réduit.

Il n'existe qu'un nombre fini d'idéaux réduits, donc qu'un nombre fini d'idéaux réduits principaux, et l'unité fondamentale $\varepsilon_0 > 1$ de $\mathbf{k}$ vérifie:

$$\varepsilon_0 = \prod_{\substack{\mathbf{I} \text{ réduit} \\ \text{et principal}}} x_0(\mathbf{I}). \tag{4}$$

Puisque d'après (1) chacun des termes de ce produit est strictement plus grand que 1, alors les identités (3) et (4) permettent de minorer ε_0 dès lors que l'on connait quelques idéaux principaux primitifs de normes inférieures à $\frac{1}{2}\sqrt{\Delta}$. Si une unité $\varepsilon > 1$ de $\mathbf{k}$ est connue, cette minoration de l'unité fondamentale peut permettre de montrer sans fastidieux calculs que l'on a $\varepsilon < \varepsilon_0^2$, ce qui impliquera que

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

cette unité ε est égale à ε_0, i.e. que cette unité ε est l'unité fondamentale de $\mathbf{k}$. Notons que nous aurons la même conclusion en montrant que l'on a $\varepsilon < \varepsilon_0^3$ dès lors que ε est de norme -1.

Illustrons sur un exemple les techniques que nous voulons développer. Considérons donc la famille de corps quadratiques réels donnée par $\mathbf{k} = \mathbf{Q}(\sqrt{D})$ où $D = m^2 + 4 \equiv 5 \pmod 8$ est supposé libre de facteurs carré, de sorte que $\mathbf{k}$ est de discriminant D et que $\varepsilon = \dfrac{m + \sqrt{D}}{2}$ est une unité de $\mathbf{k}$ telle que $1 < \varepsilon < \sqrt{D}$. Puisque l'idéal $\mathbf{I}$ de norme 1 égal à l'anneau des entiers de $\mathbf{k}$ est réduit, nous avons d'après (4) la minoration $\varepsilon_0 > \sqrt{D} - 1$, de sorte que l'on a $1 < \varepsilon < \varepsilon_0^2$, et donc $\varepsilon_0 = \varepsilon = \dfrac{m + \sqrt{D}}{2}$. De plus, si $\mathbf{I}$ est un idéal primitif et principal de $\mathbf{k}$ de norme A telle que $A < \dfrac{1}{2}\sqrt{D}$, alors nous avons la minoration $\varepsilon_0 > (\sqrt{D} - 1)\left(\dfrac{\sqrt{D}}{A} - 1\right)$, qui combinée à la majoration $\varepsilon_0 < \sqrt{D}$ implique $A > \dfrac{\sqrt{D} - 1}{2\sqrt{D} - 1}\sqrt{D}$, donc implique $A > \dfrac{m - 1}{2}$, donc implique $A \geq \dfrac{m + 1}{2} > \dfrac{1}{2}\sqrt{D}$. Il en résulte que si $\mathbf{k}$ est principal, alors p premier et $p < \dfrac{1}{2}\sqrt{D}$ impliquent que p est inerte dans $\mathbf{k}$. Puisque $\dfrac{1}{2}\sqrt{D}$ est une borne de Minkowski, la réciproque de ce résultat est également vraie et nous avons donc retrouvé un résultat de [6]:

PROPOSITION. *Le corps quadratique réel* $\mathbf{k} = \mathbf{Q}(\sqrt{D})$, *où* $D = m^2 + 4 \equiv 5 \pmod 8$ *est supposé libre de facteurs carré, est principal si et seulement si pour tout nombre premier impair* p *tel que* $p \leq \dfrac{1}{2}\sqrt{D}$ *le symbole de Legendre* $\left(\dfrac{D}{p}\right)$ *est égal à* -1.

Maintenant, si un idéal principal primitif $\mathbf{I}$ de norme $A \geq 2$ première à Δ est connu et si $n \geq 0$ est un entier tel que $A^n \leq \dfrac{1}{2}\sqrt{\Delta}$, nous connaissons $2n + 1$ idéaux réduits principaux deux à deux distincts, à savoir: l'idéal principal égal à l'anneau des entiers, les puissances $\mathbf{I}^k$ pour $1 \leq k \leq n$, les idéaux conjugués conjugués $\tilde{\mathbf{I}}^k$ de ces puissances.

De (3), de (4) et de $A^n \leq \dfrac{1}{2}\sqrt{\Delta}$, nous déduisons la minoration suivante de ε_0:

$$\varepsilon_0 \geq \sqrt{\Delta}\left(1 - \frac{1}{\sqrt{\Delta}}\right)\prod_{k=1}^{n}\frac{\Delta}{A^{2k}}\left(1 - \frac{A^k}{\sqrt{\Delta}}\right)^2 \geq \frac{\Delta^{n+\frac{1}{2}}}{A^{n(n+1)}}\prod_{k=0}^{n}\left(1 - \frac{A^{n-k}}{\sqrt{\Delta}}\right)^2$$

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

$$\geq 2^{n+1}\Delta^{n/2}\prod_{k=1}^{n}\left(1-\frac{1}{2A^k}\right)^2 \geq 2^{n+1}\Delta^{n/2}\prod_{k\geq 1}\left(1-\frac{1}{2^k}\right)^2.$$

D'où

$$(*)\qquad \varepsilon_0 \geq \frac{1}{6}2^n\Delta^{n/2}.$$

Supposons de plus connu un second idéal principal primitif $\mathbf{J}$ de norme $B \geq 2$ première à A. Soit n' un entier tel que $A^{n'}B < \frac{1}{2}\sqrt{\Delta}$. Nous connaissons alors $2n'+1$ idéaux réduits en plus des précédents: à savoir $\mathbf{J}$, les $\mathbf{I}^k\mathbf{J}$ et les $\tilde{\mathbf{I}}^k\mathbf{J}$ pour $1 \leq k \leq n'$. Nous amendons donc la minoration précédente de ε_0 du facteur Π où:

$$\Pi \overset{\text{def}}{=} \frac{\sqrt{\Delta}}{B}\left(1-\frac{B}{\sqrt{\Delta}}\right)\prod_{k=1}^{n'}\frac{\Delta}{A^{2k}B^2}\left(1-\frac{A^kB}{\sqrt{\Delta}}\right)^2 > \frac{2^{n'+1}\Delta^{n'/2}}{B^{n'}}\prod_{k\geq 1}\left(1-\frac{1}{2^k}\right)^2,$$

de sorte que nous obtenons:

$$(**)\qquad \varepsilon_0 \geq \frac{1}{36}\frac{2^{n+n'}\Delta^{(n+n')/2}}{B^{n'}}.$$

Si B est de plus supposé premier à Δ, nous avons même $2n'+1$ idéaux réduits supplémentaires, à savoir $\tilde{\mathbf{J}}$, les $\mathbf{I}^k\tilde{\mathbf{J}}$ et les $\tilde{\mathbf{I}}^k\tilde{\mathbf{J}}$ pour $1 \leq k \leq n'$. Nous obtenons donc:

$$(***)\qquad \varepsilon_0 \geq \frac{1}{216}\frac{2^{n+2n'}\Delta^{(n+2n')/2}}{B^{2n'}}.$$

Pour nos applications, et toujours sous l'hypothèse de B premier à A et premier à Δ, nous utiliserons également la minoration plus faible suivante:

$$(****)\qquad \varepsilon_0 \geq \frac{1}{6}2^n\Delta^{n/2}\frac{\Delta}{4B^2}$$

que l'on obtient en remarquant que $\mathbf{J}$ et $\tilde{\mathbf{J}}$ sont réduits, et que l'on a $\frac{\sqrt{\Delta}}{B}\left(1-\frac{B}{\sqrt{\Delta}}\right) > \frac{\sqrt{\Delta}}{2B}$. Nous avons donc prouvé:

THÉORÈME 1. *Soit* $\mathbf{k}$ *un corps quadratique réel de discriminant* $\Delta \geq 5$. *Soit* $\mathbf{I}$ *un idéal primitif et principal de* $\mathbf{k}$ *de norme* $A \geq 2$ *première à* Δ.

Alors, pourvu que n *vérifie* $A^n \leq \frac{1}{2}\sqrt{\Delta}$, *l'unité fondamentale* $\varepsilon_0 > 1$ *de* $\mathbf{k}$ *vérifie*:

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

$$\varepsilon_0 \geq \frac{1}{6} 2^n \Delta^{n/2}.$$

De plus, si $\mathbf{J}$ *est un second idéal primitif et principal de* $\boldsymbol{k}$ *de norme* $B \geq 2$ *première à* Δ *et première à* A, *nous avons*:

$$\varepsilon_0 \geq \frac{1}{6} 2^n \Delta^{n/2} \frac{\Delta}{4B^2}.$$

Nous appliquons maintenant aux corollaires (A) et (B) ce résultat à deux des familles de corps quadratiques réels étudiées par L. Bernstein. Nous allons retrouver que ses unités sont fondamentales et ce sans les fastidieux calculs dont il avait besoin, à savoir le calcul explicite de tout le cycle des idéaux réduits principaux à l'aide de l'algorithme de développement en fractions continues. Nous donnons également un critère de principalité des corps de ces familles suffisamment contraignant pour qu'il ne soit satisfait que par un petit nombre de corps de ces familles, de sorte que nous puissions sans beaucoup de calculs numériques de nombres de classes déterminer tous les corps principaux de ces familles (à au plus une exception près qui ne saurait se présenter sous l'assomption d'une forme convenable de l'hypothèse de Riemann généralisée, i.e. en supposant ou bien que les fonction zêta des corps quadratiques réels n'ont pas de zeros réels strictement positifs, ou bien en supposant que les zeros complexes non triviaux des fonctions zêta des corps quadratiques réels sont situés sur la droite $\Re(s) = \frac{1}{2}$.). Notre condition nécessaire de principalité est établie à nouveau sans que soit requise la connaissance explicite du cycle complet des idéaux réduits principaux, de sorte qu'ici encore nous simplifions grandement l'approche de ces questions telle qu'elle est par exemple considérée dans [4].

COROLLAIRE (A). *Soit* $D = (A^N + A - 1)^2 + 4A \equiv 1 \pmod 4$ *avec* $A \geq 2$ *et* $N \geq 3$.

Alors,

$$\varepsilon = \left(\frac{A^N + A - 1 + \sqrt{D}}{2A}\right)^N \frac{A^N + A + 1 + \sqrt{D}}{2}$$

est une unité de norme $(-1)^N$ *de l'ordre* $Z\left[\frac{1+\sqrt{D}}{2}\right]$. *De plus, cette unité est l'unité fondamentale du corps quadratique réel* $\mathbf{k} = \mathbf{Q}(\sqrt{D})$ *dès lors que* D *est libre de facteur carré.*

Supposons toujours D *libre de facteur carré. Si* $\mathbf{k}$ *est principal alors* A *est premier*

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

et les symboles de Legendre $\left(\frac{D}{p}\right)$ *ne valent pas* $+1$ *pour* p *premier impair ne divisant pas* A *et tel que* $p^2 \leq \frac{1}{8}\sqrt{D}$. *Il en résulte que pour* $D \leq 10^{18}$ *libre de facteur carré le corps* $\mathbf{k}$ *est principal si et seulement si* $(D, A, N) = (89,2,3), (853,3,3)$ *ou* $(1097,2,5)$. *De plus, il existe au plus un autre tel corps principal, et sous une forme convenable de l'hypothèse de Riemann généralisée, ces* 3 *corps sont les seuls de cette famille qui sont principaux.*

Preuve. Montrons premièrement que ε est une unité.

Pour cela, posons $B = A^N + A - 1$ et $\omega = \frac{B + 2 + \sqrt{D}}{2}$, de sorte que $D = B^2 + 4A$ et

$$\frac{1}{\varepsilon} = \frac{1}{\omega}\left(\frac{\sqrt{D} - B}{2}\right)^N = \frac{1}{\omega}(\omega - (B+1))^N.$$

Puisque $\omega^2 - (B+2)\omega + A^N = 0$ et puisque $\frac{(B+1)^N}{\omega} = \frac{A^N}{\omega}(A^{N-1}+1)^N$ appartient donc à $\mathbf{Z}[\omega]$, alors $1/\varepsilon$ y appartient également. De plus, $1/\varepsilon$ est de norme $(-1)^N$ et l'ordre $\mathbf{Z}[\omega]$ est stable sous l'action de τ, donc ε est une unité de $\mathbf{Z}[\omega] = \mathbf{Z}\left[\frac{1+\sqrt{D}}{2}\right]$.

Maintenant, l'idéal principal $\mathbf{I} = \left(\frac{B+\sqrt{D}}{2}\right)$ étant de norme A première à D, le lemme (a) nous permet d'appliquer le théorème 1 avec $n = N - 1$. D'où: $\varepsilon_0 \geq \frac{1}{3}2^{N-2}D^{(N-1)/2}$. D'un autre côté, puisque nous avons $A^N + A - 1 \leq \sqrt{D} \leq A^N + A$, nous avons:

$$\varepsilon \leq \left(\frac{\sqrt{D}}{A}\right)^N \frac{2A^N + 2A + 1}{2} \leq \left(1 + \frac{1}{A^{N-1}} + \frac{1}{2A^N}\right) D^{N/2} \leq \frac{21}{16} D^{N/2} \leq 2D^{N/2},$$

de sorte que le premier résultat découle de la minoration suivante:

$$\frac{\varepsilon_0^2}{\varepsilon} \geq \frac{1}{9}2^{2N-5}D^{(N-2)/2} > 1.$$

Quant à la première assertion du second résultat, elle résulte de ce que si A n'est pas premier, alors il admet un diviseur A' tel que $2 \leq A' \leq \sqrt{A}$ et qu'il existe un idéal primitif $\mathbf{I}'$ de norme A'. Si $\mathbf{k}$ était principal, nous pourrions donc appliquer la première assertion du théorème 1 avec A' et $n' = 2N - 2$, et nous obtiendrions donc une contradiction des inégalités suivantes:

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

$$\varepsilon_0 \geq \frac{1}{3} 2^{2N-3} D^{N-1} > 2D^{N/2} > \varepsilon > 1.$$

La seconde assertion du second résultat résulte de la seconde assertion du théorème 1 appliquée avec $B = p$ où p premier impair ne divisant pas A est supposé tel que $\left(\frac{D}{p}\right) = +1$ (on prend pour $\mathbf{J}$ un quelconque des deux idéaux premiers totalement décomposés au dessus de p). Nous obtenons en effet alors une contradiction des inégalités suivantes:

$$\varepsilon_0 \geq \frac{1}{3} 2^{N-2} D^{(N-1)/2} \frac{D}{4p^2} \geq \frac{1}{3} 2^{N-3} D^{N/2} \geq \frac{4}{3} D^{N/2} > \frac{21}{16} D^{N/2} > \varepsilon > 1.$$

Finalement, un calcul numérique sur ordinateur donne aisément qu'il n'existe que 22 valeurs de D avec $D \leq 10^{18}$ telles que les symboles de Legendre $\left(\frac{D}{p}\right)$ ne valent pas $+1$ pour p premier impair ne divisant pas A et tel que $p^2 \leq \frac{1}{8}\sqrt{D}$. De plus, seules 8 de ces 22 valeurs correspondent à des D libres de facteur carré tels que le 2-rang du groupe des classes d'idéaux du corps quadratique réel correspondant soit nul. Finalement, le calcul numérique des nombres de classes de ces 8 corps nous donne le dernier résultat annoncé. □

COROLLAIRE (B). *Soit $A = 2a + 1 \geq 3$ un entier impair, soit $N \geq 2$ un entier et soit $D = (A^N + a)^2 + A$. Alors,*

$$\varepsilon = \left(\frac{A^N + a + \sqrt{D}}{A}\right)^{2N} \frac{(A^N + a + 1 + \sqrt{D})^2}{2}$$

est une unité de norme $+1$ de l'ordre $\mathbf{Z}[\sqrt{D}]$. De plus, cette unité est l'unité fondamentale du corps quadratique réel $\mathbf{k} = \mathbf{Q}(\sqrt{D})$ dès lors que D est libre de facteur carré.

Preuve. La première partie de cet énoncé se prouve semblablement à celle du corollaire (A). Pour la seconde, nous remarquons préalablement que ε n'est pas le carré de l'unité fondamentale ε_0 de $\mathbf{k}$. Sinon, ε étant le carré d'un élément de $\mathbf{k}$, il en serait de même de 2 et nous aurions $\mathbf{k} = \mathbf{Q}(\sqrt{2})$, i.e. nous aurions $D = 2$. Pour montrer que ε est fondamentale, il suffit donc de voir que l'on $1 < \varepsilon < \varepsilon_0^3$.

Nous remarquons premièrement que $\mathbf{J} = (A^N + a + 1 + \sqrt{D})$ est un idéal primitif et principal de norme $2A^N$. De plus, puisque

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

$$\frac{A^N + a + 1 + \sqrt{D}}{A^N + a - \sqrt{D}} = \frac{(A^N + a + 1 + \sqrt{D})(A^N + a - \sqrt{D})}{-A}$$

appartient à $\mathbf{Z}[\sqrt{D}]$, alors $\mathbf{J}$ est inclus dans l'idéal primitif et principal $\mathbf{I} = (A^N + a - \sqrt{D})$ qui est lui de norme A. Il en résulte que $\mathbf{J} = \mathbf{K}\mathbf{I}^N$ où $\mathbf{K}$ est un idéal entier de norme 2, qui est donc primitif. D'après (**) et en remarquant que $\mathbf{K}$ est de discriminant Δ tel que $\Delta = 4D$, nous pouvons prendre $n = N$, $B = 2$ et $N' = N - 1$, de sorte que nous obtenons $\varepsilon_0 \geq \frac{1}{9} 2^{3N-3} D^{N-\frac{1}{2}}$. Puisque nous avons $A^N + a \leq \sqrt{D} \leq A^N + a + 1$, nous avons $\varepsilon \leq \frac{1}{2}\left(\frac{2A^N + A + 1}{A^N}\right)^2 D^N \leq \frac{121}{32} D^N < 4D^N$, et le résultat en découle aisément. □

Dans (par exemple) la situation du corollaire (A), et lorsque D n'est plus supposé libre de facteur carré, le résultat de L. Bernstein donne seulement que ε est l'unité fondamentale de l'ordre $\mathbf{Z}\left[\frac{1 + \sqrt{D}}{2}\right]$. Pour obtenir une expression paramétrique de l'unité fondamentale de $\mathbf{Q}(\sqrt{D})$ avec les techniques de L. Bernstein, il faudrait avec les notations du corollaire ci-dessous développer en fractions continues le réel quadratique $\frac{1 + \sqrt{\Delta}}{2}$, ce qui ne saurait être possible qu'en se fixant au préalable un f et en faisant varier A de telle sorte que la partie carrée de D fût égale à f. Pour chaque valeur de f, on obtiendrait ainsi éventuellement (et seulement après de fastidieux calculs) un développement de $\frac{1 + \sqrt{\Delta}}{2}$ qui permettrait de déterminer ε_0.

La supériorité de notre approche est claire: le corollaire précédent reste valable pourvu que f soit suffisamment petit par rapport à D. Plus précisément, nous avons par exemple le résultat suivant dont nous n'avons pas trouvé d'équivalent dans la littérature actuelle:

COROLLAIRE (C). *Soit* $D = (A^N + A - 1)^2 + 4A \equiv 1 \pmod 4$ *avec* $A \geq 2$ *et* $N \geq 3$ *impair. Alors,*

$$\varepsilon = \left(\frac{A^N + A - 1 + \sqrt{D}}{2A}\right)^N \frac{A^N + A + 1 + \sqrt{D}}{2}$$

est une unité de l'ordre $\mathbf{Z}\left[\frac{1 + \sqrt{D}}{2}\right]$. *De plus, si* $D = f^2 \Delta$ *avec* Δ *libre de facteur carré (donc égal au discriminant de* $\mathbf{k}$*), alors cette unité est l'unité fondamentale du*

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

corps quadratique réel $\mathbf{k} = \mathbf{Q}(\sqrt{D})$ *dès lors que l'on a* $f \leq 8\Delta\ (24\sqrt{\Delta})^{-3/N}$

Preuve. Elle reste semblable à celle du corollaire (A) en tenant compte de ce que le discriminant de $\mathbf{k}$ valant maintenant Δ, nous avons seulement la minoration $\varepsilon_0 \geq \frac{1}{6} 2^{N-1} \Delta^{(N-1)/2}$. Puisque nous avons $1 < \varepsilon \leq 8D^{N/2}$, et puisque ε est de norme -1, elle sera fondamentale dès lors que l'on aura: $\varepsilon < \varepsilon_0^3$, donc en particulier dès lors que l'inégalité donnée dans cet énoncé sera satisfaite. □

2. Cas des corps biquadratiques totalement imaginaires non galoisiens qui sont des extensions quadratiques d'un corps quadratique imaginaire principal

Soit $\mathbf{K}$ un tel corps biquadratique et soient $\mathbf{k}$ ce corps quadratique imaginaire principal, $\mathbf{A}_\mathbf{k}$ l'anneau des entiers de $\mathbf{k}$ et $\delta_{\mathbf{K}/\mathbf{k}}$ le discriminant relatif de l'extension $\mathbf{K}/\mathbf{k}$ (qui n'est déterminé qu'au carré d'une racine de l'unité de $\mathbf{k}$ près). Rappelons brièvement la notion d'idéaux réduits développée par H. Amara [1] dans ce cadre, ainsi que son lien avec l'unité fondamentale ε_0 de $\mathbf{K}$. Un idéal entier non nul $\mathbf{I}$ de $\mathbf{K}$ est dit $\mathbf{k}$-*primitif* lorsque $\alpha \in \mathbf{A}_\mathbf{k}$ et (α) divise $\mathbf{I}$ impliquent $(\alpha) = \mathbf{A}_\mathbf{k}$. Un idéal entier $\mathbf{I}$ de $\mathbf{K}$ de norme relative $A = N_{\mathbf{K}/\mathbf{k}}(\mathbf{I}) \in \mathbf{A}_\mathbf{k}$ est dit *réduit* lorsqu'il est non nul, entier et vérifie:

$$z \in \mathbf{I} \text{ et } z \neq 0 \text{ impliquent } \mathrm{Max}\,(|z|, |z^\tau|) \geq |A|,$$

où τ est le $\mathbf{k}$-isomorphisme non trivial de l'extension quadratique $\mathbf{K}/\mathbf{k}$ qui, semblablement au cas quadratique réel, permet de définir le conjugué d'un idéal, de sorte que le conjugué d'un idéal primitif est primitif, et que le conjugué d'un idéal réduit est réduit. Notons qu'un idéal réduit est primitif. Soit alors $\mathbf{I}$ un idéal réduit de norme relative A. Nous définissons son élément de conversion noté $h_0(\mathbf{I})$ par les trois propriétés suivantes:

$$h_0(\mathbf{I}) \in \mathbf{I},$$
$$|h_0(\mathbf{I})| < |A|,$$
$$h \in \mathbf{I},\ h \neq 0 \text{ et } |h| < |A| \text{ impliquent } |h_0^\tau(\mathbf{I})| \leq |h^\tau|.$$

On montre que cet élément de conversion existe et est unique, à multiplication par une racine de l'unité de $\mathbf{k}$ près. Semblablement au cas des corps quadratiques réels, il n'existe qu'un nombre fini d'idéaux réduits, donc qu'un nombre fini d'idéaux réduits principaux et nous avons premièrement:

$$\varepsilon_0 = \prod_{\substack{\mathbf{I} \text{ réduit} \\ \text{et principal}}} \frac{h_0^\tau(\mathbf{I})}{N_{K/\mathbf{k}}(\mathbf{I})}. \tag{5}$$

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

Nous avons secondement:

LEMME (b).

(a) *Un idéal primitif de norme relative A telle que* $|A| \leq \frac{1}{2}\sqrt{|\delta_{K/k}|}$ *est réduit.*

(b) *Si* $\mathbf{I}$ *est réduit et de norme relative A, alors*

$$\left|\frac{h_0^\tau(\mathbf{I})}{A}\right| \geq \frac{\sqrt{|\delta_{K/k}|}}{|A|}\left(1 - \frac{|A|}{\sqrt{|\delta_{K/k}|}}\right). \tag{6}$$

Preuve. Les entiers algébriques h de $\mathbf{k}$ s'écrivant sous la forme $h = \frac{\alpha + \beta\sqrt{\delta_{K/k}}}{2}$ avec α et β dans $\mathbf{A}_k$, nous avons $|h - h^\tau| \geq \sqrt{\delta_{K/k}}$ pour $h \neq 0$.

Le premier point résulte donc de ce que si $\mathbf{I}$ n'est pas réduit, alors il existe h non nul dans $\mathbf{I}$ tel que $|h| < |A|$ et $|h^\tau| < |A|$. Nous avons alors $2|A| > |h - h^\tau| \geq \sqrt{|\delta_{K/k}|}$.

Le second point résulte de ce que

$$\left|\frac{h_0^\tau(\mathbf{I})}{A}\right| = \left|\frac{h_0^\tau(\mathbf{I}) - h_0(\mathbf{I})}{A} + \frac{h_0(\mathbf{I})}{A}\right| \geq \left|\frac{h_0^\tau(\mathbf{I}) - h_0(\mathbf{I})}{A}\right| - 1 \geq \frac{\sqrt{|\delta_{K/k}|}}{|A|} - 1.$$

□

Semblablement au théorème 1 et en remarquant que $2\prod_{k\geq 0}\left(1 - \frac{1}{2(\sqrt{2})^k}\right)^2 \geq \frac{1}{31}$, nous en déduisons le résultat suivant:

THÉORÈME 2. *Soit* $\mathbf{k}$ *un corps quadratique imaginaire principal et soit* $\mathbf{K}/\mathbf{k}$ *une extension quadratique de* $\mathbf{k}$ *de discriminant relatif* $\delta_{K/k}$, *avec* $\mathbf{K}/\mathbf{Q}$ *non galoisienne. Soit* $\mathbf{I}$ *un idéal non nul de* $\mathbf{K}$ *de norme relative A première à* $\delta_{K/k}$ *et telle que* $|A|^2 \geq 2$. *Supposons de plus que* $\mathbf{I}$ *soit principal et* $\mathbf{k}$*-primitif.*

Alors, pourvu que n vérifie $|A|^n \leq \frac{1}{2}\sqrt{|\delta_{K/k}|}$, *l'unité fondamentale* ε_0 *de* $\mathbf{K}$ *vérifie:*

$$|\varepsilon_0| \geq \frac{1}{31}2^n|\delta_{K/k}|^{n/2}.$$

COROLLAIRE (D). *Soit* $A \in \mathbf{Z}[i] \setminus \{\pm 1, \pm i\}$ *tel que* $\delta = (A^N \pm (A-1))^2 + 4A$ *ne soit ni purement réel ni purement imaginaire. Alors,*

$$\varepsilon = \left(\frac{A^N \pm (A-1) + \sqrt{\delta}}{2A}\right)^N \frac{A^N \pm (A+1) + \sqrt{\delta}}{2}$$

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

est une unité du corps biquadratique non galoisien $\mathbf{K} = \mathbf{Q}(i, \sqrt{\delta})$. *Supposons de plus que* δ *soit libre de facteur carré dans* $\mathbf{Z}[i]$. *Alors, cette unité est fondamentale dès lors que l'on a* $N \geq 7$ *et si* $\mathbf{K}$ *est principal, alors* A *est irréductible dans* $\mathbf{Z}[i]$.

Preuve. La preuve de la première partie de ce résultat reste semblable à celle du corollaire (A). On remarque préalablement que $A^N \pm (A-1) = a + ib$ avec a et b deux entiers relatifs de parités contraires. En conséquence, il existe $\eta \in \{1, i\}$ tel que l'on ait $\delta \equiv \eta^2 (\mathrm{mod}\ 4\mathbf{Z}[i])$, de sorte que δ est le discriminant de $\mathbf{K}$ dès lors que δ est libre de facteur carré dans $\mathbf{Z}[i]$. De plus, demander que δ ne soit ni purement réel ni purement imaginaire, c'est demander que l'extension biquadratique $\mathbf{K}/\mathbf{Q}$ ne soit pas galoisienne, de sorte que la théorie des cycles d'idéaux réduits développée par H. Amara (voir [1]) s'y applique. Puisque ε est une unité, nous avons $|\varepsilon||\tau(\varepsilon)| = 1$. Nous pouvons donc supposer la détermination de $\sqrt{\delta}$ choisie telle que l'on ait $|\varepsilon| \geq 1$. Nous majorons maintenant ε de la manière suivante: on remarque premièrement que l'on a $\sqrt{1+x} \leq 1 + \frac{1}{2}x$ pour $x \geq 0$. On remarque socondement que l'on peut écrire

$$\varepsilon = \left(\frac{\sqrt{\delta - 4A} + \sqrt{\delta}}{2A}\right)^N \left(\frac{\sqrt{\delta - 4A} + \sqrt{\delta}}{2} \pm 1\right).$$

On en déduit troisièmement la majoration

$$|\varepsilon| \leq \frac{|\delta|^{(N+1)/2}}{|A|^N} \left(1 + \frac{|A|}{|\delta|}\right)^N \left(1 + \frac{|A|}{|\delta|} + \frac{1}{\sqrt{|\delta|}}\right).$$

De plus, nous avons $|A|^{N-3} \leq \frac{1}{2}\sqrt{|\delta|}$ dès lors que l'on a $N \geq 7$ (remarquer que l'on a $|\delta| \geq (|A|^N - |A| - 1)^2 - 4|A| \geq 4|A|^{2N-6}$ pour $N \geq 7$ (car $|A| \geq \sqrt{2}$)). Nous pouvons donc appliquer le théorème 2 avec $n = N - 3$. Nous avons donc:

$$\frac{|\varepsilon|}{|\varepsilon_0|^2} \leq \frac{31^2}{4^{N-3}|\delta|^{(N-7)/2}|A|^N} \left(1 + \frac{|A|}{|\delta|}\right)^N \left(1 + \frac{|A|}{|\delta|} + \frac{1}{\sqrt{|\delta|}}\right)$$

$$\leq \frac{31^2}{2^{(N^2-3N-5)/2}} (1 + 2^{-(2N+1)/2})^N (1 + 2^{-(2N+1)/2} + 2^{-(N-1)/2}) < 1,$$

cette avant dernière majoration résultant de $|\delta| \geq 4|A|^{2N-6}$ et de $|A|^2 \geq 2$; cette dernière majoration résultant de $N \geq 7$.

Si $\mathbf{K}$ est principal et si A n'est pas irréductible, alors il existe un idéal primitif et principal $\mathbf{I}$ de norme relative A' telle que $2 \leq |A'|^2 \leq A$. Nous pouvons donc

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

appliquer le théorème 2 avec $n = 2N - 6$ et nous obtenons une contradiction des inégalités suivantes:

$$|\varepsilon_0| \geq \frac{1}{31} 2^{2N-6} |\delta|^{N-3} \geq 2 |\delta|^{(N+1)/2} > |\varepsilon| > 1. \qquad \square$$

Remarque. Il est clair que la contrainte $N \geq 7$ n'est pas optimale. Elle n'est choisie que pour obtenir une preuve rapide et point trop technique de ce corollaire.

3. Cas des corps cubiques non totalement réels

Si $\mathbf{K}$ est un corps cubique non totalement réel, le groupe des unités de son anneau des entiers algébriques est encore de rang 1, et qu'il est donc engendré par -1 et une unité fondamentale ε_0 unique telle que $\varepsilon_0 > 1$.

Un idéal entier $\mathbf{I}$ de $\mathbf{K}$ est dit *primitif* lorsque $n \in \mathbf{N}^*$ et (n) divise $\mathbf{I}$ impliquent $n = 1$. Un idéal primitif $\mathbf{I}$ est dit *réduit* si il vérifie

$$z \in \mathbf{I} \text{ et } z \neq 0 \text{ impliquent } \mathrm{Max}\,(|z|, |z'|) \geq L(\mathbf{I}),$$

où z, z' et $z'' = \bar{z}'$ sont les trois conjugués de z et où $L(\mathbf{I}) \in \mathbf{N}^*$ est un générateur de l'idéal $\mathbf{I} \cap \mathbf{Z}$. Notons que la norme d'un idéal $\mathbf{I}$ appartenant à cet idéal $\mathbf{I} \cap \mathbf{Z}$, alors $L(\mathbf{I})$ divise A (si nous notons A cette norme).

Soient $\mathbf{I}$ un idéal réduit et $L(\mathbf{I}) \in \mathbf{N}^*$ un générateur de $\mathbf{I} \cap \mathbf{Z}$. Nous définissons l'élément de conversion de $\mathbf{I}$, noté $h_0(\mathbf{I})$, comme étant le point extrémal adjacent à $L(\mathbf{I})$, de sorte qu'il est caractérisé par les propriétés suivantes:

$$\begin{aligned}
&h_0(\mathbf{I}) \in \mathbf{I},\\
&h_0(\mathbf{I}) > L(\mathbf{I}) \text{ et } |h_0'(\mathbf{I})| < L(\mathbf{I}),\\
&h \in \mathbf{I},\ h \neq 0 \text{ et } |h| < h_0(\mathbf{I}) \text{ impliquent } |h_0'(\mathbf{I})| \leq |h'|.
\end{aligned}$$

On montre que cet élément de conversion existe et est unique. Semblablement au cas des corps quadratiques réels, il n'existe qu'un nombre fini d'idéaux réduits, donc qu'un nombre fini d'idéaux réduits principaux et nous avons premièrement (voir [8]):

$$\varepsilon_0 = \prod_{\substack{\mathbf{I} \text{ réduit} \\ \text{et principal}}} \frac{h_0(\mathbf{I})}{L(\mathbf{I})}. \tag{7}$$

La détermination de l'ensemble des idéaux réduits principaux est en général extrêmement laborieuse. On pourra par exemple consulter [8] pour avoir une idée de

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

la compléxité de cette détermination dans le cas de familles de corps cubiques pour lesquelles ils ne sont pourtant qu'en petit nombre (indépendant du corps, ne dépendant que de la famille de corps considérée), par exemple pour la famille de corps cubiques purs $\mathbf{K} = \mathbf{Q}(\sqrt[3]{M^3 - M})$, $M \geq 2$. Notre approche se passe ici encore de la complète détermination de cet ensemble.

LEMME (c). *Soit* $\mathbf{K}$ *un corps cubique non totalement réel de discriminant* D.
(a) *Un ideal primitif tel que* $L(\mathbf{I}) \leq \sqrt[6]{|D|/36}$ *est réduit.*
(b) *Si* $\mathbf{I}$ *est réduit, alors*

$$\frac{h_0(\mathbf{I})}{L(\mathbf{I})} \geq \frac{\sqrt[4]{|D|/4}}{L(\mathbf{I})}\left(1 - \frac{L(\mathbf{I})}{\sqrt[4]{|D|/4}}\right).$$

Preuve. Prouvons premièrement le point (a). Si $\mathbf{I}$ n'est pas réduit, il existe x non nul de $\mathbf{I}$ tel que $|x| < L(\mathbf{I})$ et $|x'| = |x''| < L(\mathbf{I})$. Mais alors, x n'est pas un entier relatif, de sorte que le $\mathbf{Z}$-module $\mathbf{Z}[x]$ engendré pas 1, x et x^2 est de rang 3 et inclus dans l'anneau des entiers algébriques de $\mathbf{K}$ qui est lui-même un $\mathbf{Z}$-module libre de rang 3. Il est bien connu que le discriminant $D(1, x, x^2)$ du module $\mathbf{Z}[x]$ est égal à N^2D, où N est l'indice de $\mathbf{Z}[x]$ dans l'anneau des entiers de $\mathbf{K}$. Le premier résultat désiré découle de:

$$36L^6(\mathbf{I}) = (6L^3(\mathbf{I}))^2 \geq \begin{vmatrix} 1 & x & x^2 \\ 1 & x' & x'^2 \\ 1 & x'' & x''^2 \end{vmatrix}^2 = D(1, x, x^2) = N^2|D| \geq |D|.$$

Prouvons secondement le point (b). Nous remarquons que $x = \dfrac{h_0(\mathbf{I})}{L(\mathbf{I})}$ vérifie $x > 1$ et $|x'| = |x''| < L(\mathbf{I})$. Nous avons donc $|x' - x''| < 4$. Le résultat désiré découle donc de:

$$\begin{aligned} |D| \leq D(1, h_0(\mathbf{I}), h_0^2(\mathbf{I})) &= L^4(\mathbf{I})D(1, x, x^2) \\ &= L^4(\mathbf{I})((x - x')(x' - x'')(x'' - x))^2 \\ &\leq 4L^4(\mathbf{I})(x + 1)^4. \end{aligned}$$

□

Semblablement au théorème 1 et en remarquant que $\prod_{k \geq 0}\left(1 - \dfrac{1}{2^k\sqrt{3}}\right) \geq \dfrac{1}{5}$, mais en remarquant que puisque l'on ne dispose maintenant plus de la notion d'idéal conjugué le produit à considérer ne porte plus sur $2n + 1$ termes mais seulement sur $n + 1$ termes, nous en déduisons le résultat suivant (remarquer que l'on a $L(\mathbf{I}^k) \leq L^k(\mathbf{I})$):

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

THÉORÈME 3. *Soit* $\mathbf{K}$ *un corps cubique non totalement réel de discriminant* D. *Soit* $\mathbf{I}$ *un idéal primitif non nul de* $\mathbf{K}$ *de norme* $A \geq 2$ *première à* D. *Supposons de plus que* $\mathbf{I}$ *soit principal. Alors, pourvu que* n *vérifie* $\mathfrak{N}^n \leq \sqrt[6]{\frac{|D|}{36}}$, *l'unité fondamentale* $\varepsilon_0 > 1$ *de* $\mathbf{K}$ *vérifie:*

$$\varepsilon_0 > \frac{1}{5}\left(\frac{3|D|}{4}\right)^{\frac{n+1}{6}}.$$

COROLLAIRE (E). *Si* $\mathbf{K}$ *est le corps cubique non totalement réel* $\mathbf{Q}(\omega)$ *où* ω *est la racine du pôlynome* $f(X) = X^3 - c^m X^2 - (c-1)X - c^m$ *comprise dans l'intervalle ouvert* $c^m < \omega < c^m + 1$ *où* $c \geq 2$ *et* $m \geq 1$ *sont des entiers relatifs, alors* $\varepsilon = \omega\left(\frac{\omega}{\omega - c^m}\right)^m$ *est une unité de l'anneau* $\mathbf{Z}[\omega]$. *De plus, il existe une constante* $\mathbf{K}$ *indépendante de* c *et* m *telle que l'unité fondamentale* $\varepsilon_0 > 1$ *de* $\mathbf{K}$ *vérifie* $\varepsilon = \varepsilon_0^k$ *pour un* k *tel que* $1 \leq k \leq \mathbf{K}$, *dès lors que* $\mathbf{Z}[\omega]$ *est l'anneau des entiers de* $\mathbf{K}$.

Preuve. Nous avons:

$$\frac{1}{\varepsilon} = \frac{1}{\omega}\left(\frac{\omega - c^m}{\omega}\right)^m = \frac{1}{\omega}(c + c^m\omega - \omega^2)^m \quad \text{et} \quad \frac{c^m}{\omega} = \omega^2 - c^m\omega - (c-1) \in \mathbf{Z}[\omega].$$

Il en résulte que $1/\varepsilon$ est dans $\mathbf{Z}[\omega]$. Puisque $\omega = \frac{c^m\Omega}{\Omega - 1}$, alors $\Omega \overset{\text{def}}{=} \frac{\omega}{\omega - c^m}$ est racine de $g(X) = cX^3 - (cC+1)X^2 + (c+2)X - 1$, où $C \overset{\text{def}}{=} c^{2m-1} + 2$. Il en résulte premièrement que $1/\Omega^m$ est de norme c^m dans $\mathbf{K}$, ainsi que que ω. L'élément $1/\varepsilon$ est donc un entier algébrique de norme 1, donc ε appartient à $\mathbf{Z}[1/\varepsilon] \subseteq \mathbf{Z}[\omega]$, et ε est donc bien une unité de $\mathbf{Z}[\omega]$.

Puisque $g(C) \leq 0 \leq g(C+1)$, nous avons: $c^{2m-1} + 2 \leq \Omega \leq c^{2m-1} + 3$. D'où:

$$1 < \varepsilon = \omega\Omega^m \leq c^{2m^2}\left(1 + \frac{1}{c^m}\right)\left(1 + \frac{3}{c^{2m-1}}\right)^2 \leq \frac{15}{4}c^{2m^2}.$$

D'un autre côté, l'idéal principal $\mathbf{I} = \left(\frac{\omega - c^m}{\omega}\right)$ est entier et de norme c première au discriminant $D(f) = -4c^{4m} + (c^2 - 20c - 8)c^{2m} + 4(c-1)^2$ du pôlynome $f(X)$, donc première au discriminant D de $\mathbf{K}$. Nous remarquons que l'hypothèse $c \geq 2$ implique $|D(f)| = 4c^{4m} - (c^2 - 20c - 8)c^{2m} - 4(c-1)^2 \geq 4c^{4m} - c^2c^{2m} \geq 3c^{4m}$. Notons que $\mathbf{I} = (c + c^m\omega - \omega^2)$ est clairement primitif dès lors lors que $\mathbf{Z}[\omega]$ est l'anneau des entiers de $\mathbf{K}$. Nous choisissons $n \geq 0$ tel que $36c^{6n}$

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

$\leq 3c^{4m} < 36c^{6n+6}$. Le théorème 3 s'applique avec ce n, et nous avons donc:

$$(**) \qquad \varepsilon_0 > \frac{1}{5}\left(\frac{9c^{4m}}{4}\right)^{\frac{n+1}{6}} = \frac{1}{5}\left(\frac{3}{2}\right)^{\frac{n+1}{3}}\left(\frac{c^{4m}}{12}\right)^{\frac{m}{9}} \geq \frac{1}{5}\left(\frac{2}{3}\right)^{\frac{1}{9}}\left(\frac{3c^{4m}}{16}\right)^{\frac{m}{9}}$$

(la dernière inégalité résultant de $6n + 6 \geq 4m - 2$ pour $c \geq 2$.) D'où le résultat désiré d'après (*) et (**). □

Remarques. $\mathbf{Z}[\omega]$ est l'anneau des entiers algébriques de $\mathbf{K}$ dès lors que $D(f)$ est libre de facteur carré. Il est aisé de voir (numériquement) que cela a lieu pour certaines valeurs de m et c, et probablement pour chaque valeur de m cela a t-il lieu pour une infinité de valeurs de c.

De cette preuve, il résulte aisément que si m ou c est pris suffisamment grand, alors on peut prendre $K = 4$. Pour voir que ε est fondamentale, il resterait à voir qu'elle n'est ni un carré, ni un cube. Nous montrons maintenant que ε n'est pas un carré et répondons ainsi presque positivement á une question posée par C. Levesque et G. Rhin (voir paragraphe 3 de [5]). Par souci de concision, nous ne traitons que le cas où m est supposé pair. Pour m impair, il faudrait montrer que $\omega\left(\frac{\omega}{\omega - c^m}\right)$ n'est par un carré dans $\mathbf{Z}[\omega]$. Il est clair que nos techniques permettraient d'également considérer la famille de corps cubiqus envisagée par ces auteurs au paragraphe 2 de leur article.

LEMME (d). *Si $m = 2M$ est pair, alors ε est un carré dans $\mathbf{Z}[\omega]$ si et seulement si ω est un carré dans $\mathbf{Z}[\omega]$.*

Preuve. Si $\varepsilon = \beta^2$ avec $\beta \in \mathbf{Z}[\omega]$, alors

$$\left[\beta\left(\frac{\omega - c^m}{\omega}\right)^M\right]^2 = [\beta(c + c^m\omega - \omega^2)^M]^2 = \omega$$

de sorte que ω est un carré dans $\mathbf{Z}[\omega]$. Réciproquement, si $\omega = \gamma^2$ avec $\gamma \in \mathbf{Z}[\omega]$, alors

$$\frac{1}{\varepsilon} = \frac{1}{\omega}(c + c^m\omega - \omega^2)^M = \left[\frac{1}{\gamma}(c + c^m\gamma^2 - \gamma^4)^M\right]^2.$$

Puisque ω est de norme c^{2M}, on peut en changeant au besoin γ en $-\gamma$ supposer que γ est de norme c^M, de sorte que γ étant un entier algébrique, alors c^M/γ appartient à $\mathbf{Z}[\gamma]$. Il en résulte que $1/\varepsilon$ est un carré dans $\mathbf{Z}[\gamma]$, donc dans $\mathbf{Z}[\omega]$. □

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

PROPOSITION (A). *Soit $\omega > 0$ un entier algébrique de degré 3 sur $\mathbf{Q}$. Soit $\sqrt{\omega}$ la détermination strictement positive de cette racine carrée. Alors,*

(i) *$\sqrt{\omega}$ appartient à $\mathbf{Q}(\omega)$ si et seulement si le polynôme minimal $\Pi_\omega(X)$ de ω est de la forme $\Pi_\omega(X) = X^3 - (d^2 - 2e)X^2 + (e^2 - 2df)X - f^2$ avec $(d, e, f) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{N}^*$.*

(ii) *On a alors $\sqrt{\omega} = \dfrac{\omega^2 - (d^2 - e)\omega - df}{f - de}$, de sorte que $\sqrt{\omega}$ appartient à $\mathbf{Z}[\omega]$ si et seulement si $f - de = 1$ ou $f - de = -1$.*

Preuve. Si $\Pi_\omega(X) = X^3 - aX^2 + bX - c$, alors $\Pi_\omega(X^2)$ annule $\sqrt{\omega}$ et $-\sqrt{\omega}$, de sorte que $\Pi_{\sqrt{\omega}}(X)$ et $-\Pi_{\sqrt{\omega}}(-X)$ qui sont unitaires de degré 3 et distincts divisent $\Pi_\omega(X^2)$. Il en résulte que $\Pi_\omega(X^2) = -\Pi_{\sqrt{\omega}}(X)\Pi_{\sqrt{\omega}}(-X)$. D'où le premier résultat en définissant d, e, et f par $\Pi_{\sqrt{\omega}}(X) = X^3 - dX^2 + eX - f$. De plus, puisque $\sqrt{\omega}$ est strictement positif, nous avons $f > 0$. Puisque $\Pi_{\sqrt{\omega}}(\sqrt{\omega}) = \omega\sqrt{\omega} - d\omega + e\sqrt{\omega} - f = 0$, nous avons $\sqrt{\omega} = (d\omega + f)/(\omega + e)$. Le second résultat s'en déduit aisément. □

COROLLAIRE (F). *Soient $m \geq 4$ et $c \geq 2$ deux entiers. Soit ω la racine strictement positive du polynome $f(X) = X^3 - c^m X^2 - (c - 1)X - c^m$. Alors, ω n'est pas un carré dans $\mathbf{Z}[\omega]$.*

Preuve. Si ω était un carré dans $\mathbf{Z}[\omega]$, il existerait $(d, e, f) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{N}^*$ tel que:

$$\begin{aligned} &d^2 - 2e = c^m, \\ &2df - e^2 = c - 1, \\ &f^2 = c^m \text{ avec } f > 0, \\ &f = de \pm 1. \end{aligned}$$

Il faut et il suffit donc que $m = 2M$ soit pair et que l'on ait:

$$\begin{aligned} &(1)\ d^2 - 2e = c^{2M}, \\ &(2)\ 2c^M d - e^2 = c - 1, \\ &(3)\ de = c^M - \pm 1. \end{aligned}$$

Mais alors, en utilisant (3) la combinaison $d\cdot(2) - 2c^M\cdot(1)$ donne $(3c^M \pm 1)e = d(c - 1) - 2c^{3M}$, de sorte qu'en utilisant à nouveau (3) nous obtenons:

$$(3c^M \pm 1)e^2 + 2c^{3M}e - (c - 1)(c^M - \pm 1) = 0.$$

En conséquence, le discriminant réduit $\Delta = c^{6M} - (c - 1)(3c^{2M} - \pm 2c^M - 1)$

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press

de cette équation doit être un carré parfait dans $\mathbf{Z}$. Mais il est aisé de voir que l'on a $\Delta \neq c^{6M}$ et $(c^{3M}-1)^2 < \Delta < (c^{3M}+1)^2$, de sorte que l'on a le résultat désiré. □

CONCLUSION. Soit $A \geq 2$ donné. Nous venons de voir aux théorèmes 1,2 et 3 que lorsque $\mathbf{K}$ est un corps de nombres à groupe d'unites de rang 1, de valeur absolue de discriminant $d(\mathbf{K})$ et de régulateur $\mathrm{Reg}(\mathbf{K})$, alors nous avons des minorations du type $\mathrm{Reg}(\mathbf{K}) \geq c_A \log^2(d(\mathbf{K}))$ dès lors que $\mathbf{K}$ varie parmi des corps de discriminants premiers à A pour lesquels il existe un Idéal primitif principal de norme A. Il serait intéressant de savoir ci de tels amendements sont possibles lorsque le groupe des unités de $\mathbf{K}$ de degré n n'est plus supposé de rang r tel que $r=1$. Plus précisément, on sait que pour chaque $n \geq 1$ il existe une constant c_n ne dépendant que de n telle que l'on ait $\mathrm{Reg}(\mathbf{K}) \geq c_n \log^{r-r_0}(d(\mathbf{K}))$ où r_0 désigne le maximum des rangs des groupes des unités des sous-corps propres de $\mathbf{K}$ (voir par exemple E. Friedman, Analytic formulas for the regulator of a number field, Invent. math, 98 (1989), 599-622). Peut-on amender cet exposant (que nous avons donc amendé de 1 en 2 dans les trois cas que nous avons cnosidérés dans cet article) dés lors que l'on impose de plus à $\mathbf{K}$ de varier parmi des corps de discriminants premiers à A pour lesquels il existe un idéal primitif principal de norme A?

BIBLIOGRAPHIE

[1] H. Amara, Groupe des classes et unité fondamentale des extensions quadratiques relatives à un corps quadratique imaginaire principal, Pacific J. Math., **96** (1981), 1–12.

[2] T. Azuhata, On the fundamental units and the class numbers of real quadratic fields, Proc. Japan Acad., Sci. **62** (1986), 97–100.

[3] L. Bernstein, Fundamental unit and cycles in the period of real quadratic number fields, Pacific J. Math., **63** (1976), 37–78.

[4] E. Dubois and C. Levesque, On determining certain real quadratic fields with class number one and relating this property to continued fractions and primality properties, Nagoya Math. J., **124** (1991), 157–180.

[5] C. Levesque et G. Rhin, Two families of periodic Jacobi algorithms with period lengths going to infinity, J. Number Theory., **37** (1991), 173–180.

[6] S. Louboutin, Prime producing quadratic polynomials andclass-numbers of real quadratic fields, Canad. J. Math., **42** (1990), 315–341.

[7] H. C. Williams, Continued fractions and number-theoretic computations, Rocky Mountain J. Math., **15** (1985), 621–655.

[8] H. C. Williams, The period length of Voronoi's algorithm for certain cubic orders, Publicationes Math. Debrecen., **37** (1990), 245–265.

[9] Y. Yamamoto, Real quadratic number fields with large fundamental units, Osaka J. Math., **8** (1971), 261–270.

Université de Caen, U. F. R. Sciences
Département de Mathématiques
Esplanade de la Paix
14032 Caen Cedex, FRANCE.

email: loubouti @ univ-caen. fr

https://doi.org/10.1017/S0027763000004396 Published online by Cambridge University Press