

Idéaux k -réduits des ordres des corps quadratiques réels

Par Pierre KAPLAN

(Reçu le 28 juin, 1993)

§ 1. Introduction.

Soit Δ un discriminant positif, c'est-à-dire un entier positif non carré congru à 0 ou 1 modulo 4. Il existe un discriminant fondamental Δ_0 et un entier $f > 0$ tel que $\Delta = \Delta_0 f^2$. Soit O_Δ l'ordre de conducteur f du corps $Q(\sqrt{\Delta_0})$. Les idéaux primitifs de l'anneau O_Δ sont les $\mathbf{Z}$ -modules $I = \left[a, \frac{b + \sqrt{\Delta}}{2} \right]$ tels que

$$(1.1) \quad a > 0, \quad \frac{\Delta - b^2}{4a} = c \in \mathbf{Z}, \quad (a, b, c) = 1.$$

En particulier O_Δ est obtenu en prenant $a=1$ dans (1.1). Le nombre a est la norme $N(I)$ de l'idéal I et est déterminé par I . Le nombre $\varphi = (b + \sqrt{\Delta})/2a$ est déterminé modulo 1 par I et, inversement, φ détermine I . Nous dirons que I et φ sont associés et écrirons $I = I(\varphi)$, ce qui signifie que

$$(1.2) \quad I = a[1, \varphi], \quad \varphi = \frac{b + \sqrt{\Delta}}{2a},$$

où a et b vérifient (1.1). Le nombre c , qui dépend de φ , sera noté $c(\varphi)$.

Parmi les représentants de φ modulo 1, il en existe un, et un seul, $\varphi(I)$, dont le conjugué $\bar{\varphi} = (b - \sqrt{\Delta})/2a$ vérifie $-1 < \bar{\varphi} < 0$. Alors les coefficients b et c de φ , définis par (1.1) et (1.2), sont bien déterminés et seront notés $b(I)$ et $c(I)$ de sorte que

$$(1.3) \quad I = N(I)[1, \varphi(I)], \quad \varphi(I) = \frac{b(I) + \sqrt{\Delta}}{2N(I)}, \quad -1 < \bar{\varphi}(I) < 0.$$

Nous pouvons maintenant définir les idéaux k -réduits. Soit k un entier ≥ 0 et I un idéal de l'anneau O_Δ nous dirons que

$$(1.4) \quad \begin{cases} \text{l'idéal } I \text{ est } k\text{-réduit si } k < \varphi(I), \\ \text{l'idéal } I \text{ est strictement } k\text{-réduit si } k < \varphi(I) < k+1. \end{cases}$$

De même nous dirons que

$$(1.5) \quad \begin{cases} \text{le nombre } \varphi \text{ est } k\text{-réduit si } -1 < \bar{\varphi} < 0, & k < \varphi, \\ \text{le nombre } \varphi \text{ est strictement } k\text{-réduit si } -1 < \bar{\varphi} < 0, & k < \varphi < k+1. \end{cases}$$

Ainsi les idéaux 1-réduits sont les idéaux réduits au sens usuel et les idéaux 0-réduits sont les idéaux "négativement réduits" introduits dans [3]; les nombres 1-réduits sont les nombres réduits.

Désignons par $[\lambda]$ la partie entière du nombre réel λ . Comme $-1 < \lambda + [-\lambda] < 0$ on voit que, si l'on ne précise pas le choix de φ dans sa classe modulo 1,

$$(1.6) \quad \begin{cases} \text{l'idéal } I \text{ est } k\text{-réduit si } \varphi + [-\bar{\varphi}] > k, \\ \text{l'idéal } I \text{ est strictement } k\text{-réduit si } k < \varphi + [-\bar{\varphi}] < k+1. \end{cases}$$

On sait que le nombre des idéaux 0-réduits de O_Δ est fini et donc le nombre des idéaux k -réduits pour tout $k \geq 0$. Voici une démonstration très simple de ce fait.

Il suffit de voir que le nombre des nombres 0-réduits est fini, c'est-à-dire que le nombre des solutions entières (a, b, c) de

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

est fini. Or les deux dernières inégalités montrent que $|b| < \sqrt{\Delta}$, donc le nombre des choix possibles pour a, b et c tels que $\Delta = b^2 + 4ac$, $|b| < \sqrt{\Delta}$, $a > 0$ et $2a + b > \sqrt{\Delta}$ est fini.

Nous pouvons maintenant indiquer le but de ce travail.

Soit $D \equiv 1 \pmod{4}$ un discriminant positif. Nous allons relier les idéaux primitifs réduits de l'anneau O_{4D} à ceux de l'anneau O_D . Nous désignerons par I un idéal primitif de O_{4D} et par J un idéal primitif de O_D , et nous posons

$$N = \text{card}\{I; I \text{ réduit}\},$$

$$N_- = \text{card}\{I; I \text{ 0-réduit}\},$$

$$N^* = \text{card}\{J; J \text{ réduit}\},$$

$$N^\pm = \text{card}\{J; J \text{ 0-réduit}\}.$$

Si $D \equiv 5 \pmod{8}$:

$$N_1^* = \text{card}\{J; J \text{ strictement 1-réduit}\},$$

$$N_2^* = \text{card}\{J; J \text{ strictement 2-réduit}\},$$

$$N_3^* = \text{card}\{J; J \text{ 3-réduit}\}.$$

Si $D \equiv 1 \pmod{8}$:

$$N_1^* = \text{card}\{J; J \text{ réduit}, N(J) \equiv 0, c(J) \equiv 1 \pmod{2}\},$$

$$N_2^* = \text{card}\{J; J \text{ strictement 2-réduit, } N(J) \equiv 0, c(J) \equiv 1 \pmod{2}\},$$

$$N_3^* = \text{card}\{J; J \text{ 3-réduit, } N(J) \equiv 0 \pmod{2}\},$$

$$N_{-1}^* = \text{card}\{J; J \text{ 0-réduit, } N(J) \equiv 1 \pmod{2}\},$$

$$N_{-2}^* = \text{card}\{J; J \text{ 0-réduit, } N(J) \equiv 0, c(J) \equiv 1 \pmod{2}\}.$$

Alors nous obtenons les résultats nouveaux suivants pour les idéaux réduits :

THÉORÈME 1. ($D \equiv 5 \pmod{8}$). Si $D \equiv 5 \pmod{8}$ on a $N = N_1^* + 3N_2^* + 5N_3^*$.

THÉORÈME 2. ($D \equiv 1 \pmod{8}$). Si $D \equiv 1 \pmod{8}$ on a $N = N_1^* + 2N_2^* + 2N_3^*$.

En ce qui concerne les idéaux négativement réduits (0-réduits), le cas $D \equiv 5 \pmod{8}$ est traité dans [3], mais nous obtenons un résultat nouveau si $D \equiv 1 \pmod{8}$:

THÉORÈME 3. ($D \equiv 5 \pmod{8}$) ([3], Théorème 2). Si $D \equiv 5 \pmod{8}$ on a $N_- = 3N_{-1}^* + N^*$.

THÉORÈME 4. ($D \equiv 1 \pmod{8}$). Si $D \equiv 1 \pmod{8}$ on a $N_- = N_{-1}^* + 2N_{-2}^* + N_1^*$.

On sait d'autre part qu'il existe un homomorphisme θ du groupe des classes d'idéaux H_{4D} de O_{4D} sur le groupe H_D des classes d'idéaux de O_D . Nous montrerons que les Théorèmes 1 à 4 restent vrais si, au lieu de considérer tous les idéaux d'un type indiqué, on se limite à ceux d'une classe $C^* \in H_D$ et à ceux de son image inverse $\theta^{-1}(C^*)$, et nous obtiendrons ainsi la solution suivante à un problème posé par Gauss ([2], § 256, VI) et Eisenstein ([1]); pour d'autres critères voir [7], [6] et [3].

THÉORÈME 5. Soit ($D \equiv 5 \pmod{8}$), L le nombre des idéaux primitifs réduits d'une classe C de O_{4D} , et L_1^* , L_2^* , L_3^* les nombres des idéaux de la classe $\theta(C)$ qui sont respectivement strictement 1-réduits, strictement 2-réduits et 3-réduits. Alors l'équation $x^2 - Dy^2 = 4$ a des solutions impaires x et y si, et seulement si,

$$L = L_1^* + 3L_2^* + 5L_3^*.$$

Au paragraphe suivant (§ 2) nous allons démontrer les Théorèmes 1 et 2. Pour ceci nous définirons et étudierons une application ϕ de l'ensemble E des idéaux primitifs réduits de O_{4D} dans l'ensemble E^* des idéaux primitifs réduits de O_D .

Cette application ϕ est différente de celle utilisée dans [3] pour démontrer le Théorème 3. La démonstration du Théorème 4, que nous ommettons, s'obtient en modifiant la démonstration du Théorème 3 de façon à tenir compte de ce que $D \equiv 1 \pmod{8}$ comme nous procédons ici pour le Théorème 2, en utilisant le Lemme 3.

Au § 3 nous démontrons le Théorème 5.

Au § 4 nous donnons des exemples numériques.

§ 2. Démonstration des Théorèmes 1 et 2.

Nous commençons par trois lemmes. Les Lemmes 2 et 3 décrivent respectivement les idéaux de O_{4D} et de O_D .

LEMME 1. *Les idéaux $I(\varphi)$ et $I(1/\varphi)$ sont équivalents.*

DÉMONSTRATION. On a $1/\varphi = (p\varphi + q)/(r\varphi + s)$ avec $p = s = 0$, $q = r = 1$, d'où $ps - qr = -1$ ce qui, d'après [4, Proposition 3], prouve le Lemme 1.

LEMME 2. *Soit $I = a[1, \varphi]$ un idéal primitif de O_{4D} , avec $a = N(I)$.*

α) *Il existe $b = b(\varphi) \in \mathbf{Z}$ tel que $\varphi = (b + \sqrt{D})/a$ et $D = b^2 + ac$. Si φ vérifie $-1 < \bar{\varphi} < 0$ alors $b(I) = 2b(\varphi)$.*

β) *Si $N(I) \equiv 0 \pmod{2}$ alors $N(I) \equiv 0 \pmod{4}$ et $b(\varphi) \equiv c(\varphi) \equiv 1 \pmod{2}$.*

γ) *Si $N(I) \equiv 1 \pmod{2}$ alors $b(\varphi + 1) \equiv b(\varphi) + 1 \pmod{2}$.*

DÉMONSTRATION. D'après (1.1) φ s'écrit $\varphi = (b' + \sqrt{4D})/2a$ avec $4D = b'^2 + 4ac$, donc $b' = 2b$ et $\varphi = (b + \sqrt{D})/a$ avec $D = b^2 + ac$, ce qui prouve α).

Si a est pair alors b est impair, donc $ac \equiv 0 \pmod{4}$ et, comme $(a, 2b, c) = 1$, on voit que $a \equiv 0 \pmod{4}$, $b \equiv c \equiv 1 \pmod{2}$, ce qui prouve β).

Comme $b(\varphi + 1) = b(\varphi) + a$ on voit que, si a est impair, $b(\varphi + 1) \equiv b(\varphi) + 1 \pmod{2}$, ce qui achève la démonstration du Lemme 2.

LEMME 3. *Soit $J = a[1, \varphi] = I(\varphi)$ avec $\varphi = (b + \sqrt{D})/2a$ un idéal primitif de O_D . Alors $b \equiv 1 \pmod{2}$ et*

α) *Si $D \equiv 5 \pmod{8}$ on a $N(J) \equiv c(\varphi) \equiv 1 \pmod{2}$.*

β) *Si $D \equiv 1 \pmod{8}$ et $N(J) \equiv 1 \pmod{2}$ alors $c(\varphi) \equiv 0 \pmod{2}$.*

γ) *Si $D \equiv 1 \pmod{8}$ et $N(J) \equiv 0 \pmod{2}$ alors $c(\varphi + 1) \equiv c(\varphi) + 1 \pmod{2}$.*

δ) *Les idéaux $I(\varphi/2)$ et $I(2/\varphi)$ sont des idéaux primitifs de O_{4D} si, et seulement si, $c(\varphi) \equiv 1 \pmod{2}$.*

DÉMONSTRATION. L'égalité $D = b^2 + 4ac$ montre que $b \equiv 1 \pmod{2}$ ainsi que α) et β). De l'égalité $\varphi + 1 = (b + 2a + \sqrt{D})/2a$ on déduit $c(\varphi + 1) = (D - (b + 2a)^2)/4a = c - a - b$, et, si $a = N(J) \equiv a \pmod{2}$, on voit que $c(\varphi + 1) \equiv c(\varphi) + 1 \pmod{2}$, ce qui prouve γ). On a $\varphi/2 = (2b + \sqrt{4D})/2.4a$ d'où $c(\varphi/2) = (4D - (2b)^2)/16a = c(\varphi)$ et, comme $(a, b, c) = 1$, on voit que $(4a, 2b, c) = 1$ si, et seulement si, $c = c(\varphi) \equiv 1 \pmod{2}$. Pour achever la démonstration de δ) et du Lemme 2, il suffit de remarquer que, d'après le Lemme 1, les idéaux $I(\varphi/2)$ et $I(2/\varphi)$ sont équivalents.

Nous pouvons maintenant définir l'application ϕ . Pour ceci nous commençons par définir une partition de l'ensemble E des idéaux I primitifs réduits de

O_{4D} en trois sous-ensembles E_1 , E'_1 et E_2 de la manière suivante :

$$(2.1) \quad I \in \begin{cases} E_1, & \text{si } N(I) \equiv 1 \pmod{2} \text{ et } b(I) \equiv 2 \pmod{4}, \\ E'_1, & \text{si } N(I) \equiv 1 \pmod{2} \text{ et } b(I) \equiv 0 \pmod{4}, \\ E_2, & \text{si } N(I) \equiv 0 \pmod{4}. \end{cases}$$

Puis nous définissons l'application ϕ ainsi :

DÉFINITION 1. Soit I un idéal primitif réduit de O_{4D} . Alors

$$(2.2) \quad \phi(I) = \begin{cases} I\left(\frac{2}{\varphi(I)}\right), & \text{si } I \in E_1, \\ I\left(\frac{1}{\varphi(I)-1}\right), & \text{si } I \in E'_1, \\ I(2\varphi(I)), & \text{si } I \in E_2. \end{cases}$$

Rappelons maintenant la définition de l'application θ . Soit C une classe d'idéaux de l'anneau O_{4D} et soit $I = a[1, \varphi']$ un idéal primitif de C où $\varphi' = (b(\varphi') + \sqrt{D})/a$ est tel que $b(\varphi') \equiv 1 \pmod{2}$. Alors la classe $\theta(C)$ contient l'idéal

$$(2.3) \quad \begin{cases} I\left(\frac{\varphi'}{2}\right) = \left[a, \frac{b(\varphi') + \sqrt{D}}{2} \right], & \text{si } a \equiv 1 \pmod{2}, \\ I(2\varphi') = \left[\frac{a}{4}, \frac{b(\varphi') + \sqrt{D}}{2} \right], & \text{si } a \equiv 0 \pmod{4}. \end{cases}$$

(Voir [4], Theorem 1 et Corollary 4).

LEMME 4. Soit $C(I)$ la classe de l'idéal primitif réduit $I \in E$ et $\theta(C(I))$ son image par θ . L'idéal $\phi(I)$ défini par (2.2) est un idéal de $\theta(C(I))$, primitif, réduit, et de norme paire si $D \equiv 1 \pmod{8}$.

DÉMONSTRATION. On a $I = a[1, \varphi]$ où $\varphi = \varphi(I)$ est réduit. D'après (2.1), (2.3) et Lemme 2, γ), la classe $\theta(C(I))$ contient $I(\varphi/2)$ si $I \in E_1$, $I((\varphi-1)/2)$ si $I \in E'_1$, et $I(2\varphi)$ si $I \in E_2$. Appliquant (2.3), et aussi le Lemme 1 si $I \in E_1$ ou E'_1 , on voit que $\phi(I) \in \theta(C(I))$.

Considérons le cas où $N(I) \equiv 1 \pmod{2}$ et posons $\varphi' = \varphi$ si $\varphi \in E_1$, $\varphi' = \varphi - 1$ si $\varphi \in E'_1$. Alors $I = I(\varphi')$ où $\varphi' = (b' + \sqrt{D})/a$ avec $b' \equiv 1 \pmod{2}$ et donc $D = b'^2 + 4ac'$. Comme I est primitif on a $(a, 2b', 4c') = 1$ et, comme I est réduit, $\varphi' > 0$ et $\bar{\varphi}' < 0$ donc $\varphi'\bar{\varphi}' < 0$ ce qui montre que $b'^2 < D$ et $c' > 0$. D'autre part $2/\varphi' = 2a/(b' + \sqrt{D}) = (-b' + \sqrt{D})/2c'$ ce qui prouve que l'idéal $\phi(I) = I(2/\varphi')$ est un idéal primitif de O_D de norme c' , où $c' \equiv 0 \pmod{2}$ si $D \equiv 1 \pmod{8}$. Comme φ est réduit on a $2/\varphi > 0$, $-2/\bar{\varphi} > 2$ et $2/(\varphi-1) > 0$, $-2/(\bar{\varphi}-1) > 1$ ce qui, d'après (1.6), prouve que l'idéal $\phi(I)$ est réduit.

Si $N(I) \equiv 0 \pmod{4}$ on a $\varphi = (b + \sqrt{D})/4a'$ avec $(4a', 2b, c) = 1$, et $c \equiv 1 \pmod{2}$

d'après le Lemme 3, β). Donc $2\varphi = (b + \sqrt{D})/2a'$ avec $(a', b', c) = 1$ ce qui montre que $\phi(I)$ est un idéal primitif de O_D et, comme $2\varphi + [-2\bar{\varphi}] \geq 2\varphi + 2[-\bar{\varphi}] > 2$, on voit d'après (1.6) que $\phi(I)$ est 2-réduit. Enfin l'égalité $D = b^2 + 4a'c$ montre que $a' = N(\phi(I)) \equiv 0 \pmod{2}$ si $D \equiv 1 \pmod{8}$. Ceci termine la démonstration du Lemme 4.

Nous désignerons par ϕ_1, ϕ'_1, ϕ_2 les restrictions de ϕ à E_1, E'_1 et E_2 respectivement. Avec ces notations nous avons

PROPOSITION 1. Cas où $D \equiv 5 \pmod{8}$.

a) Les images de ϕ_1 et de ϕ_2 sont formées des idéaux 2-réduits de E^* . Chaque image réciproque $\phi_1^{-1}(J)$ ou $\phi_2^{-1}(J)$ est formée de deux ou d'un idéal de E suivant que J est 3-réduit ou non.

b) ϕ'_1 est une bijection de E'_1 sur E^* .

PROPOSITION 2. Cas où $D \equiv 1 \pmod{8}$.

Si $D \equiv 1 \pmod{8}$ les trois applications ϕ_1, ϕ'_1, ϕ_2 sont des injections.

a) Les images de ϕ_1 et de ϕ_2 sont égales et formées chacune de l'ensemble des idéaux de E^* qui sont soit 3-réduits avec $N(J) \equiv 0 \pmod{2}$, soit strictement 2-réduits avec $N(J) \equiv 0, c(J) \equiv 1 \pmod{2}$.

b) L'image de ϕ'_1 est l'ensemble des idéaux $J \in E^*$ tels que $N(J) \equiv c(J) \equiv 0 \pmod{2}$.

DÉMONSTRATION. Soit $J = a[1, \omega]$ un idéal de E^* , avec ω réduit et $a \equiv 0 \pmod{2}$ si $D \equiv 1 \pmod{8}$. Nous démontrons les deux propositions ensemble.

a_1) Les nombres réduits φ définissant les idéaux $I \in E_1$ tels que $\phi_1(I) = J$ sont tels qu'il existe $n \in \mathbb{Z}$ tel que $2/\varphi = \omega - n$ et que l'idéal $I(\varphi)$ soit primitif. Ce sont donc des nombres $\varphi = 2/(\omega - n)$ tels que $2/(\omega - n) > 1, 0 < 2/(n - \bar{\omega}) < 1$ et que $I(\varphi)$ soit primitif. La première condition montre que $n = [\omega]$ ou $n = [\omega] - 1$ et, comme $0 < -\bar{\omega} < 1$, la deuxième équivaut à $n \geq 2$. Donc aucune valeur de n ne peut convenir si $\omega < 2$, $n = [\omega]$ peut convenir si $2 < \omega < 3$ et les deux valeurs $n = [\omega], n = [\omega] - 1$ peuvent convenir si $\omega > 3$. Il reste à voir quand $I(\varphi)$ est primitif. Le Lemme 3 montre que c'est toujours le cas si $D \equiv 5 \pmod{8}$.

Si $D \equiv 1 \pmod{8}$ et $\omega > 3$ alors, d'après le Lemme 3, exactement une des deux valeurs $n = [\omega]$ ou $n = [\omega] - 1$ est telle que $c(\omega - n)$ soit impair.

Si $2 < \omega < 3$ alors $[\omega] = 2$ convient si, et seulement si, $c(\omega)$ est impair. Ceci prouve les Propositions 1 et 2 pour ϕ_1 .

a_2) Les idéaux de $\phi_2^{-1}(J)$ sont les idéaux $I(\varphi)$ avec $2\varphi \equiv \omega \pmod{1}$, donc sont à chercher parmi les idéaux $I_1 = I(\omega/2)$ et $I_2 = I((\omega - 1)/2)$. Or, si $\omega = (b + \sqrt{D})/2a$ avec $D = b^2 + 4ac$ on a $\omega/2 = (2b + \sqrt{4D})/8a$ avec $4D = 4b^2 + 16ac$ ce qui montre que $c(\omega/2) = c(\omega)$. Appliquant cette remarque à I_1 et I_2 on a, puisque $-1 < (\bar{\omega} - 1)/2 < \bar{\omega}/2 < 0$, $c(I_1) = c(\omega/2) = c(\omega)$ et $c(I_2) = c((\omega - 1)/2) = c(\omega - 1)$.

D'après le Lemme 3 les idéaux I_1 et I_2 sont primitifs si $D \equiv 5 \pmod{8}$ et si $D \equiv 1 \pmod{8}$ I_1 est primitif si $c(J)=c(\omega)$ est impair et I_2 est primitif si $c(J)$ est pair. D'autre part

$$I_1 \text{ est réduit si, et seulement si, } \omega + 2 \left[-\frac{\bar{\omega}}{2} \right] > 2,$$

$$I_2 \text{ est réduit si, et seulement si, } \omega - 1 + 2 \left[-\frac{\bar{\omega}-1}{2} \right] > 2.$$

Or $[-\bar{\omega}/2] = [-(\bar{\omega}-1)/2] = 0$, ce qui montre que I_1 est réduit si, et seulement si, $\omega > 2$ tandis que I_2 est réduit si, et seulement si, $\omega > 3$.

Ainsi on voit que, si $D \equiv 5 \pmod{8}$, $\phi_2^{-1}(J) = I_1$ si $2 < \omega < 3$ et $\phi_2^{-1}(J) = I_1 \cup I_2$ si $\omega > 3$. Si $D \equiv 1 \pmod{8}$ $\phi_2^{-1}(J) = I_1$ si $c(J)$ est impair et $\omega > 2$, et $\phi_2^{-1}(J) = I_1$ si $c(J)$ est pair et $\omega > 3$. Ceci prouve les propositions 1 et 2 pour ϕ_2 .

b) Les nombres réduits φ associés définissant les idéaux $I \in E'_1$ tels que $\phi'_1(I) = J$ sont les nombres φ réduits pour lesquels il existe $n \in \mathbb{Z}$ tels que $2/(\varphi-1) = \omega - n$ et que l'idéal $I(\varphi)$ soit primitif. Ce sont donc des nombres $\varphi = 2/(\omega - n) + 1$ tels que $2/(\omega - n) > 0$ et $-2 < 2/(\bar{\omega} - n) < -1$, soit $n < \omega$ et $1 + \bar{\omega} < n < 2 + \bar{\omega}$, c'est-à-dire $n = 1$. Maintenant nous appliquons le Lemme 3 à l'idéal $I(2/(\omega-1)+1) = I(2/(\omega-1))$. Si $D \equiv 5 \pmod{8}$ l'idéal $I(2/(\omega-1))$ est toujours primitif, tandis que, si $D \equiv 1 \pmod{8}$, $I(2/(\omega-1))$ est primitif si, et seulement si, $c(\omega-1) \equiv 1 \pmod{2}$ c'est-à-dire si, et seulement si, $c(\omega) \equiv 0 \pmod{2}$. Ceci achève la démonstration des propositions 1 et 2.

Nous pouvons maintenant démontrer les Théorèmes 1 et 2.

Posons $N_1 = \text{card}(E_1)$, $N_2 = \text{card}(E_2)$ et $N'_1 = \text{card}(E'_1)$. Quand $D \equiv 5 \pmod{8}$, la Proposition 1 implique

$$(2.4) \quad N_1 = N_2 = N_2^* + 2N_3^*, \quad N'_1 = N_1^* + N_2^* + N_3^*.$$

Ceci montre que $N = N_1 + N_2 + N'_1 = N_1^* + 3N_2^* + 5N_3^*$, ce qui est le Théorème 1.

Quand $D \equiv 1 \pmod{8}$ la proposition 2 implique

$$(2.5) \quad N_1 = N_2 = N_2^* + N_3^*, \quad N'_1 = N_1^*$$

d'où $N = N_1 + N'_1 + N_2 = N_1^* + 2N_2^* + 2N_3^*$, ce qui est le Théorème 2.

§ 3. Démonstration du Théorème 5.

D'après le Lemme 4 l'application ϕ est compatible avec l'homomorphisme θ . Il en est d'ailleurs de même de l'application ϕ utilisée dans [3] pour prouver le Théorème 3 et qui permet aussi de prouver le Théorème 4. Donc dans l'énoncé des Théorèmes 1 et 2 on peut remplacer les nombres N_1^* , N_2^* , N_3^* des idéaux réduits des types indiqués par les nombres L_1^* , L_2^* , L_3^* des types indiqués

appartenant à une classe C^* de O_D , et N par le nombre L des idéaux réduits de $\theta^{-1}(C^*)$.

Or on sait que

$$(3.1) \quad \text{card Ker } \theta = \begin{cases} 3, & \text{si } D \equiv 5 \pmod{8} \text{ et } x^2 - Dy^2 = 4 \text{ n'a pas de solution impaire,} \\ 1, & \text{sinon.} \end{cases}$$

(Voir [2], § 256, VI ou [5], § 151).

Si $D \equiv 1 \pmod{8}$, θ est une bijection donc le Théorème 2 implique le résultat suivant

COROLLAIRE 1. Si $D \equiv 1 \pmod{8}$, $L = L_1^* + 2L_2^* + 2L_3^*$.

Si $D \equiv 5 \pmod{8}$ on obtient le Théorème 5 à partir du Théorème 1, de (3.1), et de la remarque qui précède.

Exemples numériques.

a) Théorème 1. ($D \equiv 5 \pmod{8}$).

Nous donnons la liste des discriminants $D \equiv 5 \pmod{8}$ de 5 à 189 ainsi que 485, et les valeurs de N_1^* , N_2^* , N_3^* , N , $h = \text{card}(H_D)$, + ou - suivant que $x^2 - Dy^2 = 4$ a ou non des solutions impaires. Dans la plupart des cas $h=1$ et le signe est +.

D	N_1^*	N_2^*	N_3^*	N	h	+/-
5	1	0	0	1	1	+
13	0	0	1	5	1	+
21	1	0	1	6	1	+
29	0	0	1	5	1	+
37	1	2	0	5	1	-
45	1	0	1	6	1	+
53	0	0	1	5	1	+
61	0	2	1	11	1	+
69	3	0	1	8	1	+
77	1	0	1	6	1	+
85	1	2	1	12	2	+
93	0	0	2	10	1	+
101	2	0	1	7	1	-
109	4	2	1	15	1	-
117	1	0	1	6	1	+
125	0	0	1	5	1	+

133	1	0	3	16	1	+
141	0	2	2	16	1	—
149	4	0	1	9	1	+
157	2	0	3	17	1	+
165	4	0	2	14	2	+
173	0	0	1	5	1	+
181	0	2	3	21	1	+
189	1	2	1	12	1	—
485	4	2	2	20	2	—

On voit bien sur ce tableau que l'égalité $N=N_1^*+3N_2^*+5N_3^*$ est vérifiée. Il est vraiment étonnant qu'un résultat si simple et si élégant soit resté ignoré jusqu'à l'aube du troisième millénaire.

b) Théorème 5. Si $h=1$ et si le signe est + le Théorème 5 se ramène au Théorème 1. Nous étudions donc les nombres du tableau précédent qui restent et indiquons pour chacun d'eux les nombres des idéaux primitifs réduits de la classe principale situés dans E_1^* , E_2^* , E_3^* et E respectivement.

D	L_1^*	L_2^*	L_3^*	L	h	$+/-$
37	2	0	1	1	1	—
85	0	0	1	5	2	+
101	2	0	1	1	1	—
141	0	2	2	4	1	—
165	1	0	1	6	2	+
189	1	2	1	4	1	—
485	2	0	1	1	2	—

On voit bien que la relation $L=L_1^*+3L_2^*+5L_3^*$ est vérifiée exactement quand le signe est +, et que $L<L_1^*+3L_2^*+5L_3^*$ quand le signe est —.

Nous allons examiner le cas de 485 qui est le plus petit discriminant fondamental pour lequel $h>1$ et $x^2-Dy^2=4$ n'a pas de solution impaire. Nous donnons la liste des idéaux sous la forme $[N(I), b(I), c(I)]$ de chaque classe des discriminants $D=485$ et $4D=4\times 485=1940$

$D=485$ P^* : $[1, 21, 11]$, $[11, 1, 11]$, $[11, 21, 1]$; $L_1^*=2$, $L_2^*=0$, $L_3^*=1$;

A^* : $[5, 15, 13]$, $[13, 11, 7]$, $[7, 17, 7]$, $[7, 11, 13]$, $[13, 15, 5]$;

$L_1'^*=2$, $L_2'^*=2$, $L_3'^*=1$;

$D=1940$ P_1 : $[1, 44, 1]$; $L_1=1$;

P_2 : $[4, 42, 11]$, $[11, 24, 31]$, $[31, 38, 4]$; $L_2=3$;

P_3 : $[11, 42, 4]$, $[4, 38, 31]$, $[31, 24, 11]$; $L_3=3$;

$$A_1: [5, 40, 17], [17, 28, 17], [17, 40, 5]; L'_1=3;$$

$$A_2: [7, 36, 23], [23, 10, 20], [20, 30, 13], [13, 22, 28], [28, 34, 7];$$

$$L'_2=5;$$

$$A_3: [7, 34, 28], [28, 22, 13], [13, 30, 20], [20, 10, 23], [23, 36, 7];$$

$$L'_3=5.$$

Ici $\{P_1, P_2, P_3\} = \theta^{-1}(P^*)$ et $\{A_1, A_2, A_3\} = \theta^{-1}(A^*)$ et on vérifie que

$$L_1 + L_2 + L_3 = 7 = L_1^* + 5L_3^* = 2 + 5 = 7,$$

$$L'_1 + L'_2 + L'_3 = 13: L'_1 + 3L'_2 + 5L'_3 = 2 + 6 + 5 = 13.$$

c) Cas $D \equiv 1 \pmod{8}$. Théorèmes 2 et 4. Nous donnons pour les discriminants $D \equiv 1 \pmod{8}$ de 17 à 129 les valeurs de $N_1^*, N_2^*, N_3^*, N, N_{-1}^*, N_{-2}^*$ et N_- .

D	N_1^*	N_2^*	N_3^*	N	N_{-1}^*	N_{-2}^*	N_-
17	1	0	0	1	1	3	8
33	0	2	0	4	2	6	14
41	3	0	0	3	3	5	16
57	2	0	2	6	4	8	22
65	2	0	2	6	4	8	22
73	3	0	2	7	5	11	30
89	1	0	2	5	5	11	28
97	3	2	2	11	7	13	36
105	2	0	2	6	6	14	36
113	5	0	2	9	7	9	30
129	2	2	2	10	8	16	42

On vérifie bien sur tous ces exemples les deux relations

$$N = N_1^* + 2(N_2^* + N_3^*) \quad \text{et} \quad N_- = N_{-1}^* + 2N_{-2}^* + N_1^*,$$

qui sont les contenus des Théorèmes 2 et 4.

Références

- [1] G. Eisenstein, J. Reine Angew. Math., 27 (1844), 86-87. (Werke I., Chelsea Publishing Company, New York, 1975, pp. 111-112.)
- [2] C.F. Gauss, Arithmetische Untersuchungen (Disquisitiones Arithmeticae), Chelsea Publishing Company, New York, 1965.
- [3] P. Kaplan et P.A. Leonard, Idéaux négativement réduits d'un corps quadratique réel et un problème d'Eisenstein, L'Enseignement Mathématique, 39 (1993), 195-210.
- [4] P. Kaplan and K.S. Williams, The distance between ideals in the orders of a real

- quadratic field, *L'Enseignement Mathématique*, **36** (1990), 321-358.
- [5] P.G. Lejeune Dirichlet and R. Dedekind, *Vorlesungen über Zahlentheorie*, Chelsea Publishing Company, New York, 1968.
 - [6] Y. Mimura, 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, pp. 110-118.
 - [7] H.C. Williams, Eisenstein problem and continued fractions, *Utilitas Math.*, **37** (1990), 145-158.

Pierre KAPLAN

Département de Mathématiques
Université de Nancy 1
B.P. 239, 54506
Vandœuvre les Nancy Cedex
France