Idéaux réduits, nombres réduits et équation $D = y^2 + 4xz$

Par Pierre KAPLAN

Département de Mathématiques, Université de Nancy I, BP 239, 54506 Vandœuvre-lès-Nancy cedex, France

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1998)

§1. Introduction. Dans ce travail les lettres latines $D, a, b, c, \ldots, u, v, x, y, z, \ldots$, désigneront toujours des entiers, éléments de l'ensemble $\boldsymbol{Z}$, et l'expression $(x, y, z) = 1$ signifie que x, y et z n'ont pas de diviseur commun. Si λ est un nombre réel sa partie entière sera désignée par $[\lambda]$.

Soit D un discriminant positif, c'est-à-dire un entier positif non carré congru à 0 ou 1 modulo 4 : nous ne supposons pas que D soit fondamental. Nous considérons d'une part l'ensemble fini $S(D)$ des solutions (x, y, z) de l'équation

(1.1) $D = y^2 + 4xz$, $(x, y, z) = 1$, $x > 0$, $|y| < \sqrt{D}$,

d'où $z > 0$, et d'autre part les idéaux et nombres 0-réduits et 1-réduits de discriminant D dont les définitions précises seront rappelées plus bas ; les nombres 1-réduits sont les nombres quadratiques dont le développement en fraction continue ordinaire est purement périodique, les nombres 0-réduits sont ceux dont le développement en fraction continue à l'entier supérieur est purement périodique. Nous noterons $s(D)$ le cardinal de l'ensemble $S(D)$ et $r_0(D)$ le cardinal de l'ensemble des idéaux ou des nombres 0-réduits de discriminant D.

Le but de ce travail est de démontrer de manière simple les résultats suivants :

Théorème 1. $s(D) = 2r_0(D)$,

Théorème 2. $s(D) = \sum_{\varphi\ 0\text{-réduit de discriminant } D} [\varphi]$,

Théorème 3. $s(D) = 2 \sum_{\varphi\ 1\text{-réduit de discriminant } D} [\varphi]$,

Théorème 4. $r_0(D) = \sum_{\varphi\ 1\text{-réduit de discriminant } D} [\varphi]$,

et les résultats analogues, Théorèmes 5, 6, 7 et 8, que l'on obtient en se limitant à une classe d'idéaux.

Pour démontrer les Théorèmes 1 à 4 (§2) et les Théorèmes 5 à 8 (§3) nous utilisons les définitions des nombres et idéaux 0-réduits et 1-réduits et leurs propriétés les plus simples, mais ne faisons pas appel aux théories des fractions continues. Dans une dernière partie (§4) nous expliquons rapidement comment on peut retrouver une partie de ces résultats à partir des théories des fractions continues, en citant des travaux antérieurs où ceci est partiellement réalisé.

Les résultats nouveaux de ce travail sont les Théorèmes 2 et 6, mais il n'est pas certain que l'on puisse trouver dans la littérature une démonstration complète des autres. Et, pour parler comme Gauss, nous espérons que la théorie simple qui suit ne déplaira pas à quelques lecteurs.

§2. Idéaux et nombres 0-réduits et 1-réduits de discriminant D. L'ordre O_D de discriminant D est le $\boldsymbol{Z}$-module $\left[1, \frac{D + \sqrt{D}}{2}\right]$, où $[\alpha, \beta]$ désigne le $\boldsymbol{Z}$-module engendré par α et β. Les idéaux primitifs de l'ordre O_D sont les $\boldsymbol{Z}$-modules $\left[a, \frac{b + \sqrt{D}}{2}\right]$ tels que

(2.1) $a > 0$, $\frac{D - b^2}{4a} = c \in \boldsymbol{Z}$, $(a, b, c) = 1$.

Le nombre a est la norme de l'idéal I. Posons $\varphi = \frac{b + \sqrt{D}}{2a}$. La classe de φ modulo 1 est déterminée par I et, inversement, le nombre φ détermine l'idéal I. On dit que I et φ sont associés, et on écrit $I = I(\varphi)$, ce qui signifie que

(2.2) $I = a[1, \varphi]$, $\varphi = \frac{b + \sqrt{D}}{2a}$,

où a et b vérifient (2.1). Si a et b vérifient (2.1) on dit que le discriminant de l'idéal I et du nombre φ définis par (2.2) est D. Deux nombres ou deux idéaux équivalents ont le même discriminant. Dans tout ce travail, le mot 《idéal》 signifiera 《idéal de discriminant D》, les lettres φ et ω désigneront des nombres de discriminant D et nous noterons $\bar{\varphi}$ le conjugué $\bar{\varphi} = \frac{b - \sqrt{D}}{2a}$ de $\varphi = \frac{b + \sqrt{D}}{2a}$. Nous désignerons par $S_0(D)$ l'ensemble des nombres $\omega = \frac{y + \sqrt{D}}{2x}$ où

$(x, y, z) \in S(D)$. On a $\text{card}(S_0(D)) = s(D)$ et les nombres ω de $S_0(D)$ sont les nombres de discriminant D tels que $\omega > 0$ et $\bar{\omega} < 0$.

Soit $I = a[1, \varphi]$ un idéal. Le nombre $[\varphi] - \bar{\varphi}$ ne dépend pas du choix de φ dans sa classe modulo 1. Pour $k \geq 0$ on dit (voir [4, p. 172], et [5, p. 287]) que l'idéal I est k-réduit si $[\varphi] - \bar{\varphi} > k$, ce qui équivaut à $\varphi + [-\bar{\varphi}] > k$. Les idéaux 1-réduits sont les idéaux réduits au sens usuel. Le nombre $r_0(D)$ des idéaux 0-réduits est fini. Nous allons retrouver une démonstration simple de ce fait en prouvant le Théorème 1 :

Démonstration (Théorème 1). Soit $I = a[1, \varphi]$ un idéal. On peut choisir φ de manière unique de sorte que $-1 < \bar{\varphi} < 0$, et l'idéal I est 0-réduit si, et seulement si, $[\varphi] - \bar{\varphi} > 0$ c'est-à-dire $\varphi > 0$ si bien que

(2.3) $r_0(D) = \text{card}(\{\varphi ; -1 < \bar{\varphi} < 0 < \varphi\})$.

Ceci montre déjà que $r_0(D)$ est fini et que $r_0(D) \leq s(D)$.

Considérant la bijection $\varphi \to 1/\varphi$ de $S_0(D)$ on voit que

(2.4) $r_0(D) = \text{card}(\{\varphi ; \bar{\varphi} < -1, 0 < \varphi\})$.

Les équations (2.3) et (2.4) montrent que $s(D) = 2r_0(D)$, ce qui est le Théorème 1.

Si l'idéal I est 1-réduit on peut choisir φ de manière unique de façon que

(2.5) $0 < \bar{\varphi} < 1 < \varphi$.

On dit alors que φ est un nombre 0-réduit et que $\varphi = \varphi_0(I)$ est le nombre 0-réduit associé à l'idéal I.

De même si l'idéal J est 1-réduit on peut choisir φ de manière unique de facon que

(2.6) $-1 < \bar{\varphi} < 0, 1 < \varphi$.

On dit alors que φ est un nombre 1-réduit et que $\varphi = \varphi_1(J)$ est le nombre 1-réduit associé à l'idéal J; le nombre 0-réduit associé à J est alors $\varphi_0(J) = \varphi_1(J) + 1$.

Avec ces notations les Théorèmes 2, 3 et 4 s'expriment ainsi :

Théorème 2. $s(D) = \sum_{I\ 0\text{-réduit}} [\varphi_0(I)]$,

Théorème 3. $s(D) = 2 \sum_{I\ 1\text{-réduit}} [\varphi_1(I)]$,

Théorème 4. $r_0(D) = \sum_{I\ 1\text{-réduit}} [\varphi_1(I)]$.

Considérons l'ensemble $R_0(D)$ des idéaux 0-réduits. Pour chaque $I \in R_0(D)$, soit $\Omega_0(I)$ l'ensemble des nombres $\varphi_0(I) - u$ où $0 < u < \varphi_0(I)$ et soit $\Omega_0(D)$ la réunion des ensembles $\Omega_0(I)$ pour $I \in R_0(D)$. La clé de ce travail est la proposition simple qui suit :

Proposition 1. a) *On a* $\text{card}(\Omega_0(I)) = [\varphi_0(I)]$. *Si* $I, I' \in R_0(D)$ *et* $I \neq I'$, *alors* $\Omega_0(I) \cap \Omega_0(I') = \emptyset$.

b) $\Omega_0(D) = S_0(D)$.

Démonstration. a) Si $\varphi_0(I_1) - u_1 = \varphi_0(I_2) - u_2$ on a aussi $\overline{\varphi_0}(I_1) - u_1 = \overline{\varphi_0}(I_2) - u_2$. Comme $0 < \overline{\varphi_0}(I_1), \overline{\varphi_0}(I_2) < 1$ on a $u_1 = u_2$ d'où $\overline{\varphi_0}(I_1) = \overline{\varphi_0}(I_2)$ et $I_1 = I_2$. Ceci prouve a).

b) Si $\omega = \varphi_0(I) - u \in \Omega_0(D)$ on a $0 < \overline{\varphi_0}(I) < 1 < u < \varphi_0(I)$ donc $\overline{\varphi_0}(I_1) - u < 0 < \varphi_0(I) - u$, ce qui prouve que $\omega \in S_0(D)$.

Soit $\omega \in S_0(D)$. Comme ω et $-\bar{\omega} > 0$ on a $[\omega] - \bar{\omega} > 0$ ce qui prouve que l'idéal $I(\omega)$ est 0-réduit. Il existe donc $u \in \boldsymbol{Z}$ tel que $\varphi = \omega + u$ soit le nombre 0-réduit $\varphi_0(I(\omega))$. Comme $\bar{\omega} < 0$ et $\bar{\varphi} > 0$ on voit que $u > 0$ et, comme $\omega > 0$, on a $u < \varphi$, ce qui prouve que $\omega \in \Omega_0(D)$ et achève la démonstration de la Proposition 1.

Nous pouvons maintenant démontrer les Théorèmes 2, 3 et 4 :

Démonstration (Théorème 2). D'après la Proposition 1 a) on a $\text{card}(\Omega_0(D)) = \sum_{I\ 0\text{-réduit}} [\varphi_0(I)]$, et d'après b), $s(D) = \text{card}(\Omega_0(D))$, ce qui prouve le Théorème 2.

Démonstration (Théorèmes 3 et 4). Si φ est un nombre 0-réduit, l'idéal $I(\varphi)$ est 1-réduit si, et seulement si, $[\varphi] - \bar{\varphi} > 1$, donc, comme $0 < \bar{\varphi} < 1$, si, et seulement si, $\varphi > 2$. Le Théorème 2 peut donc s'écrire

(2.7) $S(D) = \sum_{I\ 1\text{-réduit}} [\varphi_0(I)] + \sum_{I\ 0\text{-réduit non } 1\text{-réduit}} 1$.

Comme si l'idéal I est 1-réduit on a $\varphi_0(I) = \varphi_1(I) + 1$, la relation (2.7) s'écrit

(2.8) $s(D) = r_0(D) + \sum_{I\ 1\text{-réduit}} [\varphi_1(I)]$.

Combinant l'égalité (2.8) avec le Théorème 1 on trouve les Théorème 3 et 4.

§3. Classes d'idéaux. Les notions d'équivalence des idéaux sont bien connues, nous nous référons par exemple à [6] pour les détails et le lien avec les notions d'équivalence des nombres.

Soit C une classe d'idéaux au sens large ou strict. Nous noterons $S(C)$, de cardinal $s(C)$, l'ensemble des éléments $(x, y, z) \in s(D)$ tels que $I(\omega) \in C$ où $\omega = \frac{y+\sqrt{D}}{2x}$, et $S_0(C)$ l'ensemble de ces nombres ω. Soit $r_0(C)$ le nombre des idéaux 0-réduits de la classe C. Nous pouvons maintenant énoncer et démontrer les Théorème 5 à 8.

Théorème 5. *Soit C une classe d'idéaux au sens large. On a :*

$$s(C) = 2r_0(C).$$

Théorème 6. *Soit C une classe d'idéaux au sens large ou sens strict. On a :*

$$s(C) \sum_{I \in C, I\ 0-réduit} [\varphi_0(I)].$$

Théorème 7. *Soit C une classe d'idéaux au sens large. On a :*

$$s(C) = 2 \sum_{I \in C, I\ 1-réduit} [\varphi_1(I)].$$

Théorème 8. *Soit C une classe d'idéaux au sens large. On a :*

$$r_0(C) \sum_{I \in C, I\ 1-réduit} [\varphi_1(I)].$$

Démonstration (Théorèmes 5 à 8). D'après la Proposition 1 l'ensemble $S_0(D)$ est la réunion disjointe des ensembles $\Omega_0(I)$ quand I parcourt l'ensemble des idéaux 0-réduits. D'autre part si $\omega \in \Omega_0(I)$ on a $I(\omega) = I$ et l'idéal $I(1/\omega)$ est équivalent au sens large à l'idéal I (voir [7, p. 357]). Ainsi si C est une classe au sens strict, ou au sens large, l'ensemble $S_0(C)$ est la réunion disjointe des ensembles $\Omega_0(I)$ pour $I \in C$, ce qui prouve le Théorème 6. De plus, si C est une classe au sens large, $I(\varphi) \in C$ si, et seulement si, $I(1/\varphi) \in C$ donc on a :

$$r_0(C) = \text{card}\,(\{\varphi\,;\, -1 < \bar{\varphi} < 0 < \varphi,\ I(\varphi) \in C\})$$
$$= \text{card}\,(\{\varphi\,;\, \bar{\varphi} < -1,\ 0 < \varphi,\ I(\varphi) \in C\})$$

ce qui prouve le Théorème 5. Les Théorèmes 7 et 8 s'obtiennent à partir des Théorème 5 et 6 comme les Théorèmes 3 et 4 à partir des Théorèmes 1 et 2. Ceci achève la démonstration des Théorèmes 5 à 8.

§4. Remarques. 1) Nous avons volontairement présenté cette théorie de la manière la plus simple. Il reste à montrer que les nombres $s(C)$ et $r_0(C)$ sont non nuls : ceci vient de ce que toute classe contient un idéal 1-réduit, fait qui peut être considéré comme conséquence de la partie la plus simple de la théorie des fractions continues des nombres quadratiques (voir par exemple [6, p. 341]).

2) Expliquons rapidement comment il est possible de retrouver une grande partie des Théorèmes 1 à 8 à partir des théories complètes des fractions continues ordinaires et à l'entier supérieur des nombres quadratiques.

Si $\varphi = \varphi_0$ est un nombre 0-réduit (respectivement : 1-réduit) son développement en fraction continue défini par $\varphi_n = r_{n+1} - 1/\varphi_{n+1}$, $\varphi_{n+1} > 1$ (respectivement : $\varphi_n = q_{n+1} + 1/\varphi_{n+1}$, $\varphi_{n+1} > 1$) est purement périodique et définit la période de tous les nombres de la classe au sens strict (respectivement : au sens large) de φ. Si le nombre φ est 1-réduit le nombre 0-réduit définissant l'idéal $I(\varphi)$ est $\varphi + 1$. Si l'on suppose connue la suite q_n on peut calculer la suite r_n en développant $\varphi + 1$ en fraction continue à l'entier supérieur. Le résultat est donné, sans preuve, dans [3, p. 50], [9, p. 178], [10, p. 131]. À partir de ces développements, et en discutant suivant le signe de la norme de l'unité fondamentale de l'ordre O_D, on obtient, pour une classe C au sens large, la relation

$$\sum_{I \in C, I\ 0-réduit} [\varphi_0(I) + 1] = 3 \sum_{I \in C, I\ 1-réduit} [\varphi_1(I)],$$

ce qui, combiné avec les Théorèmes 1 et 5, permet d'obtenir nos résultats, à l'exception du Théorème 6 dans le cas des classes au sens strict.

Les auteurs cités ci-dessus prouvent le Théorème 1 ([3, p. 65], repris dans [8, p. 1278]), puis le Théorème 3 ([8, Theorem 2, p. 1276]), aprés avoir invoqué, sans preuve, le Théorème 8 ([8, p. 1278, l. 7]). Notre méthode est plus directe, nos démonstrations sont complètes et nous avons obtenu en plus les Théorèmes 2 et 6.

3) Certains auteurs ([7], puis [1]) ont exprimé les sommes $\sum_{I\ 1-réduit} [\varphi_1(I)]$ et $\sum_{I \in C, I\ 1-réduit} [\varphi_1(I)]$ en considérant le sous ensemble $T(D)$ de $S(D)$ où $y \geq 0$. Il apparaît dans leurs formules un terme correctif dont nous pouvons expliquer l'origine.

Soit C une classe d'idéaux au sens large, $t(C)$ le nombre des éléments de $T(D)$ tels que $I\left(\frac{y+\sqrt{D}}{2x}\right) \in C$, $t_1(C)$ le nombre de ceux-ci où $y > 0$, et $t_2(C)$ le nombre de ceux-ci où $y = 0$ et $0 < x < z$. Les idéaux $I\left(\frac{y+\sqrt{D}}{2x}\right)$ et $I\left(\frac{-y+\sqrt{D}}{2z}\right)$ étant équivalents puisque

$I\left(\frac{y+\sqrt{D}}{2x}\right).\ I\left(\frac{-y+\sqrt{D}}{2z}\right)=1$ on voit que

$s(C)=2t_1(C)+2t_2(C)$, $t(C)=t_1(C)+2t_2(C)$

ce qui, compte tenu du Théorème 7, donne

$$t(C)=\sum_{I\in C, I\ 1-réduit}[\varphi_1(I)]+t_2(C).$$

Rappelons qu'un idéal $I=a[1,\varphi]$ est dit ambige s'il est égal à son conjugué, ce qui se traduit par $\varphi+\bar{\varphi}\in\boldsymbol{Z}$. Nous dirons que l'idéal I est super-ambige si $\varphi+\bar{\varphi}\in 2\boldsymbol{Z}$. On voit facilement, directement ou bien en utilisant la description des idéaux ambiges 1-réduits donnée dans [2, p. 267], que $t_2(C)$ est le nombre des idéaux super-ambiges 1-réduits de la classe C. Tenant compte de l'infrastructure des classes ambiges d'idéaux telle que décrite dans [2, Théorème 2], on peut montrer que $t_2(C)$ est égal aux termes correctifs des travaux [7] et [1].

Réferences

[1] E. Dubois: Fraction continue et nombre de classes d'un corps quadratique. Dans Rencontres Arithmétiques de Caen (1995).

[2] F. Halter-Koch, P. Kaplan, K. S. Williams, and Y. Yamamoto: Infrastructure des classes ambiges d'idéaux des ordres des corps quadratiques réels. L'Enseignement Mathématique, **37**, 263–292 (1991).

[3] F. Hirzebruch and D. Zagier: Classification of Hilbert Modular Surfaces. A collection of papers dedicated to K. Kodaira. Iwanami Shoten (1977).

[4] P. Kaplan: Idéaux k-réduits des ordres des corps quadratiques réels. Journal of the Mathematical Society of Japan, **47**, 171–181 (1995).

[5] P. Kaplan and Y. Mimura: Développement en fraction continue à l'entier le plus proche, idéaux α-réduits et un problème d'Eisenstein. Acta. Arithmetica, **76**, 285–304 (1996).

[6] P. Kaplan and K. S. Williams: The distance between ideals in the orders of a real quadratic field. L'Enseignement Mathématique, **36**, 321–358 (1990).

[7] H. Lu: On the class number of real quadratic fields. Scientia Sinica, Special Issue II, 118–130 (1979).

[8] H. Lu: The continued fraction, class number and the others. Scientia Sinica, **26**, 1275-1284 (1984).

[9] D. B. Zagier: A Kronecker Limit Formula for Real Quadratic Fields. Mathematische Annalen, **213**, 153–184 (1975).

[10] D. B. Zagier: Zetafunktionen und quadratische Körper. Springer Hochschultext, Berlin, p. 3 (1981).