

IDÉAUX NÉGATIVEMENT RÉDUITS D'UN CORPS QUADRATIQUE RÉEL ET UN PROBLÈME D'EISENSTEIN

Autor(en): **Kaplan, Pierre / LEONARD, Philip A.**

Objektyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **39 (1993)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **19.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-60422>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

IDÉAUX NÉGATIVEMENT RÉDUITS D'UN CORPS QUADRATIQUE RÉEL ET UN PROBLÈME D'EISENSTEIN

par Pierre KAPLAN et Philip A. LEONARD

§ 1. INTRODUCTION

Le problème d'Eisenstein [1] dont il sera question ici est la détermination des entiers positifs $D \equiv 5 \pmod{8}$ tels que l'équation

$$(1.1) \quad X^2 - DY^2 = 4$$

a des solutions impaires. Si l'équation

$$(1.2) \quad T^2 - DU^2 = -4$$

a des solutions entières, les longueurs l_0 et l_0^* des périodes des développements en fraction continue de \sqrt{D} et $(1 + \sqrt{D})/2$ respectivement sont des nombres impairs et l'on sait ([6]) que, alors, (1.1) a des solutions impaires si, et seulement si,

$$(1.3) \quad l_0 \equiv l_0^* \pmod{4} .$$

Récemment Y. Mimura ([9]) a eu l'idée très intéressante et originale d'introduire le développement négatif en fraction continue de nombres irrationnels quadratiques réels et les périodes de ceux qui sont négativement réduits pour montrer que l'équation (1.1) a des solutions impaires si, et seulement si,

$$(1.4) \quad l_{0-} = 3l_{0-}^* + \frac{l_0^*}{k}$$

où l_{0-} et l_{0-}^* sont les longueurs des périodes négatives de \sqrt{D} et $(1 + \sqrt{D})/2$ respectivement, et $k = 1$ ou 2 suivant que (1.2) a, ou non, des solutions.

En fait, la condition (1.3) avait été généralisée et pouvait être remplacée ([4]) par

$$(1.5) \quad l \equiv l^* \pmod{4}$$

où l est la longueur de la période d'une classe ambige de discriminant $4D$ et l^* celle de son image par l'homomorphisme θ du groupe des classes de discriminant $4D$ sur le groupe des classes de discriminant D défini dans [7]. La définition de θ est rappelée ci-dessous (Lemme 4).

Le but de ce travail est de montrer comment la méthode de [7], c'est-à-dire l'utilisation des idéaux des anneaux O_D et O_{4D} , permet de généraliser la condition (1.4) de manière analogue à (1.5), et ceci tout en mettant bien en évidence l'intérêt du développement négatif en fraction continue introduit par Mimura [9]. Nous prouvons le résultat suivant:

THÉORÈME 1. *Soit D un nombre positif, congru à 5 modulo 8. Soit C une classe d'idéaux au sens strict de l'ordre O_{4D} et $\theta(C)$ son image par l'homomorphisme θ . Soit l_- (respectivement l_-^*) le nombre des idéaux primitifs négativement réduits de C (respectivement de $\theta(C)$) et l^* le nombre des idéaux primitifs réduits de $\theta(C)$. Alors l'équation (1.1) a des solutions impaires si, et seulement si,*

$$(1.6) \quad l_- = 3l_-^* + l^* .$$

Dans la section suivante (§2) nous allons rappeler ou définir les notions intervenant dans l'énoncé du Théorème 1 et exposer la théorie des idéaux négativement réduits et de leurs périodes, pour laquelle il ne semble pas exister de référence accessible.

Dans la troisième section nous prouvons le Théorème 1 après avoir prouvé deux résultats (Théorèmes 2 et 3) permettant de relier les nombres des idéaux primitifs négativement réduits de O_{4D} et O_D avec le nombre des idéaux primitifs réduits de O_D .

Nous terminons en donnant des exemples numériques (§4).

§2. CLASSES D'IDÉAUX AU SENS STRICT ET RÉDUCTION NÉGATIVE

Soit $\Delta > 0$ un discriminant. Il existe un discriminant fondamental D_0 et un entier f positif tels que $\Delta = D_0 f^2$. Soit O_{D_0} l'anneau des entiers de $Q(\sqrt{D_0})$ et O_Δ l'anneau des entiers de conducteur f . Les *idéaux primitifs* de

l'anneau O_Δ sont les \mathbf{Z} -modules $I = \left[a, \frac{b + \sqrt{\Delta}}{2} \right]$ tels que

$$(2.1) \quad a > 0, \quad \frac{b^2 - \Delta}{4a} = c \in \mathbf{Z}, \quad (a, b, c) = 1,$$

c'est-à-dire $I = a[1, \varphi]$ où $\varphi = \frac{b + \sqrt{\Delta}}{2a}$ est déterminé modulo 1 et vérifie (2.1).

Nous dirons que l'idéal I et le nombre φ sont *associés*.

Soit α un nombre non nul de $Q(\sqrt{D_0})$. Nous désignerons par $\bar{\alpha}$ le conjugué $x - y\sqrt{D_0}$ de $\alpha = x + y\sqrt{D_0}$ où x, y sont des nombres rationnels. La proposition suivante permet de définir le discriminant de α .

PROPOSITION 1. Soit α un nombre non nul de $Q(\sqrt{D_0})$. Il existe des entiers $f > 0, a > 0, b$ tels que $\alpha = \frac{b + f\sqrt{D_0}}{2a}$ où a et b vérifient (2.1) avec $\Delta = f^2 D_0$. Les nombres f, a et b sont déterminés par α .

DÉFINITION. Le nombre $\Delta = f^2 D_0$ est le discriminant de α .

Pour prouver la proposition 1, nous nous appuyerons sur le lemme suivant:

LEMME 1. Soient $\alpha = \frac{x + y\sqrt{D_0}}{z} = \frac{X + Y\sqrt{D_0}}{Z}$, avec $(x, y, z) = 1$ et $z, Z > 0$. Alors il existe un entier $h > 0$ tel que $X = hx, Y = hy, Z = hz$.

Démonstration. Posons $x = d'x', z = d'z' = d''z'', y = d''y''$ avec $(x', z') = (y'', z'') = (d', d'') = 1$, et d' et $d'' > 0$. Alors on voit qu'il existe $k > 0$ tel que $z' = kd'', z'' = kd'$ d'où $z = kd'd''$.

D'autre part on a $xZ = zX$ et $yZ = zY$ d'où $x'Z = kd''X$ et $y''Z = kd'Y$. Comme $(x', kd'') = (y'', kd') = 1$ on voit qu'il existe des entiers X' et Y'' tels que $X = x'X'$ et $Y = y''Y''$, d'où résulte $Z = kd''X' = kd'Y''$. Comme $(d', d'') = 1$ on voit qu'il existe h tel que $X' = hd', Y'' = hd''$ ce qui donne $X = hd'x', Y = hd''y'', Z = hkd'd''$, ce qu'il fallait prouver.

Démonstration de la proposition 1

D'après le lemme 1 les entiers $2a, f$ et b sont à chercher parmi les nombres hz, hy et hx , et il suffit de montrer qu'il existe un et un seul entier $h > 0$ tel que

$$(2.2) \quad h \frac{D_0 y^2 - x^2}{2z} = c \in \mathbf{Z}, \quad (hz, 2hy, 2c) = 2.$$

Posons $\frac{D_0 y^2 - x^2}{2z} = \frac{r}{s}$ avec $s > 0$ et $(r, s) = 1$. Les solutions de la première égalité (2.2) sont $h = ks$ et alors $c = kr$, où, d'après la seconde égalité (2.2), k est déterminé par $(ks, 2ksy, 2kr) = 2$. Si un nombre premier p divisait sz ,

sy et r, il diviserait y, z et $D_0y^2 - x^2$, donc x, y et z, ce qui n'est pas possible. Donc si sz est pair, la valeur de k qui convient est 1 et, si sz est impair, la valeur de k qui convient est $k = 2$. Ceci achève de prouver la proposition 1.

De la proposition 1 résulte immédiatement le résultat suivant

COROLLAIRE 1. *Les nombres associés aux idéaux primitifs de l'anneau O_Δ sont les nombres de discriminant Δ .*

Deux idéaux $I = a[1, \varphi]$ et $J = b[1, \psi]$ sont dits *équivalents au sens strict* s'il existe $\rho \in \mathcal{Q}(\sqrt{D_0})$ tel que $N(\rho) > 0$ et $J = \rho I$. D'après [7], Proposition 3, c'est le cas si, et seulement si, il existe $p, q, r, s \in \mathbf{Z}$ tels que $ps - qr = 1$ et $\psi = \frac{p\varphi + q}{r\varphi + s}$. On dit alors que φ et ψ sont strictement

équivalents. L'équivalence stricte implique l'équivalence usuelle, et l'on sait qu'un idéal $J = b[1, \psi]$ équivalent à un idéal $I = a[1, \varphi]$ primitif de O_Δ est un idéal primitif de O_Δ ([7], Corollary 3); ceci montre que le discriminant d'un nombre est conservé par équivalence.

L'ensemble des classes d'équivalence d'idéaux pour l'équivalence stricte contenant des idéaux primitifs forme un groupe fini C_Δ^+ pour la multiplication induite par la multiplication des idéaux, isomorphe au groupe des classes de formes quadratiques binaires primitives de discriminant Δ pour la composition.

Passons maintenant à la réduction. Un nombre φ de discriminant Δ est dit *réduit* si

$$(2.3) \quad -1 < \bar{\varphi} < 0, \quad 1 < \varphi,$$

négativement réduit si

$$(2.4) \quad 0 < \bar{\varphi} < 1 < \varphi.$$

L'idéal $I = a[1, \varphi]$ est dit *réduit* (respectivement *négativement réduit*) si l'on peut choisir φ modulo 1 de manière à vérifier (2.3) (respectivement 2.4). Alors on voit que

PROPOSITION 2. *Tout idéal réduit est négativement réduit.*

Démonstration. Soit $I = a[1, \varphi]$ où φ vérifie (2.3). Alors $I = a[1, \varphi + 1]$ où $\varphi + 1$ vérifie (2.4).

Plus généralement on a

LEMME 2. *L'idéal $I = a[1, \varphi]$ est réduit si, et seulement si, $\varphi + [-\bar{\varphi}] > 1$, négativement réduit si, et seulement si, $\varphi + [-\bar{\varphi}] > 0$.*

Démonstration. Il suffit de remarquer que, pour tout nombre réel φ non entier on a $-1 < \bar{\varphi} + [-\bar{\varphi}] < 0$ et $0 < \bar{\varphi} + [-\bar{\varphi}] + 1 < 1$.

Tout idéal primitif réduit (respectivement négativement réduit) I de O_Δ s'écrit de *manière unique* $I = a[1, \varphi]$ où φ est un nombre réduit (respectivement négativement réduit) de $Q(\sqrt{D_0})$ de discriminant Δ . Nous dirons que l'idéal I et le nombre φ sont *associés*.

Il est bien connu que le nombre des idéaux réduits primitifs de O_Δ est fini. La proposition suivante montre qu'il en est de même pour les idéaux négativement réduits.

PROPOSITION 3. *L'ensemble des nombres négativement réduits de discriminant Δ donné est un ensemble fini. Le nombre des idéaux négativement réduits primitifs de O_Δ est fini.*

Démonstration. Pour montrer les deux assertions de la Proposition 3, il suffit de montrer que le nombre des solutions (b, a, c) de

$$(2.5) \quad 0 < \frac{b - \sqrt{\Delta}}{2a} < 1 < \frac{b + \sqrt{\Delta}}{2a}, \quad b^2 = \Delta + 4ac$$

est fini. Comme (2.5) implique

$$(2.6) \quad 0 < b - \sqrt{\Delta} < 2a, \quad 2c < b + \sqrt{\Delta}$$

nous posons $2a = b - \alpha$, $2c = b - \alpha'$; alors $b^2 = \Delta + 4ac$ entraîne

$$(2.7) \quad \Delta + \alpha\alpha' = b(\alpha + \alpha').$$

D'après (2.6) on a $b > \sqrt{\Delta} > |\alpha|, |\alpha'|$. De plus $\alpha \equiv \alpha' \equiv b \equiv \Delta \pmod{2}$, donc $\alpha + \alpha' \equiv 0 \pmod{2}$, et $\alpha + \alpha' \geq 2$.

Si $\alpha\alpha' = 0$ alors Δ est pair et (2.7) montre que $\Delta \equiv 0 \pmod{2b}$ donc $b \leq \frac{\Delta}{2}$.

Si $\alpha\alpha' > 0$ alors $\Delta < \Delta + \alpha\alpha' = b(\alpha + \alpha') < 2\Delta$. Donc α et $\alpha' > 0$.

Si $\alpha = \alpha' = 1$ alors $b = \frac{\Delta + 1}{2}$; sinon $\alpha + \alpha' \geq 4$ donc $b < \frac{\Delta}{2}$.

Si $\alpha\alpha' < 0$ alors $0 < \Delta + \alpha\alpha' = b(\alpha + \alpha') < \Delta$, donc $b < \frac{\Delta}{2}$.

Ainsi $\sqrt{\Delta} < b \leq \frac{\Delta}{2}$ si Δ est pair, $\sqrt{\Delta} < b \leq \frac{\Delta + 1}{2}$ si Δ est impair, ce

qui prouve que le nombre des b , et par suite celui des triplets (b, c, a) , satisfaisant à (2.5) est fini. Ceci termine la démonstration de la proposition 3.

Considérons maintenant le processus de réduction négative.

Soit $\varphi_0 = \frac{b_0 + \sqrt{\Delta}}{2a_0}$ ($a_0 > 0$) un nombre de discriminant Δ . Supposons φ_n défini; nous définissons φ_{n+1} par

$$(2.8) \quad q_n = [\varphi_n + 1], \quad \varphi_n = q_n - \frac{1}{\varphi_{n+1}}.$$

On voit que φ_{n+1} est strictement équivalent à φ_n et que $\varphi_n > 1$ et $q_n \geq 2$ pour $n \geq 1$. De plus on a

$$(2.9) \quad \varphi_0 = q_0 - \frac{1}{q_1 - \frac{1}{q_2 - \dots - \frac{1}{q_n - \frac{1}{\varphi_{n+1}}}}}$$

Inversement φ_0 étant donné la condition $\varphi_n > 1$ ($n \geq 1$) et (2.9) définissent les q_i de manière unique.

Si φ_n est négativement réduit alors $0 < \bar{\varphi}_n < 1$ donc, comme $q_n \geq 2$, on a $0 < \bar{\varphi}_{n+1} < 1$ ce qui montre que φ_{n+1} est négativement réduit.

Au nombre $\varphi_n = \frac{b_n + \sqrt{\Delta}}{2a_n}$ ($a_n > 0$) est associé l'idéal I_n tel que

$$I_n = a_n [1, \varphi_n] = \left[a_n, \frac{b_n + \sqrt{\Delta}}{2} \right],$$

et tous les idéaux I_n sont *strictement* équivalents entre eux.

Comme (Proposition 3) le nombre des nombres négativement réduits de discriminant Δ est fini on voit, comme dans la théorie des idéaux réduits, que les nombres φ négativement réduits de discriminant Δ , ainsi que les idéaux I associés se répartissent en un nombre fini de périodes.

Définissons maintenant deux suites d'entiers A_n et B_n ($n \geq -2$) par

$$(2.10) \quad \begin{cases} A_{-2} = 0, & A_{-1} = +1, & A_n = q_n A_{n-1} - A_{n-2}, \\ B_{-2} = -1, & B_{-1} = 0, & B_n = q_n B_{n-1} - B_{n-2}. \end{cases}$$

On vérifie par récurrence sur n les relations suivantes

$$(2.11) \quad \varphi_n = \frac{B_{n-2} \varphi_0 - A_{n-2}}{B_{n-1} \varphi_0 - A_{n-1}}, \quad \varphi_0 = \frac{A_{n-1} \varphi_n - A_{n-2}}{B_{n-1} \varphi_n - B_{n-2}}, \quad (n \geq 0),$$

$$(2.12) \quad A_n B_{n-1} - A_{n-1} B_n = -1, \quad (n \geq -1),$$

$$(2.13) \quad \varphi_1 \cdots \varphi_n = B_{n-1} \varphi_n - B_{n-2}, \quad (n \geq 1),$$

$$(2.14) \quad B_n \geq B_{n-1} + 1 \geq 1, \quad \text{d'où } B_n \geq n + 1, \quad (n \geq 0),$$

$$(2.15) \quad A_n - \varphi_0 B_n = \frac{-1}{B_n \varphi_{n+1} - B_{n-1}}.$$

Définissons le nombre θ_n par

$$(2.16) \quad \theta_n = \varphi_1 \cdots \varphi_n.$$

Nous pouvons maintenant montrer, avec les notations qui précèdent, la

PROPOSITION 4. *Pour n assez grand le nombre φ_n et l'idéal I_n sont négativement réduits. Le nombre θ_n tend vers $+\infty$ quand n tend vers $+\infty$.*

Démonstration. Soit $\varphi_0 = \frac{b_0 + \sqrt{\Delta}}{2a_0}$ avec $a_0 > 0$. Nous avons

$$\varphi_1 = \frac{1}{q_0 - \varphi_0} > 1 \quad \text{et} \quad \bar{\varphi}_1 = \frac{1}{q_0 - \varphi_0 + (\varphi_0 - \bar{\varphi}_0)}, \quad \text{donc} \quad 0 < \bar{\varphi}_1 < \varphi_1.$$

Remplaçant φ_0 par φ_1 si nécessaire nous pouvons supposer $0 < \bar{\varphi}_0 < \varphi_0$. De (2.11) et (2.12) on déduit

$$\varphi_0 - \bar{\varphi}_0 = \frac{\varphi_n - \bar{\varphi}_n}{(B_{n-1} \varphi_n - B_{n-2})(B_{n-1} \bar{\varphi}_n - B_{n-2})}$$

Supposons $\bar{\varphi}_n > 1$. D'après (2.14) on a $B_{n-1} \bar{\varphi}_n - B_{n-2} > 1$ et $B_{n-1} \geq B_{n-2} + 1$, donc

$$\varphi_0 - \bar{\varphi}_0 < \frac{\varphi_n - 1}{B_{n-1} \varphi_n - B_{n-1} + 1} = \frac{1}{B_{n-1} + \frac{1}{\varphi_n - 1}} < \frac{1}{B_{n-1}} \leq \frac{1}{n}$$

ce qui n'est pas possible pour n assez grand donc il existe n_0 tel que, à partir de n_0 , φ_n est négativement réduit.

Pour montrer que $\theta_n \rightarrow +\infty$ quand $n \rightarrow +\infty$, il suffit de remarquer que $\varphi_i > 1$ pour $i \geq 1$ et que φ_i ne prend qu'un nombre fini de valeurs pour $i \geq n_0$. Ceci achève de prouver la Proposition 4.

L'étape suivante consiste à montrer que deux nombres strictement équivalents négativement réduits sont dans la même période négative. Nous adaptions le raisonnement classique (voir par exemple [3] §10-6, 10-10, 10-11

ou [11] §29) à notre objet en nous référant à [11], Satz 5.2, qui dit que chaque nombre réel a un développement en fraction continue négative bien déterminé. Nous commençons par le

LEMME 3. Si $\varphi_0 = \frac{P\psi - Q}{R\psi - S}$ avec $PS - QR = -1$, $R > S > 0$, et $\psi > 1$ alors il existe n tel que $\psi = \varphi_n$.

Démonstration. Nous appliquons le processus (2.8), (2.9) au nombre rationnel $\frac{P}{R} = \varphi'_0$. Dans ce cas (2.8) s'écrit successivement

$$P = q'_0 R - r_1, \quad \varphi'_0 = \frac{P}{R}, \quad q'_0 = \left[\frac{P}{R} + 1 \right], \quad 0 \leq r_1 < R,$$

$$R = q'_1 r_1 - r_2, \quad \varphi'_1 = \frac{R}{r_1}, \quad q'_1 = [\varphi'_1 + 1] \geq 2, \quad 0 \leq r_2 < r_1,$$

.....

$$r_{n-1} = q'_n r_n - r_{n+1}, \quad \varphi'_n = \frac{r_{n-1}}{r_n}, \quad q'_n = [\varphi'_n + 1] \geq 2, \quad 0 \leq r_{n+1} < r_n,$$

.....

$$r_{N-1} = q'_N r_n - r_{n+1}, \quad \varphi'_N = \frac{r_{N-1}}{r_N} = q'_N, \quad q'_N = [\varphi'_N + 1] \geq 2, \quad r_{N+1} = 0.$$

Le fait qu'il existe N tel que $r_{N+1} = 0$ vient de ce que la suite des entiers positifs r_i est strictement décroissante. Tenant compte de (2.11) et (2.10) il vient

$$\frac{P}{R} = \frac{A_{N-1} q'_N - A_{N-2}}{B_{N-1} q'_N - B_{N-2}} = \frac{A_N}{B_N},$$

puis, comme $(P, R) = (A_N, B_N) = 1$, R et $B_N > 0$ on voit que $P = A_N$, $R = B_N$ d'où $-1 = PS - RQ = PB_{N-1} - RA_{N-1}$, donc $P(S - B_{N-1}) = R(Q - A_{N-1})$.

Comme $(P, R) = 1$, R divise $S - B_{N-1}$, ce qui n'est possible que si $S = B_{N-1}$ car $0 < S < R$ et $0 \leq B_{N-1} < B_N = R$. Donc on a:

$$\varphi_0 = \frac{A_N \psi - A_{N-1}}{B_N \psi - B_{N-1}}.$$

Ceci s'écrit

$$\varphi_0 = q'_0 - \frac{1}{q'_1 - \frac{1}{q'_2 - \dots - \frac{1}{q'_N - \frac{1}{\psi}}}}$$

c'est-à-dire (2.9) pour $N = n$ où q_i est remplacé par q'_i et φ_{N+1} par ψ . En développant ψ en fraction continue négative on trouve le développement de φ_0 en fraction continue négative ([11], Satz 5.2), donc $q'_i = q_i$ et $\psi = \varphi_{N+1}$, ce qui démontre le lemme 3.

PROPOSITION 5. *Deux nombres négativement réduits strictement équivalents sont dans la même période.*

Démonstration. Supposons $\psi = \frac{a\varphi - b}{c\varphi - d}$ avec a, b, c, d entiers tels que $ad - bc = -1$, où nous pouvons supposer $c\varphi - d > 0$ en changeant, si nécessaire, les signes de a, b, c et d . Développons $\varphi = \varphi_0$ en fraction continue négative et remplaçons; il vient

$$\psi = \frac{P\varphi_n - Q}{R\varphi_n - S} \text{ avec } R = cA_{n-1} - dB_{n-1}, S = cA_{n-2} - dB_{n-2}.$$

D'après (2.13) et (2.15) on a $A_{n-1} = \varphi B_{n-1} - \frac{1}{\theta_{n-1}}$, $A_{n-2} = \varphi B_{n-2} - \frac{1}{\theta_{n-2}}$, d'où

$$R = B_{n-1}(c\varphi - d) - \frac{c}{\theta_{n-1}}, S = B_{n-2}(c\varphi - d) - \frac{c}{\theta_{n-2}}.$$

Comme $B_{n-1} \geq n$, $B_{n-2} \geq n - 1$, $B_{n-1} \geq B_{n-2} + 1$ et que θ_{n-1} et $\theta_{n-2} \rightarrow +\infty$ quand $n \rightarrow +\infty$, on voit que pour n assez grand $R > S > 0$ ce qui, d'après le Lemme 3, montre que φ_n est dans la période de ψ et prouve la Proposition 5.

§3. L'HOMOMORPHISME θ ET L'APPLICATION ψ

Soit C_Δ le groupe des classes d'idéaux au sens usuel de l'anneau O_Δ . L'homomorphisme θ de C_{Df^2} sur C_D défini et étudié dans [7], §3 est en fait un homomorphisme des groupes des classes d'idéaux au sens strict, de $C_{Df^2}^+$ sur C_D^+ . On vérifie que le Theorem 1 et le Corollary 4 de [7] soient vrais si l'on remplace classe par classe au sens strict et équivalence par équivalence au sens strict: pour adapter la démonstration du Théorème 1 il suffit de ne considérer que des substitutions linéaires de déterminant $+1$ (pages 333-334), et pour celle du Corollary 4 il suffit de remarquer que, avec les notations de [7], page 335,

$$N\left(\frac{\sqrt{D'} - b}{2a}\right) \cdot N\left(\frac{-\frac{b}{f} + \sqrt{D}}{2c}\right) > 0.$$

A partir de maintenant nous considérons le cas où $D \equiv 1 \pmod{4}$ et $f = 2$.

LEMME 4. *Un idéal primitif de O_{4D} s'écrit $I = [a, b + \sqrt{D}]$ avec $b \equiv 1 \pmod{2}$, et soit $a \equiv 1 \pmod{2}$, soit $a \equiv 0 \pmod{4}$. Si C est la classe au sens strict de I , la classe $\theta(C)$ contient l'idéal $\theta(I)$ où $\theta(I)$ est défini par*

$$(3.1) \quad \theta(I) = \begin{cases} \left[a, \frac{b + \sqrt{D}}{2} \right], & \text{si } a \equiv 1 \pmod{2}, \\ \left[\frac{a}{4}, \frac{b + \sqrt{D}}{2} \right], & \text{si } a \equiv 0 \pmod{4}, \end{cases}$$

Démonstration. Soit $I = [a, b' + \sqrt{D}]$ un idéal primitif de O_{4D} . On a donc $D = b'^2 - ac$. Si b' est pair alors a est impair, donc $I = [a, b' + a + \sqrt{D}]$, donc on peut toujours supposer $I = [a, b + \sqrt{D}]$ avec b impair. Alors $ac \equiv 0 \pmod{4}$ et, comme $(a, 2b, c) = 1$, on voit que: soit $a \equiv 1 \pmod{2}$, $c \equiv 0 \pmod{4}$, soit $a \equiv 0 \pmod{4}$, $c \equiv 1 \pmod{2}$.

Le fait que $\theta(I) \in \theta(C)$ est une conséquence immédiate de [7] Theorem 1 et Corollary 4.

Nous supposons toujours $b \equiv 1 \pmod{2}$ dans l'écriture $I = [a, b + \sqrt{D}]$ d'un idéal primitif de O_{4D} et nous poserons $I = a[1, \varphi]$ avec $\varphi = \frac{b + \sqrt{D}}{a}$

où φ est défini modulo 1.

Soit I associé à φ un idéal de O_Δ ($\Delta = D$ ou $4D$). Nous noterons I' et φ' l'idéal et le nombre associés obtenus à partir de I et φ par une étape de réduction négative, c'est-à-dire $\varphi' = \frac{1}{[\varphi + 1] - \varphi}$. Nous avons

PROPOSITION 6. *Soit $I = a[1, \varphi]$ un idéal primitif négativement réduit de O_{4D} . Si $a \equiv 1 \pmod{2}$ et si $\theta(I)$ n'est pas négativement réduit alors $(\theta(I))'$ est négativement réduit. Si $a \equiv 0 \pmod{4}$, $\theta(I)$ est négativement réduit.*

Démonstration. D'après le Lemme 2 on a $\varphi + [-\bar{\varphi}] > 0$. Si $a \equiv 1 \pmod{2}$, $\theta(I) = a \left[1, \frac{\varphi}{2} \right]$ est négativement réduit si, et seulement si, $\frac{\varphi}{2} + \left[\frac{-\bar{\varphi}}{2} \right] > 0$. Si $\theta(I)$ n'est pas négativement réduit on a simultanément

$$(3.2) \quad \varphi + [-\bar{\varphi}] > 0, \quad \varphi + 2 \left[\frac{-\bar{\varphi}}{2} \right] < 0$$

d'où, comme $[-\bar{\varphi}] > 2 \left[\frac{-\bar{\varphi}}{2} \right]$, on voit que $[-\bar{\varphi}] = 2 \left[\frac{-\bar{\varphi}}{2} \right] + 1$ et

$$(3.3) \quad \frac{1}{2} < \frac{-\bar{\varphi}}{2} - \left[\frac{-\bar{\varphi}}{2} \right] < 1.$$

Des inégalités (3.2) on déduit aussi $-\left[\frac{-\bar{\varphi}}{2} \right] - \frac{1}{2} < \frac{\varphi}{2} < -\left[\frac{-\bar{\varphi}}{2} \right]$ d'où

$$(3.4) \quad \left[\frac{\varphi}{2} + 1 \right] = -\left[\frac{-\bar{\varphi}}{2} \right] \text{ avec } 0 < \left[\frac{\varphi}{2} + 1 \right] - \frac{\varphi}{2} < \frac{1}{2}.$$

Pour vérifier que $\theta(I)'$ est négativement réduit il suffit de voir que

$$\frac{1}{\left[\frac{\varphi}{2} + 1 \right] - \frac{\varphi}{2}} + \left[\frac{-1}{-\left[\frac{-\bar{\varphi}}{2} \right] - \frac{\bar{\varphi}}{2}} \right] > 0$$

ce qui résulte de (3.3) et (3.4).

Si $a \equiv 0 \pmod{4}$, $\theta(I) = \frac{a}{4}[1, 2\varphi]$ est négativement réduit, car $2\varphi + [-2\bar{\varphi}] \geq 2\varphi + 2[-\bar{\varphi}] > 0$. Ceci achève de prouver la proposition 6.

Soit maintenant E l'ensemble des idéaux négativement réduits de O_{4D} . Nous considérons la partition suivante de E en trois sous-ensembles E_1, E_2, E_3 . Soit $I = a[1, \varphi]$ un idéal primitif de O_{4D} , négativement réduit. Alors

$$\begin{aligned} I \in E_1 & \text{ si } a \equiv 1 \pmod{2} \text{ et } \theta(I) \text{ est négativement réduit,} \\ I \in E_2 & \text{ si } a \equiv 1 \pmod{2} \text{ et } \theta(I) \text{ n'est pas négativement réduit,} \\ I \in E_3 & \text{ si } a \equiv 0 \pmod{4}. \end{aligned}$$

Soit E^* l'ensemble des idéaux négativement réduits de O_D . Nous définissons une application ψ de E dans E^* de la manière suivante:

$$\begin{aligned} \psi(I) &= \theta(I), & \text{si } I \in E_1, & \text{ ou } I \in E_3, \\ \psi(I) &= (\theta(I))', & \text{si } I \in E_2, \end{aligned}$$

de sorte que $\psi(I) \in \theta(C)$, où C désigne la classe de I .

Les propositions suivantes ne sont vraies que si $D \equiv 5 \pmod{8}$. Ce qui distingue ce cas est que, si $D \equiv 5 \pmod{8}$, pour tout idéal $J = \left[a, \frac{b + \sqrt{D}}{2} \right]$ on a $a \equiv c \equiv 1 \pmod{2}$.

PROPOSITION 7. *Si $D \equiv 5 \pmod{8}$ la restriction de ψ à E_3 est surjective. L'image réciproque d'un idéal $J \in E^*$ a deux éléments si J est réduit, un seul si J n'est que négativement réduit.*

Démonstration. Soit $J = a[1, \omega]$ un élément de E^* . On peut supposer $0 < \bar{\omega} < 1 < \omega$. Les idéaux de $\psi^{-1}(J)$ appartenant à E_3 sont à chercher parmi les idéaux $4a \left[1, \frac{\omega + k}{2} \right]$ où $k \in \mathbf{Z}$, c'est-à-dire parmi les idéaux $I_1 = 4a \left[1, \frac{\omega}{2} \right]$ et $I_2 = 4a \left[1, \frac{\omega + 1}{2} \right]$. Les idéaux I_1 et I_2 sont primitifs et I_2 est négativement réduit alors que I_1 l'est si, et seulement si, $\omega > 2$ ce qui signifie que J est réduit.

PROPOSITION 8. *Si $D \equiv 5 \pmod{8}$ les restrictions de ψ à E_1 et à E_2 sont des bijections de E_i ($i = 1, 2$) sur E^* .*

Démonstration. Soit ψ_1 la restriction de ψ à E_1 , et soit $J = a[1, \omega] \in E^*$. On a $\omega + [-\bar{\omega}] > 0$, donc $I = a[1, 2\omega]$ est négativement réduit et, comme $a \equiv 1 \pmod{2}$, on a $\theta(I) = J$ et $I \in E_1$, ce qui montre que ψ_1 est surjective. Soit $I_1 = a_1[1, \varphi_1]$ un idéal de E_1 tel que $\psi_1(I_1) = J$; alors

$\theta(I_1) = a_1 \left[1, \frac{\varphi_1}{2} \right] = J$, d'où $a_1 = a$ et $\varphi_1 \equiv 2\omega \pmod{2}$, ce qui montre que $I_1 = I$ et que ψ_1 est injective.

Considérons maintenant la restriction ψ_2 de ψ à E_2 . Soit J un idéal de E^* et ω le nombre négativement réduit associé à J . Les idéaux J_- donnant J par une étape de réduction négative sont définis par les nombres $\frac{-1}{\omega + n}$ ($n \in \mathbf{Z}$).

Comme $\frac{-2}{\omega + n}$ est un nombre de discriminant $4D$, les idéaux $\psi_2^{-1}(J)$ sont,

parmi les idéaux définis par les nombres $\frac{-2}{\omega + n}$ ($n \in \mathbf{Z}$), ceux qui sont négativement réduits sans que J_- le soit, ce qui se traduit par

$$\frac{-1}{\omega + n} + \left[\frac{1}{\bar{\omega} + n} \right] < 0, \quad \frac{-2}{\omega + n} + \left[\frac{2}{\bar{\omega} + n} \right] > 0$$

d'après le lemme 2, c'est-à-dire

$$(3.5) \quad 2 \left[\frac{1}{\bar{\omega} + n} \right] < \frac{2}{\omega + n} < \left[\frac{2}{\bar{\omega} + n} \right].$$

Tenant compte de ce que $0 < \bar{\omega} < 1 < \omega$, on vérifie que $n = 1$ est la seule valeur de n qui satisfait (3.5), ce qui montre que ψ_2 est bijective et achève de prouver la proposition 8.

Des propositions 7 et 8 résulte immédiatement le résultat suivant:

THÉORÈME 2. *Soit $D \equiv 5 \pmod{8}$ un discriminant > 0 . Soit N_- le nombre des idéaux primitifs négativement réduits de O_{4D} , et soient N_-^* et N^* respectivement le nombre des idéaux primitifs négativement réduits et réduits de O_D . Alors*

$$(3.6) \quad N_- = 3N_-^* + N^* .$$

L'application ψ étant compatible avec l'homomorphisme θ le résultat plus précis suivant est vrai.

THÉORÈME 3. *Soit $D \equiv 5 \pmod{8}$ un discriminant > 0 . Soit C^* une classe d'idéaux au sens strict de O_D et $\theta^{-1}(C^*)$ son image inverse par θ . Soit L_- le nombre des idéaux primitifs négativement réduits de $\theta^{-1}(C^*)$ et soient L_-^* et L^* le nombre des idéaux primitifs respectivement négativement réduits et réduits de C^* . Alors:*

$$(3.7) \quad L_- = 3L_-^* + L^* .$$

Nous pouvons maintenant prouver le Théorème 1. On sait que

$$(3.8) \quad \text{Card}(\text{Ker } \theta) = \begin{cases} 3, & \text{si (1.1) n'a pas de solution impaire,} \\ 1, & \text{si (1.1) a des solutions impaires.} \end{cases}$$

Ce résultat était déjà connu de Gauss ([2], §256, VI); d'autres démonstrations se trouvent dans [8], §151 et [5], page 172.

Le Théorème 1 est une conséquence immédiate de (3.7) et (3.8).

Remarque. Les résultats analogues aux Théorèmes 2 et 3 quand $D \equiv 1 \pmod{8}$ seront exposés dans un article ultérieur.

§4. EXEMPLES NUMÉRIQUES

a) THÉORÈME 2.

Nous donnons les valeurs de N_- , N_* et N^* pour tous les $D \equiv 5 \pmod{8}$ de 5 à 109, et pour 141 et 165 que nous étudierons en b).

D	N_-	N_*	N^*
5	4	1	1
13	10	3	1
21	14	4	2
29	16	5	1
37	24	7	3
45	20	6	2
53	22	7	1
61	36	11	3
69	34	10	4
77	26	8	2
85	46	14	4
93	38	12	2
101	36	11	3
109	58	17	7
141	58	18	4
165	60	18	6

b) THÉORÈMES 1 ET 3.

Nous noterons $H^+(\Delta)$ le nombre des classes d'idéaux au sens strict de l'anneau O_Δ .

Pour chacun des deux exemples le tableau correspondant donne successivement pour chaque classe C de C_{4D}^+ un idéal négativement réduit, le nombre l_- des idéaux négativement réduits de C , un idéal négativement réduit de $\theta(C)$ et enfin les nombres l_-^* et l^* des idéaux négativement réduits et réduits de $\theta(C)$.

b1) $D = 141$. C'est le plus petit $D \equiv 5 \pmod{8}$ tel que $h^+(D) > 1$ et tel que (1.1) n'a pas de solution impaire. On a $h^+(141) = 2$ et $h^+(4 \times 141) = 6$.

C	l_-	$\theta(C)$	l_-^*	l^*
$[1, 12 + \sqrt{141}]$	2	$\left[1, \frac{13 + \sqrt{141}}{2}\right]$	4	2
$[4, 13 + \sqrt{141}]$	6			
$[7, 13 + \sqrt{141}]$	6			
$[5, 14 + \sqrt{141}]$	8	$\left[5, \frac{19 + \sqrt{141}}{2}\right]$	14	2
$[11, 14 + \sqrt{141}]$	8			
$[20, 29 + \sqrt{141}]$	28			

Le Théorème 3 affirme que $2 + 6 + 6 = 3 \times 4 + 2$ et $8 + 8 + 28 = 3 \times 14 + 2$, ce qui est vrai.

Le Théorème 1 affirme que $2 \neq 3 \times 4 + 2$, $6 \neq 3 \times 4 + 2$, $8 \neq 3 \times 14 + 2$, $28 \neq 3 \times 14 + 2$, ce qui est vrai.

b2) $D = 165$. C'est le plus petit $D \equiv 5 \pmod{8}$ tel que $h^+(D) \geq 4$ et tel que (1.1) a des solutions impaires. On a $h^+(165) = h^+(4 \times 165) = 4$.

C	l_-	$\theta(C)$	l_-^*	l^*
$[1, 13 + \sqrt{165}]$	4	$\left[1, \frac{13 + \sqrt{165}}{2}\right]$	1	1
$[3, 15 + \sqrt{165}]$	8	$\left[3, \frac{15 + \sqrt{165}}{2}\right]$	2	2
$[7, 16 + \sqrt{165}]$	14	$\left[7, \frac{23 + \sqrt{165}}{2}\right]$	4	2
$[11, 22 + \sqrt{165}]$	34	$\left[11, \frac{33 + \sqrt{165}}{2}\right]$	11	1

Les Théorèmes 1 et 3 affirment que $4 = 3 \times 1 + 1$, $8 = 3 \times 2 + 2$, $14 = 3 \times 4 + 2$ et $34 = 3 \times 11 + 1$, ce qui est exact.

D'autres exemples du Théorème 1 se trouvent dans [9].

Les auteurs remercient le rapporteur pour ses indications judicieuses qui leur ont permis de parfaire leur texte.

RÉFÉRENCES

- [1] EISENSTEIN, G. Aufgaben. *J. reine angew. Math.* 27 (1844), 86-87. (Werke I. pp. 111-112, Chelsea Publishing Company, New York 1975.)
- [2] GAUSS, C. F. *Arithmetische Untersuchungen (Disquisitiones Arithmeticae)*. Chelsea Publishing Company, New York 1965.
- [3] HARDY, G. H. and E. M. WRIGHT. *An Introduction to the Theory of Numbers*. Oxford University Press, 5e Edition (1989).
- [4] ISHII, N., P. KAPLAN and K. S. WILLIAMS. On Eisenstein's problem. *Acta Arithmetica* 54 (1990), 323-345.
- [5] KAPLAN, P. *Cours d'Arithmétique*. Université de Nancy I, U.E.R. de Sciences Mathématiques, 1973.
- [6] KAPLAN, P. and K. S. WILLIAMS. Pell's equations $X^2 - mY^2 = -1, -4$ and continued fractions. *J. Number Theory* 23 (1986), 169-182.
- [7] KAPLAN, P. and K. S. WILLIAMS. The distance between ideals in the orders of a real quadratic field. *L'Enseignement Mathématique* 36 (1990), 321-358.
- [8] LEJEUNE DIRICHLET, P. G and R. DEDEKIND. *Vorlesungen über Zahlentheorie*. Chelsea Publishing Company, New York (1968).
- [9] MIMURA, Y. On odd solutions of the equation $X^2 - DY^2 = 4$. *Proceedings of the symposium on analytic number theory and related topics*, Gakushuin University, Tokyo (1992), 110-118.
- [10] PERRON, O. *Die Lehre von den Kettenbrüchen*. Teubner (1977).
- [11] TAKAGI, T. *Théorie des nombres élémentaires*. Kyoritsu, Tokyo (1971), (en japonais).

(Reçu le 10 novembre 1992)

Pierre Kaplan

Université de Nancy I
 Département de Mathématiques
 B.P. 239
 54506 Vandœuvre Les Nancy Cedex
 France

Philip A. Leonard

Arizona State University
 Tempe AZ 85281-1804
 USA