JOURNAL OF NUMBER THEORY 42, 361–368 (1992)

Norme relative de l'unité fondamentale de certains corps biquadratiques et parité des longueurs de cycles d'idéaux réduits

STÉPHANE LOUBOUTIN

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

Communicated by M. Pohst

Received October 31, 1990

Soit $\mathbf{k}=\mathbf{Q}(\sqrt{d})$ ($d>0$ libre de carrés) un corps quadratique réel de discriminant $D>0$ ayant t facteurs premiers distincts. Il est bien connu que le sous groupe du groupe des classes engendré par les t idéaux premiers ramifiés dans $\mathbf{k}/\mathbf{Q}$ est d'ordre 2^{t-1} lorque l'unité fondamentale est de norme -1, et d'ordre 2^{t-2} lorsqu'elle est de norme $+1$. Puisque (1) et $(\sqrt{d})$ sont principaux, il n'existe pas d'autre relation de principalité entre ces idéaux premiers ramifiés lorsque l'unité fondamentale est de norme -1, et il en existe précisément deux autres non triviales (duales l'une de l'autre) lorsqu'elle est de norme $+1$. Si ω_0 désigne le générateur habituel de l'anneau des entiers de $\mathbf{k}$, alors l'unité fondamentale est de norme -1 si le développement en fractions continues de ω_0 est de longueur de période primitive impaire, et de norme $+1$ si il est de longueur de période primitive paire. De plus, dans ce dernier cas les deux relations de principalité non triviales entre les idéaux premiers ramifiés sont bien déterminées par le terme médiant de ce développement (voir [5], [6]). Nous prolongeons ces résultats dans le cas de certains corps biquadratiques totalement imaginaires (donc de rang du groupe d'unités égal à 1) contenant un sous corps quadratique (de sorte que l'on puisse parler de la norme relative de cette unité fondamentale, sa norme absolue valant elle toujours $+1$), corps quadratique supposé imaginaire principal. Nous nous demandons si la parité des longueurs de cycles d'idéaux réduits (notion prolongeant celle de fractions continues puisque coïncidant avec elle dans le cas des corps quadratiques réels) donne la norme relative de l'unité fondamentale de ces extensions. Nous verrons qu'une obstruction se présente, et indiquerons quelles propriétés devrait satisfaire une nouvelle notion de cycle d'idéaux réduits pour lever cette obstruction.

Let $\mathbf{K}/\mathbf{k}$ be a quadratic extension of a principal imaginary quadratic field $\mathbf{k}$. We show that the theory of cycles of reduced ideals as developed by *H.* Amara provides us with an algorithm to test the relative norm $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})$ of the fundamental unit of $\mathbf{K}$. We then show that the well known result connecting the norm of the fundamental unit of a real quadratic field with the parity of the period length of the continued fractional expansion of $\sqrt{D}$ does not generalize.

0022-314X/92 $5.00

Dans toute la suite, $\mathbf{K}/\mathbf{k}$ désigne une extension quadratique d'un des 9 corps quadratiques imaginaires principaux $\mathbf{k}$ telle que $\mathbf{K}/\mathbf{Q}$ ne soit pas galoisienne.

La notion d'*idéal réduit* et de *cycles d'idéaux réduits* que nous adoptons est celle développée dans ce cadre par H. Amara [1]. Nous notons $\mathbf{R}_\mathbf{K}$ l'anneau des entiers de $\mathbf{K}$, $\mathbf{R}_\mathbf{k}$ celui de $\mathbf{k}$, $\delta_{\mathbf{K}/\mathbf{k}}$ le discriminant relatif de $\mathbf{K}/\mathbf{k}$, t son nombre de facteurs premiers dans $\mathbf{R}_\mathbf{k}$, τ le $\mathbf{k}$-isomorphisme non trivial de $\mathbf{K}$ et $\eta_\mathbf{K}$ l'unité fondamentale de $\mathbf{K}$ (qui étant totalement complexe et de degré 4 est de rang du groupe des unité valant 1).

Nous appelons *invariant* un idéal $\mathbf{I}$ de $\mathbf{R}_\mathbf{K}$ tel que $\mathbf{I}^\tau = \mathbf{I}$. Un tel idéal est de la forme $\mathbf{I} = (\alpha)\mathbf{R}$ avec $\alpha \in \mathbf{R}_\mathbf{k}$ et $\mathbf{R}$ un idéal de $\mathbf{K}$ produit d'idéaux premiers ramifiés deux à deux distincts. Nous appelons *primitif* un idéal $\mathbf{I}$ de $\mathbf{R}_\mathbf{K}$ tel que $n \in \mathbf{R}_\mathbf{k}$ et (n) divise $\mathbf{I}$ impliquent n est une racine de l'unité de $\mathbf{k}$. Toute classe d'idéaux contient un idéal primitif et les idéaux réduits sont primitifs. Un *idéal ramifié* est alors un idéal invariant primitif, i.e., un produit d'idéaux premiers ramifiés dans $\mathbf{K}/\mathbf{k}$ deux à deux distincts. Nous appelons *classe régulière* une classe contenant un idéal invariant, et *classe ambige* une classe invariante sous l'action de τ, i.e., une classe d'ordre 2 (car $\mathbf{k}$ est principal).

Remarquons qu'après multiplication éventuelle par une unité de $\mathbf{k}$, on peut supposer $\eta_\mathbf{K}$ de norme relative $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K})$ valant $+1$ ou -1 pour $\mathbf{k} \neq \mathbf{Q}(i)$, et de norme relative valant $+1$ ou i pour $\mathbf{k} = \mathbf{Q}(i)$. Semblablement au cas quadratique réel, les t idéaux premiers de $\mathbf{K}$ ramifiés dans $\mathbf{K}/\mathbf{k}$ engendrent le sous groupe des classes régulières, sous groupe d'ordre 2^{t-2} ou 2^{t-1} suivant que $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K}) = +1$ ou $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K}) \neq +1$ (voir [7]). Autrement dit, les seuls idéaux ramifiés principaux sont $\mathbf{R}_\mathbf{K}$ et $(\sqrt{d})$ pour $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K}) \neq +1$ (où $d \in \mathbf{R}_\mathbf{k}$ est libre de carrés dans $\mathbf{R}_\mathbf{k}$ et tel que $\mathbf{K} = \mathbf{k}(\sqrt{d})$), alors qu'il en existe encore précisément deux autres duaux l'un de l'autre lorsque $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K}) = +1$.

Nos démonstrations reposent essentiellement sur le fait que τ agit très simplement sur les cycles d'idéaux réduits. Notons sans démonstration que si $\mathbf{K}/\mathbf{Q}$ est galoisienne, il n'est nul besoin de supposer de surcroît le corps quadratique imaginaire $\mathbf{k}$ principal: on ramène la détermination de la norme relative de l'unité fondamentale de $\mathbf{K}$ à celle de la norme de l'unité fondamentale de son unique sous corps quadratiques réel (voir [7]).

LEMME 1. *Si* $\mathbf{I}$ *est un idéal réduit de successeur* $\mathbf{I}_1$, *alors* $h_0((\mathbf{I}_1)^\tau) = h_0(\mathbf{I})$.

Preuve. $h_0((\mathbf{I}_1)^\tau)$ est caractérisé par:

$h_0((\mathbf{I}_1)^\tau) \in (\mathbf{I}_1)^\tau$, $|h_0((\mathbf{I}_1)^\tau)| < |N_{\mathbf{K}/\mathbf{k}}((\mathbf{I}_1)^\tau)|$

$h \in (\mathbf{I}_1)^\tau$ et $|h| < |N_{\mathbf{K}/\mathbf{k}}((\mathbf{I}_1)^\tau)|$ impliquent $|h^\tau| \geqslant |h_0^\tau((\mathbf{I}_1)^\tau)|$.

$h_0(\mathbf{I})$ est lui caractérisé par:

$h_0(\mathbf{I}_1) \in \mathbf{I}$, $|h_0(\mathbf{I})| < |N_{\mathbf{K}/\mathbf{k}}(\mathbf{I})|$

$h \in \mathbf{I}$ et $|h| < |N_{\mathbf{K}/\mathbf{k}}(\mathbf{I})|$ impliquent $|h^\tau| \geqslant |h_0^\tau(\mathbf{I})|$.

Nous montrons que $h_0(\mathbf{I})$ satisfait aux propriétés caractérisant $h_0((\mathbf{I}_1)^\tau)$, ce qui nous donnera le résultat. En effet, nous avons successivement:

(a) $\mathbf{I}_1 = (h_0^\tau(\mathbf{I})/N(\mathbf{I}))\mathbf{I}$, donc $\mathbf{I}_1\mathbf{I}^\tau = (h_0^\tau)$, et conséquemment $h_0 \in (\mathbf{I}_1)^\tau$.

(b) $|N_{\mathbf{K}/\mathbf{k}}(\mathbf{I}_1)| = |h_0 h_0^\tau|/|N(\mathbf{I})|$ implique $|h_0| = (|N(\mathbf{I})|/|h_0^\tau|)\,|N_{\mathbf{K}/\mathbf{k}}(\mathbf{I}_1)| < |N_{\mathbf{K}/\mathbf{k}}(\mathbf{I}_1)|$.

(c) Si $h = (h_0/|N(\mathbf{I})|)H^\tau$ appartient à $(\mathbf{I}_1)^\tau$, i.e. si H appartient à $\mathbf{I}$, et si nous avons $|h| < |N_{\mathbf{K}/\mathbf{k}}((\mathbf{I}_1)^\tau)|$, i.e. si nous avons $|H^\tau| < |h_0^\tau|$, alors nous en déduisons $|H| \geqslant |N_{\mathbf{K}/\mathbf{k}}(\mathbf{I})|$, ce qui implique $|h^\tau| \geqslant |h_0^\tau|$. ∎

Si $\{\mathbf{I}_i;\ 0 \leqslant i \leqslant L-1\}$ est un cycle d'idéaux réduits de longueur L, semblablement à [6], pour $i \in \mathbf{Z}$ nous posons $\mathbf{I}_i = \mathbf{I}_{i'}$ où i' est l'unique entier vérifiant $0 \leqslant i' \leqslant L-1$ et $i' \equiv i \pmod{L}$.

COROLLAIRE 2. *$(\mathbf{I}_i)^\tau = (\mathbf{I}^\tau)_{-i}$ pour $\mathbf{I}$ un idéal réduit.*

Conséquemment, si $\mathbf{I} = \mathbf{I}_0$ est réduit et invariant et de cycle d'idéaux réduits de longueur $L = 2k$ paire, alors $\mathbf{I}_k$ est réduit et invariant.

Tout cycle d'idéaux réduits de longueur impaire correspondant à une classe ambige contient (exactement) un idéal réduit invariant.

Preuve. Nous prouvons le premier point par récurrence sur i. Seul le premier cran $i = 1$ pose problème. Il nous faut donc voir que $(\mathbf{I}_1)^\tau = (\mathbf{I}^\tau)_{-1}$, i.e. que $((\mathbf{I}_1)^\tau)_1 = \mathbf{I}^\tau$. Mais $((\mathbf{I}_1)^\tau)_1 = (h_0^\tau((\mathbf{I}_1)^\tau)/N((\mathbf{I}_1)^\tau))(\mathbf{I}_1)^\tau$, de sorte que d'après le lemme 1 nous avons $((\mathbf{I}_1)^\tau)_1 = (h_0^\tau(\mathbf{I})/N(\mathbf{I}_1)(\mathbf{I}_1)^\tau$. Puisque $\mathbf{I}_1 = (h_0^\tau(\mathbf{I})/N(\mathbf{I}))\mathbf{I}$ et que donc $(h_0(\mathbf{I})\,h_0^\tau(\mathbf{I})) = (N(\mathbf{I}_1)\,N(\mathbf{I}))$ (prendre les normes relatives dans l'égalité précédente), nous obtenons le résultat. La preuve des autres points suit celle donnée dans [6, Proposition 7]. ∎

PROPOSITION 3. *Si un cycle d'idéaux réduits contenant un idéal réduit invariant est de longueur paire, alors $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}}) = +1$.*

Si le cycle d'idéaux réduits d'un idéal réduit invariant est de longueur $L = 2k+1$ impaire, alors la norme relative $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})$ de l'unité fondamentale de $\mathbf{K}$ est bient déterminée par le k-ième idéal réduit de ce cycle.

Preuve. Soit $L = 2k$ la longueur paire d'un cycle d'idéaux réduits contenant un idéal invariant $\mathbf{I}$ que l'on peut supposer être le premier idéal $\mathbf{I}_0$ de ce cycle. Puisque $(\mathbf{I}_0)^\tau = \mathbf{I}_0$, nous avons $(\mathbf{I}_i)^\tau = (\mathbf{I}^\tau)_{-i} = \mathbf{I}_{-i}$. D'où

$N(\mathbf{I}_i)=N(\mathbf{I}_{-i})$, ainsi que $h_0(\mathbf{I}_{i-1})=h_0((\mathbf{I}_i)^\tau)=h_0(\mathbf{I}_{-i})$, la première égalité résultant du lemme 1. Nous avons donc:

$$\eta_{\mathbf{K}}=\prod_{i=0}^{L-1}\frac{h_0(\mathbf{I}_i)}{N(\mathbf{I}_i)}=\prod_{i=0}^{k-1}\frac{h_0(\mathbf{I}_i)\,h_0(\mathbf{I}_{L-i-1})}{N(\mathbf{I}_i)\,N(\mathbf{I}_{L-i-1})}=\left(\frac{\prod_{i=0}^{k-1}h_0(\mathbf{I}_i)}{\prod_{i=0}^{k-1}N(\mathbf{I}_i)}\right)^2\frac{N(\mathbf{I}_0)}{N(\mathbf{I}_k)}. \quad (*)$$

Mais alors, $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})=y^2$ pour un y dans $\mathbf{k}$, entier sur $\mathbf{Z}$, donc pour y un entier de $\mathbf{k}$. Mais y^2 étant une unité de $\mathbf{k}$, il en est de même de y. Il en résulte que $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})$ est le carré d'une racine de l'unité de $\mathbf{k}$, donc vaut $+1$.

Soit $L=2k+1$ la longueur impaire d'un cycle d'idéaux réduits d'un idéal invariant $\mathbf{I}$ que nous supposons donc être le premier idéal $\mathbf{I}_0$ de ce cycle. Nous avons de même:

$$\eta_{\mathbf{K}}=\left(\frac{\prod_{i=0}^{k-1}h_0(\mathbf{I}_i)}{\prod_{i=0}^{k-1}N(\mathbf{I}_i)}\right)^2\frac{N(\mathbf{I}_0)}{N(\mathbf{I}_k)}h_0(\mathbf{I}_k). \quad (**)$$

De plus, $\mathbf{J}=\mathbf{I}_k$ est un idéal réduit tel que $\mathbf{J}^2=(h_0(\mathbf{J}))$. En effet, $\mathbf{I}_{k+1}=(h_0^\tau(\mathbf{I}_k)/N(\mathbf{I}_k))\mathbf{I}_k$ et $(\mathbf{I}_{k+1})^\tau=\mathbf{I}_{-k-1}=\mathbf{I}_{2k+1-k-1}=\mathbf{I}_k$. Donc $\mathbf{I}_k=(h_0(\mathbf{I}_k)/N(\mathbf{I}_k))\mathbf{I}_k^\tau$. On en déduit notre affirmation en utilisant $(N(\mathbf{I}_k))=\mathbf{I}_k\mathbf{I}_k^\tau$. En particulier, $N_{\mathbf{K}/\mathbf{k}}(h_0(\mathbf{J}))/(N(\mathbf{J}))^2=\varepsilon$ est une racine de l'unité de $\mathbf{k}$ et, comme précédemment, nous avons $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})=\varepsilon$ à multiplication par le carré d'une racine de l'unité de $\mathbf{k}$ près. ∎

Remarque. Voir [9] pour un rappel de relations analogues à (*) et (**) dans le cas des corps quadratiques réels.

Soit $\mathbf{I}=\mathbf{I}_0$ un idéal réduit invariant. Montrons maintenant que, semblablement au cas des corps quadratiques réels pour l'algorithme des fractions continues ordinaire, ou pour celui des meilleures approximations (voir [8, 9]), il existe un test permettant de trouver lorsque la demi-période du cycle d'idéaux réduits de $\mathbf{I}$ est atteinte, divisant ainsi d'après (*) et (**) par deux les temps de calcul (numérique) de la longueur de ces cycles d'idéaux réduits, de l'unité fondamentale de $\mathbf{K}$, et du régulateur de $\mathbf{K}$.

PROPOSITION 4. *Soient* $(\mathbf{I}_i)_{0\leqslant i\leqslant L-1}$ *les* L *idéaux réduits d'un cycle d'idéaux réduits d'un idéal réduit invariant* $\mathbf{I}_0$ (*dans la pratique on choisit* $\mathbf{I}_0=\mathbf{R}_{\mathbf{K}}$), *et soit* k *tel que* $1\leqslant k\leqslant L-1$.

(a) *Si* $N(\mathbf{I}_k)$ *divise* $\delta_{\mathbf{K}/\mathbf{k}}$ *dans* $\mathbf{R}_{\mathbf{k}}$, *alors* $L=2k$;

(b) *si* $N(\mathbf{I}_{k+1})=\varepsilon N(\mathbf{I}_k)$ *avec* ε *une racine de l'unité de* $\mathbf{k}$, *alors* $L=2k+1$.

Conséquemment, pour déterminer la norme relative de l'unité fondamentale $\eta_{\mathbf{K}}$ *de* $\mathbf{K}$ (*ainsi que son régulateur*), *il suffit de calculer le cycle d'idéaux réduits de* $\mathbf{R}_{\mathbf{K}}$: *à chaque* k-*ième étape*, $k\geqslant 1$,

on teste si $N(\mathbf{I}_k)$ *divise* $\delta_{\mathbf{K}/\mathbf{k}}$, *auquel cas* $L=2k$, $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})=+1$ *et* $\mathbf{I}_k$ *et son idéal dual sont les deux idéaux ramifiés principaux non triviaux,*

sinon, on teste si $N(\mathbf{I}_{k+1})=\varepsilon N(\mathbf{I}_k)$ *pour* ε *une racine de l'unité de* $\mathbf{k}$, *auquel cas* $L=2k+1$ *et* $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})=N_{\mathbf{K}/\mathbf{k}}(h_0(\mathbf{I}_k))/(N_{\mathbf{K}/\mathbf{k}}(\mathbf{I}_k))^2$, *au carré d'une racine de l'unité de* $\mathbf{k}$ *près.*

Preuve. Remarquons préalablement que lorsque $\mathbf{I}$ est réduit son élément de conversion $h_0(\mathbf{I})$ est primitif, i.e. l'idéal $(h_0(\mathbf{I}))$ est primitif.

Lorsqu'il existe k (choisi le plus petit tel que) répondant au (a), l'idéal $\mathbf{I}_k$ est invariant. D'où $\mathbf{I}_k=(\mathbf{I}_k)^\tau=\mathbf{I}_{-k}$ et $\mathbf{I}_{2k}=\mathbf{I}$ et L divise $2k$. Puisque $1\leqslant k<L$, nous avons $L=2k$.

Lorsqu'il existe k (choisi le plus petit tel que) répondant au (b), $\mathbf{I}_{k+1}=(h_0^\tau(\mathbf{I}_k)/N(\mathbf{I}_k))\mathbf{I}_k$ donne $N_{\mathbf{K}/\mathbf{k}}(h_0(\mathbf{I}_k))=\varepsilon'(N_{\mathbf{K}/\mathbf{k}}(\mathbf{I}_k))^2$ pour ε' une racine de l'unité de $\mathbf{k}$. Puisque $h_0(\mathbf{I}_k)$ est primitif et dans $\mathbf{I}_k$ il en résulte que $(h_0(\mathbf{I}_k))=(\mathbf{I}_k)^2$. D'où $\mathbf{I}_{k+1}=(\mathbf{I}_k)^\tau=\mathbf{I}_{-k}$, et $\mathbf{I}_{2k+1}=\mathbf{I}$. D'où $L=2k+1$. ∎

Montrons finalement que les résultats du cas des corps quadratiques réels ne se prolongent pas au cas de ces extensions quadratiques d'un corps quadratique imaginaire principal: il peut arriver qu'un idéal ramifié ne soit pas réduit et que son *idéal dual* (voir [6] pour cette définition) ne le soit pas non plus, comme en atteste la proposition suivante appliquée au cas: $d=-63+28i=7(-9+4i)$, pour lequel $z=((-9+4i)/7)^{1/2}=((\sqrt{9\,7}-9)/14)^{1/2}+i((\sqrt{9\,7}+9)/14)^{1/2}$.

PROPOSITION 5. *Soient* $d\in\mathbf{R}_\mathbf{k}$, $d\equiv 1 \pmod 4$ *libre de carrés dans cet anneau principal et* $\mathbf{K}=\mathbf{k}(\sqrt{d})$. *Soit* $d=\delta_1\,\delta_2$ *une factorisation de d dans* $\mathbf{R}_\mathbf{k}$ *telle que* $(\delta_1)^2\equiv 1 \pmod 4$. *Soient* $\mathbf{I}$ *l'idéal ramifié de* $\mathbf{K}$ *de norme relative* δ_1 *et* $\mathbf{J}$ *l'idéal dual de* $\mathbf{I}$, *i.e. l'idéal ramifié de norme* δ_2. *Pour que ni* $\mathbf{I}$ *ni* $\mathbf{J}$ *ne soit réduit il faut et il suffit que* $z=\sqrt{\delta_2/\delta_1}$ *ou* $1/z$ *vérifie:* $|z|>1$, $|z-1|<2$ *et* $|z+1|<2$.

Preuve. $\mathbf{I}=(\delta_1,(\delta_1+\sqrt{d})/2)_{\mathbf{R}_\mathbf{k}}$, de sorte que $\mathbf{I}$ n'est pas réduit si et seulement si il existe m et n de $\mathbf{R}_\mathbf{k}$ non tous deux simultanément nuls tels que $|2m+n+nz|<2$ et $|2m+n-nz|<2$. D'où $(1/2)(|2m+n+nz|^2+|2m+n-z|^2)=|2m+n|^2+|nz|^2<4$. De même, $\mathbf{J}$ n'est pas réduit si et seulement si il existe m' et n' de $\mathbf{R}_\mathbf{k}$ non tous deux simultanément nuls tels que $|2m'+n'+n'(1/z)|<2$ et $|2m'+n'-n'(1/z)|<2$. D'où $|2m'+n'|^2+|n'(1/z)|^2<4$.

Supposons par exemple que nous avons $|z|>1$. Nous avons alors $|2m+n|^2+|n|^2<4$ et ces carrés de modules étant des normes d'éléments de $\mathbf{R}_\mathbf{k}$, ce sont des entiers. Conséquemment, $|n|^2=0$, 1, 2 ou 3.

Si $|n|^2=3$, alors $|2m+n|^2<1$, donc $2m+n=0$. Mais alors, $n=-2m$ et $|n|^2=4\,|m|^2$ ne saurait être égal à 3.

Si $|n|^2=2$, alors $|2m+n|^2<2$, donc $2m+n=0$ ou $|2m+n|^2=1$. Cette

première occurence ne saurait encore se produire, non plus que la seconde qui s'écrivant $4|m|^2+|n|^2+2Tr_{\mathbf{k}/\mathbf{Q}}(m\bar{n})=1$ conduirait pour des questions de parité à une contradiction.

D'où $|n|^2=1$ et n est une unité de $\mathbf{k}$. On peut donc supposer que $n=1$. Nous avons alors $|2m+1|^2<3$, et pour des raisons de parité, la seule possibilité est $|2m+1|^2=1$. Puisque $\mathrm{Re}(2m)=2\,\mathrm{Trace}_{\mathbf{k}/\mathbf{Q}}(m)$ appartient à $2\mathbf{Z}$, un dessin donne aisément $m=0$. D'où la condition nécessaire. Elle est suffisante puisqu'il suffit alors de prendre $(m', n')=(2, -1)$. ∎

Cette proposition 5 est une circonstance dirimante à une preuve de la formule du 2-rang du groupe des classes de ces corps biquadratiques par simple adaptation de celle que nous donnions ailleurs pour le cas des corps quadratiques réels (voir [6]). Plus fâcheuse, en est la conséquence que les cycles d'idéaux réduits n'ont pas nécessairement même parité de longueur, même en se restreignant au cas des cycles représentant des classes invariantes.

En effet, dans la situation de cette proposition 5, avec de plus $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})\neq+1$, le cycle d'idéaux réduits de l'idéal réduit $\mathbf{R}_{\mathbf{K}}$ est de longueur impaire (proposition 3), alors que le cycle d'idéaux réduits représentant la classe de l'idéal $\mathbf{I}$ est de longueur paire (il ne contient pas $\mathbf{I}$ qui n'est pas réduit et cela ne contredit donc pas la proposition 3). En effet, si il était de longueur impaire, il contiendrait d'après le corollaire 2 un idéal réduit invariant équivalent à $\mathbf{I}$. Mais $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})$ ne valant pas $+1$, il n'y a que les 2 relations de principalité triviales entre les idéaux premiers ramifiés dans $\mathbf{K}/\mathbf{k}$, i.e. les seuls idéaux ramifiés principaux sont $\mathbf{R}_{\mathbf{K}}$ et $(\sqrt{d})$, où $\mathbf{K}=\mathbf{k}(\sqrt{d})$ avec $d\in\mathbf{R}_{\mathbf{K}}$ libre de carrés dans cet anneau principal. Il en résulte que seul $\mathbf{I}$ et son idéal dual $\mathbf{J}$ sont invariants, primitifs et dans la classe de $\mathbf{I}$. Mais $\mathbf{J}$ n'étant pas réduit, cette contradiction nous donne le résultat.

Par exemple, pour $d=-63+28i=7(-9+4i)$ le cycle d'idéaux réduits de $\mathbf{R}_{\mathbf{K}}$ est de longueur 5 et celui de l'idéal premier ramifié $\mathbf{P}_7$ de norme relative 7 est de longueur 6.

Dans l'esprit de cette remarque, nous avons le résultat suivant plus faible que la proposition 3:

PROPOSITION 6. *Si le cycle d'idéaux réduits de* $\mathbf{R}_{\mathbf{K}}$ *est de longueur paire, alors* $N_{\mathbf{K}/\mathbf{k}}(\eta_{\mathbf{K}})=+1$.

Preuve. Sinon, contenant déjà un idéal invariant, il en contiendrait un second qui ne saurait être que $(\sqrt{d})$. Ce dernier idéal n'étant pas réduit, nous avons le résultat. ($z=\sqrt{d}$ appartient à $\mathbf{I}=(\sqrt{d})$ et vérifie $|z|=|z^\tau|<|N_{\mathbf{K}/\mathbf{k}}(\mathbf{I})|$ sauf pour $|d|^2=1$. Mais alors $\mathbf{K}/\mathbf{Q}$ est galoisienne.) ∎

Cette proposition 5 nous permet également de clairement comprendre pourquoi la simple parité ou imparité de la longueur du cycle d'idéaux

réduits de $\mathbf{R}_\mathbf{K}$ ne saurait donner la norme relative de l'unité fondamentale de $\mathbf{K}$. En effet, nous avons:

PROPOSITION 7. *Si* $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K}) = +1$ *et si* $\mathbf{R}_\mathbf{K}$, $(\sqrt{d})$, $\mathbf{I}$ *et son idéal dual* $\mathbf{J}$ *sont les quatre idéaux ramifiés principaux de* $\mathbf{K}$, *alors* $\mathbf{I}$ *ou* $\mathbf{J}$ *est réduit si et seulement si le cycle des idéaux réduits de* $\mathbf{R}_\mathbf{K}$ *est de longueur paire.*

Preuve. Puisque ce cycle contient $\mathbf{I}_0 = \mathbf{R}_\mathbf{K}$ qui est invariant, il est de longueur paire si et seulement si il contient un second idéal réduit invariant principal (voir [6, Proposition 7]). Puisque $(\sqrt{d})$ n'est pas réduit, nous avons le résultat. ∎

COROLLAIRE 8. *Soit* $\mathbf{K} = \mathbf{k}(\sqrt{d})$ *tel que* $\delta_{\mathbf{K}/\mathbf{k}} = d = \pi_1\pi_2 \equiv 1 \pmod 4$ *avec* π_1 *et* π_2 *irréductibles distincts de* $\mathbf{R}_\mathbf{k}$ *tels que* $\pi_1^2 \equiv 1 \pmod 4$.

Si (π_1) *ou* (π_2) *est réduit (et la proposition* 5 *teste cette occurence), alors* $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K}) = +1$ *si et seulement si le cycle des idéaux réduits de* $\mathbf{R}_\mathbf{K}$ *est de longueur paire.*

Si ni (π_1) *ni* (π_2) *n'est réduit, alors le cycle des idéaux réduits de* $\mathbf{R}_\mathbf{K}$ *est de longueur impaire, et sa parité ne saurait donc déterminer* $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K})$.

EXEMPLE. Pour $\mathbf{k} = \mathbf{Q}(i)$ et $d = (1 - 2i)(-3 + 2i) = 1 + 8i$, $z = \sqrt{(-3+i)/(1-2i)}$ vérifie $|z \pm 1| < 2$. Nous nous attendons donc à ce que le cycle des idéaux réduits de $\mathbf{R}_\mathbf{K}$ soit de longueur impaire. Effectivement, un calcul numérique montre qu'il est de longueur 3.

QUESTIONS OUVERTES

Lorsque $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K}) = +1$ et lorsque le cycle des idéaux réduits de $\mathbf{R}_\mathbf{K}$ est de longueur $L = 2k$ paire, une des relations de principalité non triviale entre les idéaux premiers ramifiés dans $\mathbf{K}/\mathbf{k}$ est $\mathbf{I}_k = (\alpha)$, l'autre étant la duale de celle-ci. Lorsque $N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K}) = +1$ et lorsque le cycle des idéaux réduits de $\mathbf{R}_\mathbf{K}$ est de longueur impaire, est-il posible de déterminer une des deux relations de principalité non triviales entre les idéaux premiers de $\mathbf{K}$ ramifiés dans $\mathbf{K}/\mathbf{k}$ par simple considération du cycle de $\mathbf{R}_\mathbf{K}$?

D'après la proposition 7, il est clair que la seule obstruction à l'équivalence

> "$N_{\mathbf{K}/\mathbf{k}}(\eta_\mathbf{K}) = +1$ si et seulement si le cycle des idéaux réduits de $\mathbf{R}_\mathbf{K}$ est de longueur paire",

ainsi qu'au fait que la seule considération du cycle d'idéaux réduits de $\mathbf{R}_\mathbf{K}$ donne toutes les relations de principalité entre les idéaux premiers ramifiés

dans $\mathbf{K}/\mathbf{k}$ est le fait qu'un idéal ramifié et son idéal dual peuvent n'être ni l'un ni l'autre réduits.

Il serait donc particulièrement satisfaisant d'amender la définition de la réduction d'un idéal de telle sorte que la répartition en cycles et l'action remarquable de τ sur ces cycles soient conservées, mais que maintenant un idéal ramifié ou son idéal dual soit réduit. Notons que dans notre cadre, la réduction d'un idéal au sens de J. Buchmann [2, 3] impliquant sa réduction au sens de H. Amara, cette réduction au sens de J. Buchmann (définie pour tout corps de nombres) est également inadéquate pour lever notre obstruction.

BIBLIOGRAPHIE

1. H. AMARA, Groupe des classes et unité fondamentale des extensions quadratiques relatives d'un corps quadratique imaginaire principal, *Pacific J. Math.* **96** (1981), 1–12.
2. J. BUCHMANN, On the computation of units and class numbers by a generalization of Lagrange's algorithm, *J. Number Theory* **26** (1987), 8–30.
3. J. BUCHMANN, The computation of the fundamental unit of totally complex quartic orders, *Math. Comp.* **48** (1987), 39–54.
4. J. C. LAGARIAS, On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$, *Trans. Amer. Math. Soc.* **260** (1980), 485–508.
5. S. LOUBOUTIN, Continued fractions and real quadratic fields, *J. Number Theory* **30** (1988), 167–176.
6. S. LOUBOUTIN, Groupe des classes d'idéaux triviaux, *Acta Arith.* **54** (1989), 61–74.
7. S. LOUBOUTIN, Norme relative de l'unité fondamentale et 2-rang du groupe des classes d'idéaux de certains corps biquadratiques, *Acta Arith.* **58** (1991), 273–288.
8. H. C. WILLIAMS, Some results concerning the nearest integer continued fraction expansion of $\sqrt{D}$, *J. Reine Angew. Math.* **315** (1980), 1–15.
9. H. C. WILLIAMS AND J. BROERE, A computational technique for evaluating $L(1, \chi)$ and the class number of real quadratic fields, *Math. Comp.* **30** (1976), 887–893.