ACTA ARITHMETICA
LIV (1989)

Groupes des classes d'idéaux triviaux

par

STÉPHANE LOUBOUTIN (Paris)

à Jacqueline G.

Introduction et notations. Nous prolongeons ici les méthodes développées par S. Louboutin [7] en non plus une caractérisation de la principalité d'un corps quadratique réel, mais en une caractérisation de la trivialité de son groupe des classes d'idéaux, où nous appelons trivial un groupe des classes $\mathcal{H}$ réduit à son 2-sous-groupe $\mathcal{A}$ des classes ambiges (classes d'ordre 2).

Nous reprenons les notations de [7]: d désigne un entier libre de carrés supérieur ou égal à 2, D le discriminant du corps quadratique réel $\boldsymbol{Q}(\sqrt{d})$, $\mathcal{H}$ son groupe des classes d'idéaux, $\mathcal{A}$ son 2-sous-groupe des classes ambiges, $\mathcal{R}$ le sous groupe de $\mathcal{A}$ engendré par les idéaux premiers ramifiés (i.e. le sous-groupe des classes contenant au moins un idéal invariant), $h(d)$ son nombres de classes, χ son caractère, $\boldsymbol{R}$ son anneau des entiers, ω_0 le générateur habituel de cet anneau des entiers (égal à $\sqrt{d}$ si 4 divise D et égal à $(1+\sqrt{d})/2$ si 4 ne divise pas D), $f_D(X)$ le polynôme $-N(\omega_0-X)$, ($f_D(X) = -X^2+X+(d-1)/4$ si 4 ne divise pas D et $f_D(X) = d-X^2$ si 4 divise D) et ε_0 son unité fondamentale.

Notre théorème 3 prolonge les résultats de [2], [5], [7], [8], [10] et caractérise la trivialité de $\mathcal{H}$ par la nature arithmétique des $f_D(k)$ lorsque k varie de 1 à la partie entière de $(1/2)\sqrt{D}$. Cette caractérisation fait intervenir des invariants $Q_i(\boldsymbol{I})$ liés à des développements en fractions continues, $\boldsymbol{I}$ parcourant un système complet d'idéaux ambiges représentant les classes ambiges. Aussi, au deuxième paragraphe, nous donnons une démonstration des résultats bien connus sur l'ordre du sous-groupe $\mathcal{A}$ nous permettant d'obtenir explicitement un tel système complet de représentants. Nous illustrons au troisième paragraphe ce critère sur les quatre exemples: $\boldsymbol{Q}(\sqrt{d})$ avec $d = 5\times 13\times 29$ et $d = 13\times 17\times 29\times 37\times 41$ et les deux familles: $\boldsymbol{Q}(\sqrt{d})$, $d = m^2-1$ et $d = m^2-4$. Nos théorèmes 10 et 11 donnent deux exemples de prolongement des résultats de [2], [8] et [10] en non plus une caractérisation de la principalité d'une famille de corps quadratiques réels, mais de la trivialité de leurs groupes des classes. Au quatrième et dernier paragraphe, nous utilisons les techniques que nous venons de développer pour déterminer, sous

l'hypothèse de Riemann faible $\zeta_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(1/2) \leqslant 0$, les corps quadratiques réels $\mathbf{Q}(\sqrt{d})$ tels que leur caractère ne prenne pas la valeur $+1$ sur les nombres premiers inférieurs ou égaux à $(1/2)\sqrt{D}$ (pour ces corps $\mathscr{H} = \mathscr{A} = \mathscr{R}$) en majorant d par 30272. Ceci nous permet de lister les corps à groupe de classes d'idéaux réduit à $\mathscr{A}$ pour la famille $\mathbf{Q}(\sqrt{d})$, $d = m^2-1$ (avec $m-1$ ou $m+1$ premier) et réduit à $\mathscr{R}$ pour la famille $\mathbf{Q}(\sqrt{d})$, $d = m^2-4$ (avec $m-2$ ou $m+2$ premier). Ces résultats prolongent ceux de R. A. Mollin et H. C. Williams [8], [9] qui, sous l'hypothèse de Riemann, déterminent les corps quadratiques réels tels que leur caractère ne prenne que la valeur -1 sur les nombres premiers inférieurs à $(1/2)\sqrt{D}$ en majorant leur discriminant par 10^{13}.

Un idéal entier I est dit primitif si il n'est divisible par aucun idéal de la forme (n), n entier et $n \geqslant 2$; les idéaux primitifs s'écrivent, en tant que $\mathbf{Z}$-modules, sous la forme $I = (a, b+\omega_0)_{\mathbf{Z}}$, $a = N(I)$ divisant $N_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(b+\omega_0)$. Un idéal primitif est dit réduit si on peut choisir b (alors de façon unique) modulo a pour que son réel quadratique associé, défini par $x_0(I) = (b+\omega_0)/a$, soit réduit (i.e. vérifie $x_0(I) > 1$ et $-1/X_0(I)' > 1$, où "$'$" désigne le conjugué dans le corps). Si I est un idéal réduit, nous supposerons toujours $x_0(I)$ choisi réduit. L'application qui à un idéal associe son réel quadratique définit une bijection de l'ensemble des idéaux réduits du corps sur l'ensemble fini des réels quadratiques réduits de discriminant D. Les idéaux primitifs de norme inférieure à $(1/2)\sqrt{D}$ étant réduits d'après le lemme 1 de [7] et la borne de Minkowski valant $(1/2)\sqrt{D}$ dans le cas quadratique réel, nous en déduisons que chaque classe d'idéaux contient un idéal réduit. Le nombre de classes d'idéaux $h(d)$ est donc fini. Deux idéaux réduits sont équivalents dans le groupe des classes d'idéaux si et seulement si leurs réels quadratiques associés sont équivalents sous l'action de $\mathrm{GL}_2(\mathbf{Z})$. Soit I un idéal réduit, $x_0(I)$ admet un développement en fractions continues purement périodique:

$$x_0(I) = \overline{[n_0, n_1, \ldots, n_{L(I)-1}]}.$$

Les $L(I)$ réels quadratiques réduits définis par

$$x_i(I) = \overline{[n_i, \ldots, n_{L(I)-1}, n_0, \ldots, n_{i-1}]}, \quad 0 \leqslant i \leqslant L(I)-1,$$

sont alors les seuls réels quadratiques réduits équivalents, sous l'action de $\mathrm{GL}_2(\mathbf{Z})$, à $x_0(I)$; ils s'écrivent de manière unique sous la forme $x_i(I) = (P_i(I) + \sqrt{D})/2Q_i(I)$ avec $P_i(I)$ et $Q_i(I)$ entiers strictement positifs et $Q_i(I)$ divisant $(D-P_i(I)^2)/4$. Les $\mathbf{Z}$-modules $I_i = (Q_i(I), (P_i(I)+\sqrt{D})/2)_{\mathbf{Z}}$ sont alors les idéaux réduits de réels quadratiques associés $x_0(I_i)$ égaux à $x_i(I)$; ils sont de norme $N(I_i) = Q_i(I)$. L'ensemble $\{I_i;\ 0 \leqslant i \leqslant L(I)-1\}$ (en posant $I_0 = I$) est appelé le cycle des idéaux réduits de l'idéal réduit I. Nous partitionnons donc les, disons, $m(d)$ idéaux réduits du corps en $h(d)$ cycles d'idéaux réduits. $m(d)$ est appelé, suivant G. Lachaud [6], le calibre du corps et le calibre $m(\mathscr{C})$ d'une classe d'idéaux $\mathscr{C}$ est par définition la longueur du cycle d'idéaux réduits d'un idéal réduit quelconque de cette classe. Pour des détails et précisions sur ces rappels, nous renvoyons le lecteur à [4], [7] et [11]; pour une illustration de l'utilisation des cycles d'idéaux à H. Amara [1].

1. Critère de réduction du groupe des classes a son sous-groupe des classes ambiges

LEMME 1. *Si I est un idéal réduit, son idéal conjugué I' est réduit.*

Preuve. Si $I = (a, b+\omega_0)_{\mathbf{Z}}$ alors $I' = (a, b+\omega_0')_{\mathbf{Z}} = (a, -b-\omega_0')_{\mathbf{Z}} = (a, b'+na+\omega_0)_{\mathbf{Z}}$ avec $b' = -b-\mathrm{Trace}(\omega_0)$ et n quelconque dans $\mathbf{Z}$. I étant réduit, nous pouvons supposer $x_0(I) = (b+\omega_0)/a$ réduit; nous devons montrer que nous pouvons choisir n dans $\mathbf{Z}$ tel que $x_0(I') = (b'+na+\omega_0)/a = n-x_0(I)'$ soit réduit. Si $x_0(I) = \overline{[n_0, n_1, \ldots, n_{L-1}]}$, nous avons d'après H. Hasse [4]: $-1/x_0(I)' = \overline{[n_{L-1}, \ldots, n_1, n_0]}$, et donc $x_0(I') = \overline{[n, n_{L-1}, \ldots, n_1, n_0]}$. Puisque $x_0(I')$ est réduit si et seulement si son développement en fractions continues est purement périodique (H. Hasse [4]), il faut et il suffit de prendre $n = n_0$ pour que $x_0(I')$ soit réduit. I' est donc réduit et $x_0(I') = \overline{[n_0, n_{L-1}, \ldots, n_1]}$. ∎

PROPOSITION 2. *Soit I un idéal réduit ambige de cycle d'idéaux réduits ambiges de longueur $L(I)$; un idéal réduit J tel que J et J' soient les seuls idéaux de norme $N(J)$ appartient au cycle de I si et seulement si $N(J)$ appartient à $\{Q_i(I);\ 0 \leqslant i \leqslant L(I)-1\}$.*

Preuve. Si J appartient au cycle de I et $J = I_i$, alors $N(J) = N(I_i) = Q_i(I)$.

Réciproquement, si $N(J) = Q_i(I) = N(I_i)$, par hypothèse I_i est égal à J ou J', ou encore, J est égal à I_i ou $(I_i)'$. Chaque idéal I_i du cycle de I étant équivalent dans le groupe des classes d'idéaux à l'idéal ambige I est également ambige. Conséquemment, l'idéal $(I_i)'$ est équivalent dans le groupe des classes à l'idéal I_i. Puisqu'il est réduit d'après le lemme précédent, il appartient au cycle d'idéaux de I_i qui est égal à celui de I, d'où: $(I_i)' = I_j$, pour un indice j convenable, et nous avons le résultat. ∎

Nous définissons l'ensemble $E(D)$ par: $E(D) = \{N(I);\ I$ idéal réduit ambige$\}$. $E(D)$ est fini puisqu'il n'existe qu'un nombre fini d'idéaux réduits. Nous avons:

THÉORÈME 3. (a) *$\mathscr{H} = \mathscr{A}$ si et seulement si $\{p;\ p$ premier, $p \leqslant (1/2)\sqrt{D}$ et $\chi(p) \neq -1\}$ est inclus dans $E(D)$.*

(b) *$\mathscr{H} = \mathscr{A}$ si et seulement si les diviseurs premiers inférieurs à $(1/2)\sqrt{D}$ des $f_D(k)$ non-premiers, lorsque k entier varie de 1 à $(1/2)\sqrt{D}$, sont dans l'ensemble $E(D)$.*

Preuve. Rappelons que les idéaux primitifs de norme inférieure à $(1/2)\sqrt{D}$ sont réduits (Lemme 1 de [7]).

Si $\mathscr{H} = \mathscr{A}$ et p est premier avec $p \leqslant (1/2)\sqrt{D}$ et $\chi(p) \neq -1$ et si $\mathscr{P}$ est un idéal premier de norme p au dessus de (p), $\mathscr{P}$ est réduit. Puisqu'il est supposé ambige, p appartient à $E(D)$.

Si $\mathscr{H} = \mathscr{A}$ et p premier divise un $f_D(k)$ pour k tel que $1 \leqslant k \leqslant (1/2)\sqrt{D}$, $\chi(p)$ est différent de -1 et, par l'implication ci-dessus, p appartient à $E(D)$.

Réciproquement, si $E(D)$ contient l'ensemble $\{p;\ p \text{ premier}, \chi(p) \neq -1 \text{ et } p \leqslant (1/2)\sqrt{D}\}$, tous les idéaux premiers $\mathscr{P}$ non-inertes de norme p inférieure à $(1/2)\sqrt{D}$ sont ambiges d'après la proposition 2. Puisqu'ils engendrent le groupe des classes, $\mathscr{H} = \mathscr{A}$.

De même, si les diviseurs premiers inférieurs à $(1/2)\sqrt{D}$ des $f_D(k)$ sont dans $E(D)$, les idéaux premiers non-inertes de norme inférieure à $(1/2)\sqrt{D}$ sont ambiges, et donc $\mathscr{A} = \mathscr{H}$. En effet, si $\mathscr{P} = (p, \omega_0 - n_p)_{\mathbf{Z}}$ est non-inerte de norme p vérifiant $p \leqslant (1/2)\sqrt{D}$, nous pouvons supposer que n_p, qui n'est défini que modulo p, vérifie $1 \leqslant n_p \leqslant p$; soit $1 \leqslant n_p \leqslant (1/2)\sqrt{D}$. Puisque $\mathscr{P}$ est de norme p, p divise la norme de $\omega_0 - n_p$ qui est égale à $-f_D(n_p)$, p est donc dans $E(D)$. Par la proposition 2, $\mathscr{P}$ est ambige. ∎

Pour appliquer ce critère, il nous faut connaitre tous les idéaux réduits ambiges. Les développements en fractions continues nous permettant de déterminer un cycle à partir d'un de ses idéaux, il nous suffit de connaitre un idéal réduit ambige dans chacun des cycles d'idéaux réduits ambiges (i.e. un idéal réduit représentant chaque classe d'idéaux ambiges). Si $\mathscr{A}$ est réduit à $\mathscr{R}$, le lemme a) de [7] (reproduit au lemme 5 ci-dessous) nous permet de le faire. Nous montrons maintenant que nous pouvons également y parvenir pour $\mathscr{A} \neq \mathscr{R}$.

2. Le sous-groupe des classes ambiges. Si $I = I_0$ est un idéal réduit nous notons $L(I)$, ou L si il n'y a pas de risque de confusion, la longueur du cycle de I (i.e. la longueur de la période primitive de $x_0(I)$) et définissons, pour i dans $\mathbf{Z}$, l'idéal I_i dans le cycle de I par $I_i = I_{i'}$, où i' est congru à i modulo $L(I)$ et vérifie $0 \leqslant i' \leqslant L(I)-1$. Nous avons donc $I_i = I_{i+L}$ pour i dans $\mathbf{Z}$.

LEMME 4. *Soit I un idéal réduit, son conjugué I' est réduit et $(I')_i = (I_{-i})'$.*

Preuve. Si $x_0(I) = \overline{[n_0, n_1, \ldots, n_{L-1}]}$, nous avons vu au lemme 1 que I' était réduit et que nous avions $x_0(I') = \overline{[n_0, n_{L-1}, \ldots, n_1]}$. Nous avons donc

$$x_0(I_{-i}) = x_0(I_{L-i}) = x_{L-i}(I) = \overline{[n_{L-i}, \ldots, n_{L-1}, n_0, \ldots, n_{L-i-1}]};$$

nous en déduisons donc que

$$x_0((I_{-i})') = \overline{[n_{L-i}, n_{L-i-1}, \ldots, n_0, n_{L-1}, \ldots, n_{L-i+1}]}.$$

D'un autre côté, puisque $x_0(I') = \overline{[n_0, n_{L-1}, \ldots, n_1]}$, nous avons

$$x_i(I') = \overline{[n_{L-i}, \ldots, n_0, n_{L-1}, \ldots, n_{L-i+1}]}.$$

Finalement, $x_0((I')_i) = x_0((I_{-i})')$ et donc $(I')_i = (I_{-i})'$. ∎

Un idéal est dit invariant ou ramifié si il est primitif et égal à son conjugué, ou encore, si il est primitif et produit d'idéaux premiers ramifiés. Si il est de norme δ libre de carrés et divisant D, nous le notons I_δ. Soit alors δ' défini par: δ' est libre de carrés et $d\delta = n^2\delta'$; l'idéal ramifié $I_{\delta'}$ est appelé l'idéal ramifié "dual" de l'idéal ramifié I_δ et noté $\tilde{I}_\delta$. Puisque $(n)\tilde{I}_\delta = (\sqrt{d})I_\delta$, I_δ et son idéal "dual" $\tilde{I}_\delta$ sont dans la même classe d'idéaux.

Soit I un idéal reduit, I est ambige si et seulement si son idéal conjugué I', qui est également réduit, lui est équivalent; donc si et seulement si son idéal conjugué I' appartient au cycle d'idéaux réduits de I, i.e. est un certain I_i. L'égalité entre idéaux $I' = I_i$ étant équivalente à l'égalité entre leur réel quadratique associé: $x_0(I') = x_0(I_i) = x_i(I)$, l'idéal I est ambige si et seulement si il existe i tel que: $0 \leqslant i \leqslant L-1$ et $x_0(I) = \overline{[n_0, \ldots, n_i, n_{i+1}, \ldots, n_{L-1}]}$, avec les deux effets "palindromiques": $n_j = n_{i-j}$ pour $0 \leqslant j \leqslant i$, et $n_j = n_{L+i-j}$ pour $i+1 \leqslant j \leqslant L-1$; il est invariant si et seulement si $x_0(I) = \overline{[n_0, \ldots, n_{L-1}]}$ avec l'effet "palindromique": $n_j = n_{L-j}$ pour $0 \leqslant j \leqslant L-1$. Rappelons que tous les cycles ont même parité de longueur, puisque $N(\varepsilon_0) = (-1)^{L(I)}$.

LEMME 5. *Le nombre d'idéaux ramifiés réduits est précisément 2^{t-1}.*

Preuve. C'est le lemme 5 de [7]: si δ libre de carrés divise D, exactement un des deux idéaux ramifiés I_δ ou son idéal "dual" I_δ est réduit: celui de plus petite norme.

LEMME 6. *Si $I = (a, (b+\sqrt{D})/2)_{\mathbf{Z}}$ est un idéal réduit avec $x_0(I) = (b+\sqrt{D})/2a$ réduit, $I' = I_{-1}$ si et seulement si $D = 4a^2+b^2$. Si d est somme de deux carrés, il y a précisément 2^{t-1} tels idéaux.*

Preuve. Si $x_0(I) = \overline{[n_0, n_1, \ldots, n_{L-1}]}$, nous avons $x_0(I') = \overline{[n_0, n_{L-1}, \ldots, n_1]}$ puis $x_1(I') = \overline{[n_{L-1}, \ldots, n_1, n_0]} = -1/x_0(I)'$. $I' = I_{-1}$ si et seulement si $(I')_1 = I_0 = I$, donc si et seulement si $x_0((I')_1) = x_1(I') = x_0(I)$, nous avons donc $I' = I_{-1}$ si et seulement si $x_0(I) = -1/x_0(I)'$, donc si et seulement si la norme de $x_0(I)$ vaut -1, d'où le premier résultat. Il est connu, et aisé de montrer en travaillant dans l'anneau principal $\mathbf{Z}[i]$, que D est somme de deux carrés si et seulement si ses diviseurs premiers impairs sont congrus à 1 modulo 4; D a alors exactement 2^{t-1} écritures sous la forme: $D = 4a^2+b^2$. ∎

PROPOSITION 7. (a) *Si $N(\varepsilon_0) = -1$ chaque cycle d'idéaux réduits ambiges contient exactement 1 idéal invariant et 1 idéal J tel que $J' = J_{-1}$.*

(b) *Si* $N(\varepsilon_0) = +1$ *on est dans un des deux cas exclusifs suivants:*

(α) *Le cycle d'idéaux réduits ambiges contient exactement* 2 *idéaux invariants et aucun idéal* $\boldsymbol{J}$ *tel que* $\boldsymbol{J}' = \boldsymbol{J}_{-1}$. *Il y a exactement* 2^{t-2} *tels cycles d'idéaux réduits ambiges.*

(β) *Le cycle d'idéaux réduits ambiges ne contient pas d'idéal invariant et exactement* 2 *idéaux* $\boldsymbol{J}$ *tels que* $\boldsymbol{J}' = \boldsymbol{J}_{-1}$. *Il n'existe de tels cycles d'idéaux réduits ambiges que si* d *est somme de deux carrés; il y en a alors* 2^{t-2}.

De plus, on est dans le cas (α) *si et seulement si* $\boldsymbol{I}' = \boldsymbol{I}_i$ *avec* i *pair pour tout idéal* $\boldsymbol{I}$ *du cycle et les deux idéaux invariants du cycle sont* $\boldsymbol{I}_{i/2}$ *et* $\boldsymbol{I}_{(i+L)/2}$; *on est dans le cas* (β) *si et seulement si* $\boldsymbol{I}' = \boldsymbol{I}_i$ *avec* i *impair pour tout idéal* $\boldsymbol{I}$ *du cycle et les deux idéaux du cycle tels que* $\boldsymbol{J}' = \boldsymbol{J}_{-1}$ *sont* $\boldsymbol{I}_{(i+1)/2}$ *et* $\boldsymbol{I}_{(L+i+1)/2}$.

Preuve. Si $\boldsymbol{J} = \boldsymbol{I}_j$ est un idéal réduit ambige du cycle de $\boldsymbol{I}$ et si $\boldsymbol{I}' = \boldsymbol{I}_i$, d'après le lemme 4 nous avons: $\boldsymbol{J}' = (\boldsymbol{I}_j)' = (\boldsymbol{I}')_{-j} = (\boldsymbol{I}_i)_{-j} = \boldsymbol{I}_{i-j} = (\boldsymbol{I}_j)_{i-2j} = \boldsymbol{J}_{i-2j}$. D'où $\boldsymbol{J}' = \boldsymbol{J}$ si et seulement si $i = 2j$ modulo L. Si $N(\varepsilon_0) = -1$, L est impair et cette congruence admet exactement une solution modulo L. Si $N(\varepsilon_0) = +1$, L est pair et cette congruence admet au moins une solution si et seulement si i est pair; elle admet alors exactement deux solutions: $j = i/2$ et $j = (i+L)/2$. De même, $\boldsymbol{J}' = \boldsymbol{J}_{-1}$ si et seulement si $i-2j = -1$ modulo L. Si L est impair, cette congruence admet exactement une solution modulo L; si L est pair elle n'admet de solution que si i est impair, et elle admet alors exactement deux solutions modulo L: $j = (i+1)/2$ et $j = (L+i+1)/2$.

Les résultats sur les nombres de cycles découlent des lemmes 5 et 6.

THÉORÈME 8. (1) *Si* $N(\varepsilon_0) = -1$, $\mathscr{A} = \mathscr{R}$ *est d'ordre* 2^{t-1}.

(2) *Si* $N(\varepsilon_0) = +1$ *et* $D \neq 4a^2+b^2$, $\mathscr{A} = \mathscr{R}$ *est d'ordre* 2^{t-2}.

(3) *Si* $N(\varepsilon_0) = +1$ *et* $D = 4a^2+b^2$, $\mathscr{A} \neq \mathscr{R}$ *et* $\mathscr{A}$ *est d'ordre* 2^{t-1} *et* $\mathscr{R}$ *est d'ordre* 2^{t-2}.

Preuve. Immédiate à l'aide de la proposition 6.

Pour a et b tels que $D = 4a^2+b^2$ nous notons $\boldsymbol{I}_{a,b}$ l'idéal réduit ambige de norme a égal à $(a, (b+\sqrt{D})/2)_{\mathbf{Z}}$; pour δ libre de carrés divisant D nous notons $\boldsymbol{I}_\delta$ l'idéal ramifié de norme δ. De la preuve de la proposition 7, nous déduisons:

(1) $N(\varepsilon_0) = -1$: les 2^{t-1} idéaux $\boldsymbol{I}_{a,b}$, ou les 2^{t-1} idéaux ramifiés réduits représentent simplement les classes ambiges.

(2) $N(\varepsilon_0) = +1$ et $D \neq 4a^2+b^2$: les 2^{t-1} idéaux ramifiés réduits représentent doublement les classes ambiges et les méthodes de [7] permettent de sélectionner 2^{t-2} de ces idéaux les représentant simplement: si $L = L(\omega_0) = L(\boldsymbol{R})$ et $d_1 = Q_{L/2}(\boldsymbol{R})$, nous retrouvons donc avec l'aide de la proposition 7(b) (α) les résultats de [7]: d_1 est libre de carrés, divise D et $\boldsymbol{I}_{d_1}$ est principal. Soit $\boldsymbol{I}_\delta$ un idéal réduit ramifié; écrivons $d_1\delta = n^2\delta'$ avec δ' libre de carrés. $\boldsymbol{I}_{\delta'}$ et son idéal "dual" $\tilde{\boldsymbol{I}}_{\delta'}$ sont équivalents à $\boldsymbol{I}_\delta$ et celui de ces deux idéaux qui est réduit (i.e. de plus petite norme) est le second idéal ramifié réduit du cycle d'idéaux réduits de $\boldsymbol{I}_\delta$.

(3) $N(\varepsilon_0) = +1$ et $D = 4a^2+b^2$: les 2^{t-1} idéaux ramifiés réduits représentent doublement les classes ambiges contenant au moins un idéal invariant (et les méthodes de [7] permettent comme précédemment de sélectionner 2^{t-2} de ces idéaux représentant simplement ce sous groupe $\mathscr{R}$) et les 2^{t-1} idéaux réduits $\boldsymbol{I}_{a,b}$ représentent doublement les classes ambiges ne contenant pas d'idéal invariant (et les développements en fractions continues des $x_0(\boldsymbol{I}_{a,b})$ permettent de sélectionner 2^{t-2} de ces idéaux $\boldsymbol{I}_{a,b}$ représentant simplement ces classes de $\mathscr{A} \setminus \mathscr{R}$). En effet, si $L = L(\boldsymbol{I}_{a,b})$, Lest pair et $x_{L/2}(\boldsymbol{I}_{a,b}) = (b'+\sqrt{D})/2a'$ avec $D = 4a'^2+b'^2$ et $\boldsymbol{I}_{a',b'}$ est équivalent dans le groupe des classes à $\boldsymbol{I}_{a,b}$ car dans le même cycle que $\boldsymbol{I}_{a,b}$, et nous avons $a' = Q_{L/2}(\boldsymbol{I}_{a,b})$.

3. Exemples

EXEMPLE 1. $d = 1885 = 5 \times 13 \times 29$. Ici $L(\boldsymbol{R})$ (longueur du cycle d'idéaux réduits principaux = longueur de la période primitive de ω_0) $= 4$ et $Q_2(\boldsymbol{R}) = 29$, donc $N(\varepsilon_0) = +1$ et le sous groupe $\mathscr{R}$ engendré par les idéaux ramifiés est d'ordre 2 et engendré par l'idéal premier ramifié réduit $\mathscr{P}_5 = (5, (35+\sqrt{d})/2)_{\mathbf{Z}}$ au dessus de (5) ([7], théorème 5). Les quatre décompositions de $D = d$ en $d = 4a^2+b^2$ sont obtenues pour $(a, b) = (3, 43)$, $(17, 27)$, $(19, 21)$ et $(21, 11)$. Nous donnons ci-dessous le tableau des $L(\boldsymbol{I}_{a,b})$, $Q_i(\boldsymbol{I}_{a,b})$, $L(\mathscr{P}_5)$ et $Q_i(\mathscr{P}_5)$:

idéal $\boldsymbol{I}$	$L(\boldsymbol{I})$	$\{Q_i(\boldsymbol{I});\ 0 \leqslant i \leqslant L(\boldsymbol{I})-1\}$
$\boldsymbol{R} = \boldsymbol{Z}[\omega_0]$	4	1, 9, 29, 9
$\mathscr{P}_5$	6	5, 33, 7, 13, 7, 33
$\boldsymbol{I}_{3,43}$	4	3, 17 et $\boldsymbol{I}_{17,27} \sim \boldsymbol{I}_{3,43}$, 17, 3
$\boldsymbol{I}_{19,21}$	10	19, 21, 15, 11, 21 et $\boldsymbol{I}_{21,11} \sim \boldsymbol{I}_{19,21}$, 21, 11, 15, 21, 19

La partie entière de $(1/2)\sqrt{D}$ valant 22, $E(D)$ contenant tous les entiers impairs inférieurs ou égaux à 21 et d étant congru à 5 modulo 8 (donc $x(2) = -1$), nous déduisons du théorème 3(a): $\mathscr{H} = \mathscr{A} = (\mathbf{Z}/2\mathbf{Z})^2$.

EXEMPLE 2. $d = 9722453 = 13 \times 17 \times 29 \times 37 \times 41$ est congru à 5 modulo 8 (d'où $x(2) = -1$). Ici $L(\omega_0) = 32$ et $Q_{16}(\boldsymbol{R}) = 17 \times 29$, donc $N(\varepsilon_0) = +1$ et $\mathscr{H}$ est d'ordre 8 engendré par les idéaux premiers $\mathscr{P}_{13}$, $\mathscr{P}_{17}$ et $\mathscr{P}_{37}$ ([7], théorème 5). Afin de simplifier les calculs numériques, nous remarquons que dans le théorème 3(a) nous pouvons remplacer $\{p;\ p$ premier, $p \leqslant (1/2)\sqrt{D}$ et $x(p) \neq -1\}$ par $\{p;\ p$ premier, $p \leqslant \sqrt{D/8}$ et $x(p) = +1\}$ puisqu'il est connu que pour $D \neq 5$ toute classe d'idéaux contient un idéal entier de norme inférieure à $\sqrt{D/8}$. Nous avons programmé sur calculatrice la recherche des nombres premiers inférieurs à $\sqrt{D/8}$, c'est à dire à 1102, tels que le symbole de Legendre (d/p) vaille $+1$ (Il y a 89 tels nombres premiers) et la détermination des $Q_i(\boldsymbol{I})$, $\boldsymbol{I}$ parcourant les 8 idéaux ramifiés réduits représentant $\mathscr{R}$ et les 16 idéaux $\boldsymbol{I}_{a,b}$. Nous avons alors vérifié que $E(D)$ contenait ces 89 nombres premiers.

Nous avons donc $\mathscr{H} = \mathscr{A} = (\mathbf{Z}/2\mathbf{Z})^4$ et $h(d) = 16$. Nous donnons ci-dessous le tableau des $L(\mathfrak{I}_\delta)$ et $L(\mathfrak{I}_{a,b})$ ainsi que les (a', b') tels que $\mathfrak{I}_{a,b}$ soit équivalent dans le groupe des classes à $\mathfrak{I}_{a',b'}$ (et remarquons que si l'idéal $\mathfrak{I}_{13\times17\times37}$ n'est pas réduit, son idéal "dual" $\mathfrak{I}_{29\times41}$ l'est):

a	$L = L(\mathfrak{I}_{a,b})$	$a' = Q_{L/2}(\mathfrak{I}_{a,b})$	δ	$L(\mathfrak{I}_\delta)$
89	18	331	1	32
181	32	589	13	38
569	38	1199	17	32
709	30	1541	37	34
811	54	1009	13×17	48
1121	42	1381	13×37	30
1279	40	1471	17×37	36
1499	32	1599	$13\times17\times37 \sim 29\times41$	40

EXEMPLE 3. Prenons $d = m^2-1$, m pair et $m-1$ ou $m+1$ premier. Ici $L(\mathbf{R}) = 2$ et $N(\varepsilon_0) = +1$, $Q_1(\mathbf{R}) = 2(m-1)$. Puisque $m-1$ ou $m+1$ est congru à 3 modulo 4, d n'est pas somme de deux carrés et $\mathscr{A}$ est réduit à $\mathscr{R}$ et d'ordre 2^{t-2}. Les trois relations de principalité entre les idéaux ramifiés étant (théorème 5 de [7]): $\mathfrak{I}_d = (\sqrt{d})$, $\mathfrak{I}_{2(m-1)} = (\alpha)$ et $\mathfrak{I}_{2(m+1)} = (\beta)$, $\mathscr{R}$ est engendré par $t-2$ quelconques des idéaux premiers $\mathscr{P}_p$ au dessus des (p) lorsque p parcourt les diviseurs premiers de d. Si nous supposons $m-1$ ou $m+1$ premier (ce qui est le cas pour $t \leqslant 4$) et notons d' l'autre terme, $\mathscr{R}$ est donc représenté (simplement) par les 2^{t-2} idéaux ramifiés $\mathfrak{I}_\delta = (\delta, \sqrt{d})_{\mathbf{Z}}$, δ parcourant les diviseurs de d'. Nous donnons ci-dessous la norme des idéaux réduits du cycle de $\mathfrak{I}_\delta$.

LEMME. (a) *Si δ divise $m-1$, alors*

$$\sqrt{d}/\delta = [(m-1)/\delta, \overline{\delta, 2(m-1)/\delta}] \quad \text{et} \quad \{Q_i(\mathfrak{I}_\delta)\} = \{\delta, 2(m-1)/\delta\}.$$

(b) *Si δ divise $m+1$ et $\delta \neq 1$, $m+1$ alors*

$$\sqrt{d}/\delta = [(m+1)/\delta - 1, \overline{1, \delta-2, 1, 2(m+1)/\delta-2}]$$

et

$$\{Q_i(\mathfrak{I}_\delta)\} = \{\delta, 2(m+1)/\delta, 2(m+1)-\delta-2(m+1)/\delta\}.$$

$2(m+1)-\delta-2(m+1)/\delta$ étant supérieur à $(1/2)\sqrt{D}$ (pour δ divisant $m+1$ et $\delta \neq 1$, $m+1$) les éléments de $E(D)$ inférieurs à $(1/2)\sqrt{D}$ divisent D. Le théorème 3(a) donne alors que pour $m-1$ ou $m+1$ premier le groupe des classes $\mathscr{H}$ se réduit à $\mathscr{A}$ si et seulement si $(d/p) = \chi(p) \neq +1$, $3 \leqslant p \leqslant m-1$. Nous montrons, réciproquement, que cette condition implique la primalité de $m-1$ ou $m+1$.

LEMME 9. *Si a et b sont les normes des deux idéaux ramifiés d'un cycle d'idéaux réduits ambiges d'un corps quadratique réel d'unité fondamentale de norme $+1$ et tel que $\chi(p) \neq +1$, $2 \leqslant p \leqslant (1/2)\sqrt{D}$, le discriminant D du corps s'écrit alors $D = M^2-4r$, M^2+4r avec $r = ab$ divisant M, ou $D = M^2+r$ avec $r = ab$ divisant $2M$.*

PREUVE. La proposition 16 et le lemme 17 donnent: $\sqrt{D}/a = \sqrt{\Delta}/\alpha$ et $\sqrt{D}/b = \sqrt{\Delta}/\beta$. Nous en déduisons $D/ab = \Delta/\alpha\beta = \alpha\beta+4$, $\alpha\beta-4$ ou $\alpha\beta+1$ puis $D/a^2 = \Delta/\alpha^2$, qui implique $\alpha b = \beta a$. Le carré du P.G.C.D. de a et b divisant D, il vaut 1 ou 2. Si il vaut 1, il existe q tel que $\alpha = qa$ et $\beta = qb$ et nous avons le résultat. Si il vaut 2, il existe q tel que $\alpha = q(a/2)$ et $\beta = q(b/2)$ et nous avons le résultat.

COROLLAIRE. *Si $d = m^2-1$ (respectivement $d = m^2-4$) est libre de carrés et tel que $\chi(p) \neq +1$, $2 \leqslant p \leqslant (1/2)\sqrt{D}$, alors $m-1$ ou $m+1$ est premier (respectivement $m-2$ ou $m+2$ est premier).*

PREUVE. Nous prouvons le cas: $D = 4d = 4m^2-4$. Supposons $m-1$ et $m+1$ non premiers. d étant libre de carrés, il existe alors un diviseur d_1 de $m-1$ et un diviseur d_2 de $m+1$ vérifiant: $1 < d_1 < \sqrt{m-1}$ et $1 < d_2 < \sqrt{m+1}$, et tels que $\delta = d_1 d_2$ soit libre de carrés (et impair). L'idéal ramifié $\mathfrak{I}_\delta$ de norme $\delta = d_1 d_2$ est réduit (puisque son idéal "dual" est de norme d/δ supérieure à δ). $m-1$ et $m+1$ étant premiers entre eux (car impairs), d_1 et d_2 sont premiers entre eux et δ ne divise donc ni $2m-2$, ni $2m+2$, ni 4. Les seules écritures de D sous la forme $D = M^2-4r$, M^2+4r avec r divisant M ou $D = M^2+r$ avec r divisant $2M$ sont obtenues pour $D = (2m+2)^2-4(2m+2)$, $D = (2m)^2-4$ et $D = (2m-2)^2+4(2m-2)$ (Raisonner sur la partie entière de $\sqrt{D}$ pour obtenir M, puis en déduire la valeur de r). Le lemme 9 nous donnant que δ divise $2m-2$, $2m+2$ ou 4, nous avons le résultat. ∎

Nous pouvons maintenant énoncer notre théorème:

THÉORÈME 10. *Pour $d = m^2-1$ libre de carrés il y a équivalence entre les propriétés suivantes:*

(a) *$m-1$ ou $m+1$ est premier et $\mathscr{H} = \mathscr{A} (= \mathscr{R})$.*

(b) *$3 \leqslant p \leqslant m-1$ et p premier impliquent $(d/p) = \chi(p) \neq +1$.*

(c) *Les diviseurs premiers impairs inférieurs ou égaux à $m-1$ des $d-k^2$, lorsque k varie de 1 à $m-1$, divisent d.*

(d) *De plus, si $(d/p) = +1$ pour p premier et $p \leqslant m-1$, $h(d)$ est minoré par $2^{t-2}(\mathrm{Log}(\sqrt{d})/\mathrm{Log}(p))$.*

PREUVE. Il ne reste qu'à prouver le dernier point. Soit p tel que $(d/p) = +1$ et $p \leqslant m-1$, soit $p \leqslant (1/2)\sqrt{D}$, et $\mathscr{P}$ un idéal premier au dessus de (p). Pour $p^k \leqslant (1/2)\sqrt{D}$ l'idéal $\mathscr{P}^k$ de norme p^k inférieure à $(1/2)\sqrt{D}$ est réduit. D'après la proposition 2 et le fait que les éléments de $E(D)$ ne divisant pas D sont minorés par $(1/2)\sqrt{D}$, l'idéal $\mathscr{P}^k$ n'appartient pas à $\mathscr{A}$. ∎

Remarque. Pour $m = 34$ et 56, le groupe des classes est encore trivial mais ni $m-1$ ni $m+1$ ne sont premiers.

En reprenant exactement le même schéma, il est aisé de voir que nous avons un résultat analogue pour $d = m^2-4$, sauf qu'ici nous ne pouvons pas affirmer que $\mathscr{A} = \mathscr{R}$, puisque d peut être somme de deux carrés. Aussi, nous ne pouvons établir que des résultats sur la réduction de $\mathscr{H}$ à $\mathscr{R}$.

THÉORÈME 11. *Pour $d = m^2-4$ libre de carrés il y a équivalence entre les propriétés suivantes:*

(a) *$m-2$ ou $m+2$ est premier et $\mathscr{H} = \mathscr{R}$.*

(b) *$3 \leqslant p \leqslant (m-1)/2$ et p premier impliquent $(d/p) = \chi(p) \neq +1$.*

(c) *Les diviseurs premiers impairs inférieurs ou égaux à $(m-1)/2$ des $-k^2+k+(d-1)/4$, lorsque k varie de 1 à $(m-1)/2$, divisent d.*

(d) *De plus, si $(d/p) = +1$ pour p premier et $p \leqslant (m-1)/2$, $h(d)$ est minoré par $2^{t-2}\big(\mathrm{Log}((1/2)\sqrt{d})/\mathrm{Log}(p)\big)$.*

Remarque. Pour $m = 37$, 53, 67, 89, 93 et 163 le groupe des classes est encore réduit à $\mathscr{R}$ mais ni $m-2$ ni $m+2$ ne sont premiers.

Les corps de ces deux familles à groupe de classes $\mathscr{H}$ réduit à son sous-groupe $\mathscr{A}$ appartiennent donc à la famille de corps quadratiques réels

$$(\mathscr{F}) = \{\boldsymbol{Q}(\sqrt{d});\ d \text{ libre de carrés et } \chi(p) \neq +1 \text{ pour } 2 \leqslant p \leqslant (1/2)\sqrt{D}\}.$$

Au paragraphe qui suit, nous déterminons sous l'hypothèse de Riemann faible $\zeta_{\boldsymbol{Q}(\sqrt{d})/\boldsymbol{Q}}(1/2) \leqslant 0$ tous les corps de cette famille $(\mathscr{F})$ en en majorant d par 30272. Nous obtenons alors:

THÉORÈME 12. *Sous l'hypothèse de Riemann faible $\zeta_{\boldsymbol{Q}(\sqrt{d})/\boldsymbol{Q}}(1/2) \leqslant 0$, les corps à groupe de classes réduit à son sous groupe $\mathscr{A}$ des classes ambiges dans la famille des corps quadratiques réels $\boldsymbol{Q}(\sqrt{d})$, $d = m^2-1$ libre de carrés, $m-1$ ou $m+1$ premier, sont obtenus pour les* 8 *valeurs suivantes*: $m = 2$, 4, 6, 12, 14, 16, 22 *et* 36.

Sous la même hypothèse, les corps à groupe de classes réduit à son sous groupe $\mathscr{R}$ dans la famille des corps quadratiques réels $\boldsymbol{Q}(\sqrt{d})$, $d = m^2-4$ libre de carrés et $m-2$ ou $m+2$ premier, sont obtenus pour les 10 *valeurs suivantes*: $m = 3$, 5, 9, 13, 17, 19, 21, 31, 33 *et* 49.

4. Une famille de corps quadratiques reels. Soit $\boldsymbol{Q}(\sqrt{d})$, $d \geqslant 2$ libre de carrés, un corps quadratique réel de discriminant D. Le groupe $\mathscr{H}$ des classes d'idéaux étant engendré par les idéaux premiers $\mathscr{P}$ de norme p au dessus des idéaux (p) non inertes avec $p \leqslant (1/2)\sqrt{D}$ (borne de Minkowski), si nous voulons que le groupe des classes soit réduit à son 2-sous-groupe $\mathscr{R}$ des classes engendrées par les idéaux premiers ramifiés, il suffit d'imposer au caractère χ du corps de ne prendre que les valeurs 0 ou -1 sur les nombres premiers

inférieurs à $(1/2)\sqrt{D}$. Nous notons $(\mathscr{F})$ la famille de corps quadratiques réels définie par cette propriété.

PROPOSITION 13. *d libre de carrés et $d \geqslant 2$; il y a équivalence entre* (a) *et* (b):

(a) *$2 \leqslant p \leqslant (1/2)\sqrt{D}$ implique $\chi(p) = 0$ ou -1.*

(b) *Les diviseurs premiers des $f_D(k)$ non premiers divisent D lorsque k entier varie de 1 à $(1/2)\sqrt{D}$.*

Preuve. Similaire à la preuve du théorème 3. ∎

PROPOSITION 14. *Si $2 \leqslant p \leqslant (1/2)\sqrt{D}$ implique $\chi(p) \neq +1$, le corps $\boldsymbol{Q}(\sqrt{d})$ est de Richaud–Degert, i.e. on peut écrire $d = m^2+r$ avec $-m < r \leqslant m$ et r divise $4m$, ou $d = m^2 \pm 4m/3$.*

Preuve. On peut toujours écrire d sous la forme $d = m^2+r$ avec $-m < r \leqslant m$, et donc $|r| \leqslant \sqrt{d}$. Si p premier impair divise r, d est congru à m^2 modulo p et donc $\chi(p) \neq -1$. En particulier, si p est inférieur ou égal à $(1/2)\sqrt{D}$, p divise d, donc aussi m et p^2 ne divise pas r. Il en résulte que la partie impaire de r est libre de carrés et divise m et que nous avons donc le résultat, sauf dans le cas m pair et d congru à 1 modulo 4. Dans ce dernier cas, le lemme 9 nous donne le résultat puisque les idéaux ramifiés sont alors de norme impaire. ∎

LEMME 15. *Si $\boldsymbol{I} = (Q, (P+\sqrt{D})/2)_{\boldsymbol{Z}}$ est un idéal réduit de norme Q tel que $x_0(\boldsymbol{I}) = (P+\sqrt{D})/2Q$ soit réduit alors $Q \leqslant \sqrt{D}$ et si p premier divise Q, p n'est pas inerte. De plus, pour $Q = N(\boldsymbol{I}) \geqslant (1/2)\sqrt{D}$, la partie entière n_0 de $x_0(\boldsymbol{I})$ vaut* 1.

Preuve. Les inégalités de réduction $x_0(\boldsymbol{I}) > 1$ et $-1/x_0(\boldsymbol{I})' > 1$ impliquent le premier et dernier résultats; la congruence $D \equiv P^2 (4Q)$ provenant de la divisibilité de $N_{\boldsymbol{Q}(\sqrt{d})/\boldsymbol{Q}}((P+\sqrt{D})/2)$ par Q implique le second. ∎

PROPOSITION 16. *Si $2 \leqslant p \leqslant (1/2)\sqrt{D}$ implique $\chi(p) \neq +1$, on est dans un des deux cas exclusifs suivants:*

(a) *$N(\varepsilon_0) = -1$ et $d = 2$ ou $d = m^2+4$ avec d premier et la condition est alors équivalente à $h(d) = 1$.*

(b) *$N(\varepsilon_0) = +1$ et tous les cycles d'idéaux réduits ambiges sont de longueur* 2, 4 *ou* 6 *et de développements donnés au lemme suivant.*

Preuve. Soit $\boldsymbol{J}$ un idéal réduit non-invariant d'un cycle d'idéaux réduits ambiges. Sa norme ne divise pas D et ses diviseurs premiers inférieurs à $(1/2)\sqrt{D}$ ne sont pas inertes (lemme 15), donc divisent D par l'hypothèse faite sur le caractère; cette norme est donc supérieure à $(1/2)\sqrt{D}$.

Supposons la norme de l'unité fondamentale égale à -1, nous sommes dans le cas (a) à la proposition 7. Soit $\boldsymbol{J} = (Q, (P+\sqrt{D})/2)_{\boldsymbol{Z}}$ l'unique idéal vérifiant $\boldsymbol{J}' = \boldsymbol{J}_{-1}$ d'un cycle d'idéaux réduits ambiges de longueur donc impaire supposée au moins égale à 3. $\boldsymbol{J}$ n'est pas invariant et $-1/x_0(\boldsymbol{J})' = x_0(\boldsymbol{J})$ (lemme 6) et donc $x_0(\boldsymbol{J}) - x_0(\boldsymbol{J})' = \big((x_0(\boldsymbol{J}))^2+1\big)/x_0(\boldsymbol{J})$ est strictement supérieur à 2. Mais cette différence valant $\sqrt{D}/Q = \sqrt{D}/N(\boldsymbol{J})$, elle est inférieure à 2; nous

arrivons à une contradiction nous permettant d'affirmer que tous les cycles d'idéaux réduits ambiges sont de longueur 1. Or il est aisé de voir que le seul cycle d'idéaux réduits qui puisse être de longueur 1 est le cycle des idéaux réduits principaux et qu'il est de longueur 1 si et seulement si d est de la forme m^2+4 ou m^2+1 avec m impair (En effet, si $\boldsymbol{I} = (Q, (P+\sqrt{D})/2)_{\boldsymbol{Z}}$ est l'idéal d'un cycle d'idéaux réduits de longueur 1, $x_0(\boldsymbol{I}) = [\overline{n}] = (n+\sqrt{\delta})/2$ avec $\delta = n^2+4$ et donc $D = Q^2(n^2+4)$. Il en résulte aisément que Q est égal à 1; l'idéal $\boldsymbol{I}$ est donc l'anneau $\boldsymbol{R}$ des entiers). Nous avons donc les résultats sur la forme de d (puisque pour $d = m^2+1$, m impair supérieur ou égal à 3, les diviseurs premiers p de m sont inférieurs à $(1/2)\sqrt{D}$ et tels que $x(p) = +1$) ainsi que celui sur le nombre de classes d'idéaux, puisque si il n'y a qu'un cycle d'idéaux réduits, il n'y a qu'une seule classe d'idéaux et le corps est principal; la norme de son unité fondamentale valant -1, son discriminant est premier. Réciproquement, si pour $d = m^2+4$ le corps est principal, d'après le théorème 3 le caractère ne prend que la valeur -1 sur les nombres premiers inférieurs à $(1/2)\sqrt{D}$.

Supposons la norme de l'unité fondamentale égale à $+1$. Il y a alors exactement deux idéaux invariants dans chaque cycle d'idéaux réduits ambiges. Soit $\boldsymbol{I} = \boldsymbol{I}_0$ un idéal invariant d'un cycle d'idéaux réduits ambiges de longueur L donc paire, l'autre idéal invariant de ce cycle étant $\boldsymbol{I}_{L/2}$ (proposition 7(b)(α)), nous déduisons du lemme 14 que le développement en fractions continues de $x_0(\boldsymbol{I})$ est de la forme $[\overline{a, 1, \ldots, 1, b, 1, \ldots, 1}]$ où les séries de "1" sont toutes deux de longueur k avec $k = (L/2)-1$. Posons $\boldsymbol{J} = \boldsymbol{I}_2$ et supposons $L \geqslant 8$ (soit $k \geqslant 3$), $\boldsymbol{J}$ n'est pas invariant et $x_0(\boldsymbol{J})-x_0(\boldsymbol{J})' = [\overline{1, \ldots, 1, b, 1, \ldots, 1, a, 1}] + [\overline{0, 1, a, 1, \ldots, 1, b, 1, \ldots, 1}] = [1, 1, \alpha]+[0, 1, \beta]$, avec α et β strictement supérieurs à 1. $x_0(\boldsymbol{J})-x_0(\boldsymbol{J})'$ est donc minoré strictement par $[1, 1, 1]+[0, 1, 1] = 2$. Similairement au cas précédent nous arrivons à une contradiction de laquelle nous déduisons que les cycles d'idéaux réduits ambiges sont de longueur strictement inférieure à 8; puisqu'ils sont de longueur paire, ils sont de longueur 2, 4 ou 6. ∎

LEMME 17. (a) $[\overline{a, b}] = (\alpha\beta+\sqrt{\Delta})/2\beta$ *avec* $\Delta = \alpha\beta(\alpha\beta+4)$ *où* $\alpha = a$ *et* $\beta = b$.

(b) $[\overline{a, 1, b, 1}] = ((\alpha-2)\beta+\sqrt{\Delta})/2\beta$, *avec* $\Delta = \alpha\beta(\alpha\beta-4)$ *où* $\alpha = a+2$ *et* $\beta = b+2$.

(c) $[\overline{a, 1, 1, b, 1, 1}] = ((\alpha-1)\beta+\sqrt{\Delta})/2\beta$ *avec* $\Delta = \alpha\beta(\alpha\beta+1)$ *où* $\alpha = a+1$ *et* $\beta = b+1$.

Preuve: immédiate.

Suivant G. Lachaud [6], nous décomposons la fonction zêta partielle $\zeta(s, \mathscr{C})$ de chaque classe d'idéaux $\mathscr{C}$ en une somme de $m(\mathscr{C}) = L(\boldsymbol{I})$ fonctions méromorphes $H_i(s, \mathscr{C})$, où $\boldsymbol{I}$ est un idéal réduit dans la classe $\mathscr{C}$, telles que: $\sqrt{D}H_i(1/2, \mathscr{C}) = \sqrt{k_i}(\mathrm{Log}(k_i)-\omega)+\varepsilon$ avec $k_i = \sqrt{D}/N(\boldsymbol{I}_i) = x_i(\boldsymbol{I})-x_i(\boldsymbol{I})'$, ε terme d'erreur appartenant à $[-0{,}02; +1]$ et $\omega = \pi/2+\mathrm{Log}(8\pi)-\gamma$ (γ constante d'Euler).

Pour x_0 réduit de longueur de période L égale à 2, 4 ou 6 admettant un des développements de la forme donnée au lemme ci-dessus, nous minorons maintenant l'expression $\sum\sqrt{k_i}\cdot(\mathrm{Log}(k_i)-\omega)$, où la somme porte sur les indices i variant de 0 à $L-1$ et où $k_i = x_i-x_i'$. Nous posons $\delta = \Delta/\alpha\beta$, $x = \beta/\alpha$ et remarquons que nous avons $k_0 = \sqrt{\Delta}/\beta = \sqrt{\delta/x}$, et $k_{L/2} = \sqrt{\Delta}/\alpha = \sqrt{\delta x}$ avec α et β supérieurs ou égaux à 1.

La fonction $f(x) = \sqrt{x}\cdot(\mathrm{Log}(x)-\omega)$ passant par son minimum $-2e^{(\omega-2)/2}$ pour $x = e^{\omega-2}$, la somme $\sum\sqrt{k_i}\cdot(\mathrm{Log}(k_i)-\omega)$ portant sur les indices i variant de 0 à $L-1$ et distincts de 0 et $L/2$ est donc minorée par $-2(L-2)e^{(\omega-2)/2}$.

Posons $f(x) = \sum\sqrt{k_i}\cdot(\mathrm{Log}(k_i)-\omega)$, où la somme porte sur les indices 0 et $L/2$; nous avons $f(x) = \sqrt{\delta/x}\cdot(\mathrm{Log}(\delta/x)-\omega)+\sqrt{\delta x}\cdot(\mathrm{Log}(\delta x)-\omega)$. Un calcul élémentaire donne $f'(x) = (1/2x)\cdot\sqrt{\delta/x}\cdot h(x)$ avec

$$h(x) = x\cdot(\mathrm{Log}(\delta x)-\omega+2)-(\mathrm{Log}(\delta/x)-\omega+2);$$

puis $h'(x) = \mathrm{Log}(\delta x)-\omega+3+1/x$ et $h''(x) = (x-1)/x$. Si δ est supérieur ou égal à $e^{\omega-4}$, soit $\delta \geqslant 2$, la fonction h est donc monotone strictement croissante de $-\infty$ à $+\infty$ lorsque x croit de 0 à $+\infty$ et s'annule une seule fois, et ce pour $x = 1$. f passe donc, sous la condition $\delta \geqslant 2$, par son minimum pour $x = 1$ et donc $f(x) \geqslant f(1) = 2\sqrt{\delta}\cdot(\mathrm{Log}(\delta)-\omega)$, pour $\delta \geqslant 2$.

Nous minorons donc par $2\sqrt{\delta}\cdot(\mathrm{Log}(\delta)-\omega)-2(L-2)e^{(\omega-2)/2}$ notre expression $\sum\sqrt{k_i}\cdot(\mathrm{Log}(k_i)-\omega)$ de départ, où la somme porte sur les indices variant de 0 à $L-1$. Cette minoration ne dépend que de δ, et donc que de Δ.

Si $\boldsymbol{I} = (Q, (P+\sqrt{D})/2)_{\boldsymbol{Z}}$ est un idéal réduit invariant d'une classe d'idéaux ambiges $\mathscr{C}$ d'un corps d'unité fondamentale de norme $+1$ de notre famille $(\mathscr{F})$, $\sqrt{D}/Q = x_0(\boldsymbol{I})-x_0(\boldsymbol{I})' = \sqrt{\Delta}/\beta$ et donc $D\beta^2 = d(D/d)\beta^2 = Q^2\Delta$. Il en résulte la divisibilité de $(D/d)\beta^2$ par Q^2 puis la majoration de d par Δ. Δ est lui majoré par $\delta(\delta+4)$. Posons $\delta_0 = \sqrt{d+4}-2$ et supposons d tel que $\delta_0 \geqslant e^{\omega-2}$ (soit $d \geqslant 122$), nous avons: $\zeta(1/2, \mathscr{C}) \geqslant 2\sqrt{\delta_0}\,(\mathrm{Log}(\delta_0)-\omega)-8e^{(\omega-2)/2}-0{,}12$ (L est majoré par 6). Cette minoration ne dépendant pas de la classe d'idéaux, nous obtenons, sous l'hypothèse de Riemann faible $\zeta_{\boldsymbol{Q}(\sqrt{d})/\boldsymbol{Q}}(1/2) \leqslant 0$, la majoration: $\mathrm{Log}(\delta_0) \leqslant \omega+(4e^{(\omega-2)/2}+0{,}06)/\sqrt{\delta_0}$. Cette inégalité implique $\delta_0 \leqslant 172$, puis $d \leqslant 30272$. Nous avons programmé sur calculatrice la recherche exhaustive de ces corps; d'où:

THÉORÈME 18. *Sous l'hypothèse de Riemann faible* $\zeta_{\boldsymbol{Q}(\sqrt{d})/\boldsymbol{Q}}(1/2) \leqslant 0$ *les corps quadratiques réels tels que* p *premier et* $p \leqslant (1/2)\sqrt{D}$ *impliquent* $\chi(p) \neq +1$ *vérifient* $d \leqslant 30272$. *Il y a* 60 *tel corps*:

(1) $N(\varepsilon_0) = -1$: $d = 2$, 5**([1]), 13, 29, 53, 173 et 293.

(2) $N(\varepsilon_0) = +1$ *et* $h(d) = 1$:

([1])* : d est de la forme m^2-1; ** : d est de la forme m^2-4.

(a) $d \equiv 1\ (4)$: $d = 3\times 7^{**}, 3\times 23, 7\times 11^{**}, 3\times 31, 3\times 71, 3\times 79, 7\times 59, 19\times 23^{**}, 3\times 151, 3\times 239, 3\times 359, 11\times 103$ *et* 7×179.

(b) $d \equiv 2, 3\ (4)$: $d = 3^{*}, 2\times 3, 7, 11, 2\times 7, 23, 2\times 19, 47, 2\times 31, 83, 167, 227$ *et* 2×199.

(3) $N(\varepsilon_0) = +1$ *et* $h(d) = 2$:

(a) $d \equiv 1\ (4)$: $d = 3\times 5\times 11^{**}, 3\times 5\times 19^{**}, 3\times 7\times 17^{**}, 3\times 11\times 29^{**}, 5\times 7\times 31^{**}, 3\times 5\times 131, 3\times 5\times 139$ *et* $3\times 17\times 47^{**}$.

(b) $d \equiv 2, 3\ (4)$: $d = 3\times 5^{*}, 2\times 3\times 5, 5\times 7^{*}, 2\times 3\times 7, 3\times 29, 2\times 5\times 11, 2\times 3\times 23, 11\times 13^{*}, 2\times 7\times 13, 5\times 43, 2\times 3\times 53, 3\times 149$ *et* 5×127.

(4) $N(\varepsilon_0) = +1$ *et* $h(d) = 4$:

$d \equiv 2, 3\ (4)$: $d = 3\times 5\times 13^{*}, 3\times 5\times 17^{*}, 3\times 7\times 23^{*}, 2\times 3\times 5\times 31, 5\times 7\times 37^{*}$ *et* $2\times 3\times 7\times 41$.

Références

[1] H. Amara, *Cycles canoniques d'idéaux réduits et nombres de classes de certains corps quadratiques réels*, Nagoya Math. J. 103 (1986), 127–132.

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

[3] A. Chatelet, *L'arithmétique des corps quadratiques*, L'enseignement des mathématiques, N° 9; Genève 1962.

[4] H. Hasse, *Vorlesungen über Zahlentheorie*, §16, Berechnung der Grundeinheit, Springer-Verlag, 1964.

[5] M. Kutsuna, *On a criterion for the class number of a quadratic number field to be one*, Nagoya Math. J. 79 (1980), 123–129.

[6] G. Lachaud, *Sur les corps quadratiques réels principaux*. Séminaire de théorie de nombres, Paris 1984–85, Progress in Mathematics, Vol. 63, p. 165–175.

[7] S. Louboutin, *Continued fractions and real quadratic fields*, J. Number Theory 3 (1988), 167–176.

[8] R. A. Mollin and H. C. Williams, *On prime valued polynomials and class number of real quadratic fields*, Research paper N° 653, July 1987; University of Calgary.

[9] — —*A conjecture of S. Chowla via the generalized Riemann hypothesis*, Proc. Amer. Math. Soc. 102 (1988), 794–796.

[10] R. A. Mollin, *Class number one criteria for real quadratic fields*, Proc. Japan Acad., Ser. A, 63 (1987), I, 121–125; II, 162–164.

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

UNIVERSITÉ PARIS VII
UER DE MATHÉMATIQUES ET INFORMATIQUE
UNITÉ ASSOCIÉE AU CNRS N°212
Tour 45 55, 5ème étage;
2 Place Jussieu
75251 Paris Cedex 05
France

Reçu le 3.2.1988
et dans la forme modifiée le 28.4.1988 (1782)

ACTA ARITHMETICA
LIV (1989)

Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique

par

ALAIN KRAUS (Paris)

A. Introduction. Soit K un corps de caractéristique nulle muni d'une valuation discrète v normalisée par $v(K^*) = \mathbf{Z}$.

On introduit les notations suivantes:

O_K l'anneau de valuation;

p la caractéristique résiduelle;

e la valuation de p.

À une équation de Weierstrass affine (W) à coefficients dans O_K:

$$(W) \qquad y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6,$$

on associe des invariants c_4, c_6 et Δ que l'on calcule par le procédé suivant [1]:

$$\begin{aligned}
b_2 &= a_1^2+4a_2,\\
b_4 &= a_1a_3+2a_4,\\
b_6 &= a_3^2+4a_6,\\
b_8 &= a_1^2a_6-a_1a_3a_4+4a_2a_6+a_2a_3^2-a_4^2,\\
c_4 &= b_2^2-24b_4,\\
c_6 &= -b_2^3+36b_2b_4-216b_6,\\
\Delta &= -b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6.
\end{aligned}$$

Ces grandeurs sont reliées par:

$$4b_8 = b_2b_6-b_4^2, \qquad 1728\Delta = c_4^3-c_6^2.$$

La cubique définie par l'équation (W) est non singulière si et seulement si Δ est non nul.

Étant donnés des éléments c_4, c_6 et Δ de O_K satisfaisant à

$$(*) \qquad c_4^3-c_6^2 = 1728\Delta \quad \text{et} \quad \Delta \neq 0$$

on se propose de déterminer des conditions nécessaires et suffisantes simples pour que c_4, c_6 et Δ puissent être réalisés comme les invariants $c_4(W)$, $c_6(W)$ et $\Delta(W)$ d'une équation de Weierstrass (W) définie sur O_K. Si tel est le cas, on écrira $c_4 = c_4(W)$, $c_6 = c_6(W)$, $\Delta = \Delta(W)$.