156. Comparaison des 2-groupes des classes d'idéaux au sens large et au sens étroit d'un corps quadratique réel

Par Pierre KAPLAN*)

(Comm. by Kenjiro SHODA, M. J. A., Nov. 12, 1974)

Introduction. Soit D un entier sans diviseur carré. Deux idéaux fractionnaires $\mathfrak{a}$ et $\mathfrak{a}'$ du corps $\boldsymbol{Q}(\sqrt{D})$ sont équivalents au sens large s'il existe un nombre λ de $\boldsymbol{Q}(\sqrt{D})$ tel que $\mathfrak{a}=\lambda\mathfrak{a}'$. Si la norme de λ est un nombre positif, $\mathfrak{a}$ et $\mathfrak{a}'$ sont équivalents au sens étroit. Ces deux notions coïncident si le corps $\boldsymbol{Q}(\sqrt{D})$ est imaginaire ($D<0$), ou si $\boldsymbol{Q}(\sqrt{D})$ est réel ($D>0$) et si la norme de son unité fondamentale est -1.

Si au contraire, ce que nous supposons dans tout ce travail, le corps $\boldsymbol{Q}(\sqrt{D})$ est réel et les normes de ses unités positives, c'est-à-dire si D est positif et si l'équation $x^2-Dy^2=-1$ n'a pas de solution en nombres entiers rationnels, chaque classe d'idéaux au sens large se décompose en deux classes au sens étroit. En particulier la classe des idéaux principaux au sens large est formée de la classe I des idéaux principaux engendrés par un nombre de norme positive et de la classe J des idéaux principaux engendrés par un nombre de norme négative. La classe I est la classe unité du groupe (C^*) des classes d'idéaux au sens strict et le groupe $(C^{*\prime})$ des classes d'idéaux au sens large est isomorphe au quotient de (C^*) par le sous-groupe P^* formé de I et de J.

Soient R_n et R'_n les 2^n rangs de (C^*) et de $(C^{*\prime})$, c'est-à-dire les nombres de cycles d'ordre 2^k avec $k\geqslant n$ dans toute décomposition de (C^*) et de $(C^{*\prime})$ en produit direct de groupes cycliques dont l'ordre est puissance de nombre premier. Le but de ce travail est de comparer R_n et R'_n. Nous allons prouver le résultat suivant:

Théorème. *Soit N l'entier bien déterminé tel que la classe J soit une puissance 2^{N-1}-ème, mais ne soit pas une puissance 2^N-ème.*

On a $R'_N=R_N-1$ et $R'_n=R_n$ si $n\neq N$.

Explicitant les conditions sur J pour que $N>1$, puis $N>2$, on trouvera:

Corollaire 1. *On a $R'_1=R_1$ si, et seulement si, D est somme de deux carrés.*

Corollaire 2. *Si $R'_1=R_1$, on a $R'_2=R_2$ si, et seulement si, il existe des décompositions $D=\alpha^2+\beta^2$ où α est impair et résidu quadratique de tous les facteurs premiers impairs de D.*

Une autre formulation du corollaire 1, que nous rappelerons plus

*) 9, rue des Soeurs Macarons, 54000—Nancy, France.

bas, est connue au moins depuis Hilbert ([4], § 77 et 84). Mais le théorème et le corollaire 2 semblent être des résultats nouveaux.

§ 1. Démonstration du théorème. Le théorème est en fait un résultat de théorie des groupes:

Soit G un groupe abélien fini, I son unité, J un élément d'ordre premier q, P le sous-groupe à q éléments, engendré par J, G' le groupe quotient G/P, R_n et R'_n les q^n-rangs de G et de G'.

Considérons une décomposition de G en somme directe de groupes cycliques dont les ordres sont des puissances de nombres premiers; le nombre R_n est le nombre de ces cycles dont l'ordre est q^m avec $m \geqslant n$. Désignons par g_i $(i=1, \cdots, R_1)$ les générateurs dont l'ordre est une puissance q^{n_i} de q, et par h_e ceux dont l'ordre est premier à q. L'ensemble B des g_i et h_e est une base de G.

L'élément J étant d'ordre q, on a $J=\prod_{i\in E} g_i^{q^{n_i-1}}$, où E désigne un sous-ensemble de l'ensemble des nombres $\{1, \cdots, R_1\}$. Soit N la plus petite valeur prise par n_i quand i appartient à E. On a $J=j^{q^{N-1}}$, avec $j=\prod_{i\in E} g_i^{q^{n_i-N}}$, mais il n'existe pas d'élément j' de G tel que $J=j'^{q^N}$; cette propriété caractérise le nombre N. L'élément j est d'ordre q^N.

Soit i_0 un nombre de E tel que $n_{i_0}=N$; posons $g_{i_0}=g$. On a:

$$j=g\prod_{i\in E-i_0} g_i^{q^{n_i-N}} \quad \text{et} \quad g=j\prod_{i\in E-i_0} g^{-q^{n_i-N}}.$$

Donc si on remplace g par j dans la base B, on obtient un ensemble de générateurs de G qui est aussi une base de G, car désignant par H le sous-groupe engendré par les h_e, toute relation $j^{x_{i_0}}\prod_{i\neq i_0} g_i^{x_i}\in H$ entraîne $g^{x_{i_0}}\prod_{i\neq i_0} g_i^{x_i}\in H$, donc x_{i_0} est multiple de q^N, donc x_i multiple de q^{n_i}.

Le groupe G est donc produit direct de groupes cycliques dont l'un est engendré par j et le sous-groupe P est un sous-groupe à q éléments du cycle engendré par j. Donc quand on passe de G à G', le cycle engendré par j, d'ordre q^N, est remplacé par un cycle d'ordre q^{N-1}. Donc $R'_N=R_N-1$ et $R'_n=R_n$ si $n\neq N$. Donc nous avons prouvé le résultat suivant, avec les notations ci-dessus.

Proposition. *Si l'élément J du groupe est une puissance q^{N-1}-ème, mais n'est pas une puissance q^N-ème, on a $R'_N=R_N-1$ et $R'_n=R_n$ si $n\neq N$.*

Le théorème est le cas particulier de la proposition pour $G=(C^*)$, $G'=(C'^*)$ et $q=2$.

Démontrons la proposition d'une autre manière. Le nombre q^{R_n} est le nombre des éléments A de G tels que $A^q=I$ et tels qu'il existe a tel que $A=a^{q^{n-1}}$. Si A est un tel élément de G, AJ est aussi un tel élément si, et seulement si, $n\leqslant N$. En effet, $(AJ)^q=I$ et, d'autre part, $AJ=(aj)^{q^{n-1}}$ si $n\leqslant N$ (car alors J est puissance q^{n-1}-ème), mais si $n>N$, il ne peut exister d'élément j' tel que $AJ=(j')^{q^{n-1}}$, sinon on aurait

$J=(j'a^{-1})^{q^{n-1}}$.

Donc si $n>N$, les éléments A tels que $A^a=I$ et $A=a^{q^{n-1}}$ ne peuvent être congrus modulo P, mais leurs classes dans $G'=G/P$ vérifient $(AP)^q=A^qP=P$ et $AP=a^{q^{n-1}}P=(aP)^{q^{n-1}}$.

Si $n>N$, on a donc $R'_n\geqslant R_n$.

Supposons maintenant $n\leqslant N$. Pour qu'une classe KP de G' soit puissance q^{n-1}-ème et que $(KP)^q=P$, il faut et il suffit, d'une part, que $KP=J^x$ avec $0\leqslant x<q$ et que, d'autre part, il existe un élément k de G tel que $KP=(kP)^{q^{n-1}}=k^{q^{n-1}}P$, donc que $K=k^{q^{n-1}}J^y$ avec $0\leqslant y<q$. Mais comme on suppose $n\leqslant N$, J^y est une puissance q^{n-1}-ème. Donc pour que la classe KP soit une des $q^{R'_n}$ classes qui soit puissance q^{n-1}-ème et telle que $(KP)^q=P$, il faut et il suffit que K soit une classe A, ou bien une classe H telle que $H^q=J^x$ avec $0<x<q$ et qu'il existe h telle que $H=h^{q^{n-1}}$. Il existe des classes H si, et seulement si, $n<N$, et comme si $n\leqslant N$, les q classes AJ^x $(0\leqslant x<q)$ sont congrues modulo P, on voit que $q^{R'_N}=\dfrac{1}{q}q^{R_N}$, donc $R'_N=R_N-1$ et que $q^{R'_n}\geqslant q^{R_n}$ si $n<N$.

On a donc $R'_N=R_N-1$ et $R'_n\geqslant R_n$ si $n\neq N$. Comme l'ordre de G est q fois l'ordre de G', la seule possibilité est que $R'_n=R_n$ si $n\neq N$ C.Q.F.D.

§ 2. Démonstration des corollaires 1 et 2. Cherchons à quelles conditions la classe J des idéaux principaux de norme négative est un carré. Soit d le discriminant du corps $\boldsymbol{Q}(\sqrt{D})$; une classe est un carré dans (C^*) si, et seulement si, la norme d'un idéal premier à d de cette classe donne la valeur 1 à tous les caractères génériques (cf. [3], page 197). Or le nombre $1+\sqrt{d}$ a pour norme le nombre $1-d$, qui est un entier négatif ; l'idéal principal $1+\sqrt{d}$ appartient à la classe J et sa norme en tant qu'idéal est le nombre $|1-d|=d-1\equiv -1 \pmod d$. Donc J est un carré si, et seulement si, -1 donne la valeur 1 à tous les caractères génériques, (ceci est la formulation de Hilbert), ou encore si, et seulement si, D n'est divisible par aucun nombre premier $q\equiv -1 \pmod 4$, ou encore si, et seulement si, D est somme de deux carrés. Ceci démontre le corollaire 1.

Pour démontrer le corollaire 2, il sera indispensable d'utiliser la théorie des formes quadratiques binaires.

On sait que le groupe (C^*) est isomorphe au groupe (C) des classes de formes quadratiques binaires $ax^2+bxy+cy^2=\{a, b, c\}$ à coefficients entiers, telles que $b^2-4ac=d$, où d est le discriminant du corps $\boldsymbol{Q}(\sqrt{D})$ (ce groupe est noté (C_1) dans [6]). Rappelons que la multiplication des classes de (C), dite aussi composition, est donnée par la règle suivante : Deux classes K et K' de (C) étant données, il existe des couples de formes $\{a, b, a'c\}\in K$ et $\{a', b, ac\}\in K'$; la classe de la forme $\{aa', b, c\}$, qui ne dépend que de K et K', est la classe composée de K et de K'.

Cherchons l'image du sous-groupe P^* des classes des idéaux principaux dans (C). Comme la norme du nombre $\sqrt{D}$ est $-D$, il suffit de trouver un représentant de la classe de formes correspondant à la classe de $(\sqrt{D})$. D'après [3], page 213 (cf. aussi [1], chapitre III, § 8. 4), on peut procéder ainsi :

Soit (α_1, α_2) une base de l'idéal $(\sqrt{D})$ telle que $\alpha_1\alpha_2' - \alpha_2\alpha_1' = -D\sqrt{d}$ (α_i' désigne le conjugué de α_i ; comme la norme de l'idéal $(\sqrt{D})$ est $-D$, pour toute base sur $\boldsymbol{Z}$ de l'ideal $(\sqrt{D})$, on a : $\alpha_1\alpha_2' - \alpha_1'\alpha_2 = +D\sqrt{d}$ ou $-D\sqrt{D}$). La forme $g = \frac{1}{D}(\alpha_1 X + \alpha_2 Y)(\alpha_1' X + \alpha_2' Y)$ est une forme de la classe cherchée.

Si $D \not\equiv 1 \pmod 4$, $(1, -\sqrt{D})$ est une base de l'anneau des entiers de $\boldsymbol{Q}(\sqrt{D})$, donc $(\sqrt{D}, -D)$ est une base de l'idéal $(\sqrt{D})$; on a :

$$\sqrt{D}(-D) - (-\sqrt{D})(-D) = -2D\sqrt{D} = -D\sqrt{d}.$$

Donc une forme correspondant à $(\sqrt{D})$ est :

$$\frac{1}{D}(\sqrt{D}X - DY)(-\sqrt{D}X - DY) = -X^2 + DY^2 = \{-1, 0, D\}.$$

Si $D \not\equiv 1 \pmod 4$, $\left(1, \frac{1-\sqrt{D}}{2}\right)$ est une base de l'anneau des entiers de $\boldsymbol{Q}(\sqrt{D})$, la base $\left(\sqrt{D}, \frac{\sqrt{D}-D}{2}\right)$ de l'idéal $(\sqrt{D})$ convient.

Donc une forme correspondant à $(\sqrt{D})$ est :

$$\frac{1}{D}\left(\sqrt{D}X + \frac{\sqrt{D}-D}{2}Y\right)\left(-\sqrt{D}X + \frac{-\sqrt{D}-D}{2}Y\right)$$
$$= -X^2 - XY + \frac{D-1}{4}Y^2 = \left\{-1, -1, \frac{D-1}{4}\right\}.$$

Ainsi P est le sous-groupe à deux éléments de (C) formé des deux classes I représentant 1 (classe unité de (C)) et J représentant -1 et (C') est le quotient du groupe (C) par le sous-groupe P formé des classes I et J représentant 1 et -1 respectivement.

Le fait que J soit un carré signifie que les formes de la classe J représentent des carrés premiers à d, donc que l'équation $-z^2 = x^2 - Dy^2$ si $D \not\equiv 1 \pmod 4$, ou $-z^2 = x^2 + xy + \frac{1-D}{4}y^2$ si $D \equiv 1 \pmod 4$ a des solutions entières, c'est-à-dire (divisant par z^2) que -1 est norme. Le fait que J soit un carré signifie aussi que tous les caractères génériques valent 1 pour -1, ce qui prouve à nouveau le corollaire 1.

Démontrons le corollaire 2. Supposons maintenant que D soit somme de deux carrés : $D = p_1 \cdots p_n$ ou bien $D = 2p_1 \cdots p_m$ où les nombres premiers p_i sont congrus à 1 modulo 4. Soit $D = \alpha^2 + \beta^2$ une décomposition de D où α est impair, et β pair ou impair suivant que D est impair

ou pair.

Si D est pair, $\{\alpha, 2\beta, -\alpha\}^2=\{\alpha^2, 2\beta, -1\}$ et $4\beta^2+4\alpha^2=4D=d$, donc le carré de la classe de $\{\alpha, 2\beta, -\alpha\}$ est J.

Si $D\equiv 1 \pmod 4$, $\left\{\frac{\beta}{2}, \alpha, -\frac{\beta}{2}\right\}^2=\left\{\frac{\beta^2}{4}, \alpha, -1\right\}$ et donc le carré de la classe de $\left\{\frac{\beta}{2}, \alpha, -\frac{\beta}{2}\right\}$ est J.

Inversement, pour toute forme $\{a, b, c\}$, on a:

$$\{a, b, c\}\{-c, b, -a\}=\{-ac, b, -1\}\in J.$$

Donc $\{a, b, c\}^2\in J$ si, et seulement si, les formes $\{a, b, c\}$ et $\{-c, b, -a\}$ sont équivalentes. De là on déduit que toute classe de carré J contient exactement deux formes dont les coefficients extrêmes sont opposés. La démonstration de ce fait se trouve déjà chez Gauss ([2], § 265; cf. aussi [7], chapitre VIII, § 1).

Ainsi les classes H telles que $H^2=J$ sont les classes contenant des formes $\varphi=\{\alpha, 2\beta, -\alpha\}$ si D est pair, ou $\psi=\left\{\frac{\beta}{2}, \alpha, -\frac{\beta}{2}\right\}$ si $D\equiv 1 \pmod 4$. Dans les deux cas, le nombre α est un nombre premier à $2D$ représenté par H pour les valeurs des intéterminées $(1, 0)$ et $(1, 1)$ respectivement, si bien que la classe H est dans le genre principal si, et seulement si, $\left(\frac{\alpha}{p}\right)=e_p(H)=1$ pour tous les diviseurs premiers p impairs de D (cf. [6], § 1; si D est pair, $e_2(H)$ vaut 1 dès que les $e_p(H)$ valent 1, par la formule du produit).

Donc la classe J est une puissance quatrième si, et seulement si, il existe un tel nombre α, ce qui prouve le corollaire 2.

Raisonnant comme dans [8], on trouve aussi le:

Corollaire 3. *Si $R_1'=R_1$ et $R_2=R_2'$, les formes quadratiques $\alpha X^2+2\beta XY-\alpha Y^2$ où α vérifie la condition du corollaire 2 représentent proprement des carrés de nombres m premiers à $2D$.*

On a $R_3'=R_3$ si, et seulement si, au moins un de ces nombres m est résidu quadratique de tous les facteurs premiers impairs de D.

Références

[1] I. Borevitch and I. R. Chafarevich: Théorie des nombres. Gauthiers-Villars.
[2] C. F. Gauss: Disquisitiones Arithmeticae, Werke I.
[3] E. Hecke: Vorlesungen über die Theorie der Algebraischen Zahlen. Chelsea.
[4] D. Hilbert: Die Theorie der Algebraischen Zahlkörper, Werke I. Springer.
[5] P. Kaplan: Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-sous-groupe des classes est cyclique et réciprocité biquadratique. Journal of the Mathematical Society of Japan, **25**, 596–608 (1973).

[6] P. Kaplan: Sur le 2-groupe des classes d'idéaux des corps quadratiques. Journal für die reine und angew. Math. (à paraître).
[7] ——: Cours d'Arithmétique, U. E. R. de Mathématiques. Université de Nancy.
[8] ——: Cycles d'ordre au moins 16 dans le 2-groupe des classes d'idéaux de certains corps quadratiques (à paraître).