数理解析研究所講究録
603 巻 1987 年 169-176

DEUX GROUPE DES CLASSES DE FORMES QUADRATIQUES BINAIRES DEFINIES POSITIVES DE DISCRIMINANT -4^nD EN FONCTION DE n

Pierre KAPLAN

§ 1.- Introduction.

Une forme quadratique binaire $F(x,y)$ à coefficients a, b, c entiers rationnels sera notée $[a,b,c]$; deux formes sont équivalentes si l'on peut passer de l'une à l'autre par une substitution linéaire de déterminant $+1$. Nous ne considérons ici que des formes définies positives, dont le discriminant $b^2 - 4ac$ est donc négatif. L'ensemble des classes des formes primitives, positives, de discriminant $\Delta < 0$ donné, forme un groupe fini G pour la composition qui peut être définie ainsi : si K et K' sont deux classes de G on peut choisir des représentants de la forme $[a,b,a'c] \in K$ et $[a',b,ac] \in K$ et alors $[aa',b,c]$ est un représentant de KK'.
Nous noterons (k) un groupe cyclique d'ordre k.

Nous considérerons ici le groupe $G = G_f$ pour $\Delta = Df^2$ où D est fixe et f variable, et noterons C_n le deux sous-groupe de G_f quand $f = 2^n$. Dans le cas où D est le discriminant du corps quadratique $Q(\sqrt{D})$, le groupe G_f est isomorphe au groupe des classes d'idéaux premiers à f de l'anneau de conducteur f de $Q(\sqrt{D})$, et les groupes C_n interviennent dans les problèmes de représentations de nombres premiers par des formes quadratiques binaires (voir par exemple l'exposé de Franz Halter-Koch).

Notre point de départ sera les résultats suivants, dus à Gauss : [2, § 253-257] qui nous permettront de passer du discriminant D au discriminant Df^2 :

A) Il existe un homomorphisme surjectif θ de G_f sur G_1 défini ainsi : toute classe K de G_f contient des représentants de la forme $[a,bf,cf^2]$ avec $(a,Df) = 1$; pour tout tel représentant la classe $\theta(K)$ contient la forme $[a,b,c]$. Le noyau H de θ est formé des classes $K \in G_f$ représentant f^2.

/

B) Si $f = 2$ et $D < 0$ on a

$$\text{card } H = 2 \quad \text{si} \quad D \text{ est pair,}$$

$$\text{card } H = 1 \quad \text{si} \quad D \equiv 1 \pmod 8 \quad \text{ou} \quad D = -3 ,$$

$$\text{card } H = 3 \quad \text{si} \quad D \equiv 5 \pmod 8 , \ D < -3 .$$

(Le résultat A est vrai aussi si $D > 0$) .

Comme nous voulons examiner ce que devient le 2-groupe des classes quand on multiplie le discriminant par des puissances de 4 , il est clair qu'il suffit de partir d'un discriminant "2-fondamental", c'est-à-dire :

$$D = -m \ , \ m \equiv 3 \pmod 4 \quad m > 0 ,$$

$$D = -4m \ , \ m \equiv 1 \pmod 4 \quad m > 0 ,$$

$$D = -8m \ , \ m \text{ impair} \quad m > 0$$

et de chercher comment varie le groupe C_n quand n augmente.
Pour cela nous remarquons que le 2-rang r_n de C_n a aussi été déterminé par Gauss, à savoir :

C) Si le discriminant D est 2-fondamental on a :

$D = -m$, $m \equiv 3 \pmod 4$: $r_1 = r_0$, $r_2 = r_0 + 1$, $r_n = r_0 + 2$ pour $n \geq 3$;

$D = -4m$, $m \equiv 1 \pmod 4$: $r_1 = r_0$, $r_n = r_1 + 1$ pour $n \geq 2$;

$D = -8m$, m impair : $r_n = r_0 + 1$ pour $n \geq 1$.

Tenant compte de A), B) et C) on voit que :

1) Si $D = -m$, $C_1 = C_0$, $C_2 = C_0 \times (2)$, $C_3 = C_0 \times (2) \times (2)$.

2) Si $D = -4m$, $C_2 = C_1 \times (2)$.

3) Si $D = -8m$, $C_1 = C_0 \times (2)$.

Il reste à examiner ce qui se passe quand on passe de C_n à C_{n+1} sans que le 2-rang augmente. Le groupe C_{n+1} est produit d'autant de cycles que le groupe C_n , mais un de ces cycles est deux fois plus long. Si l'on pouvait

déterminer chaque fois quel cycle devient plus long, on aurait résolu le problème de la structure de C_n . Malheureusement ce n'est possible que dans certains cas dont nous allons parler maintenant.

§ 2.- Détermination du groupe C_n dans certains cas.

a) Caractères génériques : Soit $m = p_1^{s_1} \dots p_k^{s_k}$ où les nombres p_i sont des nombres premiers. Soit x un nombre premier à $2m$ représenté par une classe K de discriminant $\Delta = 4^n D$. Les caractères génériques de K sont les symboles de Legendre $\left(\frac{x}{p_i}\right)$ pour un entier x représenté par K et, suivant les valeurs de D et n , certaines des expressions (caractères supplémentaires) $\varepsilon = (-1)^{\frac{x-1}{2}}$, $\eta = (-1)^{\frac{x^2-1}{8}}$, $\varepsilon\eta$ et leurs produits.

Une classe est un carré si, et seulement si, tous les caractères génériques de cette classe valent 1 .

Les classes d'ordre 2 (ou classes ambiguës) forment un sous-groupe du groupe des classes dont nous connaissons des générateurs. En raisonnant sur ces générateurs et leurs caractères génériques, nous obtiendrons des informations sur la structure des groupes C_n .

b) Cas où $D = -m$, $m \equiv 3 \pmod 4$: Comme $C_0 = C_1$ nous partons de $n = 1$, et donnons un ensemble de générateurs des classes ambiguës

	$n = 1$	2	3	4
	$\Delta = 4D$	$16D$	$64D$	$256D$
Caractères	$\left(\frac{x}{p_i}\right)$	$\left(\frac{x}{p_i}\right), \varepsilon$	$\left(\frac{x}{p_i}\right), \varepsilon, \eta$	Idem
Classes ambiguës génératrices	$\left[p_i^s, 0, \frac{m}{p_i^s}\right]$	$\left[p_i^s, 0, \frac{4m}{p_i^s}\right]$	$\left[p_i^s, 0, \frac{16m}{p_i^s}\right]$	$\left[p_i^s, 0, \frac{64m}{p_i^s}\right]$
		$[4,0,m]$	$[16,0,m]$	$[64,0,m]$
			$[4,4,1+4m]$	$[4,4,1+16m]$

Pour avoir un système de générateurs indépendants des classes ambiguës il suffit d'enlever une forme parmi celles de la première ligne. Remarquons que, à partir de $\Delta = 16D$, la forme de la deuxième ligne n'est jamais dans le genre principal, et que la forme de la troisième ligne l'est toujours à partir de $\Delta = 256D$. De plus si le 4-rang de $C_0 = C_1$ est nul, ce qui est le cas si m est un nombre premier, aucune forme de la première ligne n'est dans le genre principal, et donc, quel que soit $n \geq 4$, il n'y a qu'un seul cycle de longueur > 2 , donc $C_n = C_0 \times (2) \times (2^{n-2}) = (2)^k \times (2^{n-2})$ pour $n \geq 2$.

c) Cas $D = -8m$, m impair : Ici nous partons de $n = 0$ et écrivons un ensemble de générateurs des classes ambiguës

	$n = 0$	1	2
	$\Delta = 4D$	$4D$	$16D$
Caractères	$\left(\frac{x}{p_i}\right)$, η ou $\varepsilon\eta$	$\left(\frac{x}{p_i}\right)$, ε , η	$\left(\frac{x}{p_i}\right)$, ε , η
Classes ambiguës génératrices	$\left[p_i^s, 0, \frac{2m}{p_i^s}\right]$	$\left[p_i^s, 0, \frac{8m}{p_i^s}\right]$	$\left[p_i^s, 0, \frac{32m}{p_i^s}\right]$
	$[2,0,m]$	$[8,0,m]$	$[32,0,m]$
		$[4,4,1+2m]$	$[4,4,1+8m]$

Un système de générateurs indépendants s'obtient ici en omettant une forme des deux premières lignes (on aurait pu omettre la deuxième ligne). On voit, plus haut, que, si le 4-rang de C_0 est nul, on a

$$C_n = C_0 \times (2^{n-1}) \qquad (n \geq 0) \ .$$

Dans certains cas on peut obtenir aussi des informations partielles. Si, par exemple, le 4-rang de C_0 est égal à son 2-rang, c'est-à-dire si toutes les classes ambiguës sont dans le genre principal et si $m \equiv 1 \pmod 8$ alors

$$C_1 = C_0 \times (2) \quad , \quad C_2 = C_0 \times (4) \ .$$

d) Cas $D = -4m$, $m \equiv 1 \pmod 4$: Commençons par étudier le passage de $n = 0$ à $n = 1$

	$n = 0$, $\Delta = -4m$	$n = 1$, $\Delta = -16m$
Caractères	$\left(\frac{x}{p_i}\right), \varepsilon$	$\left(\frac{x}{p_i}\right), \varepsilon$
Classes ambiguës génératrices	$\left[p_i^s, 0, \frac{m}{p_i^s}\right]$	$\left[p_i^s, 0, \frac{4m}{p_i^s}\right]$

$$\left[2,2,\frac{1+m}{2}\right] \xleftarrow{\ \theta\ } \left(\left[8,4,\frac{1+m}{2}\right]\right) \xrightarrow{\text{carré}} [4,0,m]$$

Ici les classes de la première ligne pour $n = 0$ engendrent un sous-groupe du groupe des classes ambiguës que nous appellerons "classes impaires". Une image inverse par θ de la classe de $\left[2,2,\frac{1+m}{2}\right]$ est la classe de $\left[8,4,\frac{1+m}{2}\right]$, dont le carré est la classe de $[4,0,m]$, élément non trivial du noyau de θ .

Ceci permet de conclure dans le cas où aucune classe impaire n'est dans le genre principal. Alors

$$C_0 = (2)^{k-1}(2^t)$$

avec $t > 1$ si, et seulement si, $m \equiv 1 \pmod 8$, et on a

$$C_1 = (2)^{k-1}(2^{t+1}) .$$

Tenant compte de A), B) et C) on voit en outre que, dans tous les cas,

$$C_2 = C_1 \times (2) .$$

Nous allons maintenant considérer le passage de C_2 à C_n pour $n > 2$.

	$n = 2$, $\Delta = -64m$	$n = 3$, $\Delta = -256m$
Caractères	$\left(\frac{x}{p_i}\right), \varepsilon, \eta$	$\left(\frac{x}{p_i}\right), \varepsilon, \eta$
Classes ambiguës génératrices	$\left[p_i^{s_i}, 0, \frac{16m}{p_i^{s_i}}\right]$	$\left[p_i^{s_i}, 0, \frac{64m}{p_i^{s_i}}\right]$
	$[16,0,m]$	$[64,0,m]$
	$[4,4,1+4m]$	$[4,0,1+16m]$

On voit donc que, si aucune classe impaire (pour $n = 0$) n'est dans le genre principal et que si, en outre, $m \equiv 5 \pmod 8$, on a

$$C_n = (2)^k \times (2^n) \qquad n \geq 2 .$$

Si $m \equiv 1 \pmod 8$ on a $C_2 = (2)^k(2^{t+1})$ et $C_3 = (2)^{k-1}(4)(2^{t+1})$ car le 2-groupe C_3 contient deux cycles d'ordre ≥ 4 . Mais on ne peut savoir "quel cycle" devient plus long quand n augmente ensuite.

En résumé nous avons démontré le résultat suivant

Théorème : Supposons que le 4-rang du groupe des classes de formes quadratiques de discriminant négatif et 2-fondamental D soit nul. Alors la structure des 2-groupes des classes de formes quadratiques de discriminant 4^nD est déterminée par son 2-rang et la condition qu'un invariant au plus ait une longueur > 2 . Plus précisément, posant $m = p_1^{s_1} \ldots p_k^{s_k}$ on a :

$D = -m$, $m \equiv 3 \pmod 4$: $C_0 = C_1 = (2)^{k-1}$, $C_n = (2)^k(2^{n-2})$ pour $n \geq 2$;

$D = -8m$, m impair : $C_n = (2)^k(2^{n-2})$

$D = -4m$, $m \equiv 1 \pmod 4$: $C_0 = (2)^k$, $C_1 = (2)^{k-1}(4)$, $C_n = (2)^k(2^n)$ pour $n \geq 2$.

§ 3.- Applications.

Voici deux exemples d'application de ces résultats :

Considérons le cas de $D = -4p$ où $p \equiv 1 \pmod 8$, ou alors $C_0 = (2^r)$ avec $r \geq 1$, et soit q un autre nombre premier $\equiv 1 \pmod 4$ tel que $\left(\frac{q}{p}\right) = 1$. Alors le nombre q est représenté par une classe de discriminant $-4p$ qui est un carré, et un raisonnement dont le principe (pour $p = 17$) remonte à Dirichlet montre que le nombre q est représenté par une classe puissance quatrième si, et seulement si, $\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4$, autrement dit, comme on le sait depuis Scholz [7], si $\left(\frac{\varepsilon_p}{q}\right) = 1$ (ou $\left(\frac{\varepsilon_q}{p}\right) = 1$). Que se passe-t-il si $p \equiv 5 \pmod 8$? Alors $C_0 = (2)$ donc la question n'a pas de sens, mais comme $C_1 = (4)$, on peut penser qu'il suffit de considérer les classes de discriminant $-16p$, et, on trouve en fait que, dans ce groupe, q est représenté par une puissance quatrième si, et seulement si, $\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = 1$.

Voici un autre exemple, dû à Halter-Koch [2] et Ishii [7], que l'on peut interpréter de la même manière.

Soit p un nombre premier $\equiv 7 \pmod 8$ et $D = -p$. Dans ce cas $C_0 = (1)$, C_n contient un cycle d'ordre 4 pour $n = 4$ et d'ordre 8 pour $n = 5$. Soit alors $q \equiv 1 \pmod 8$ un nombre premier tel que $\left(\frac{p}{q}\right) = 1$, si bien que q est représenté par un carré dans tous les groupes de discriminant $-4^n p$. Le résultat que l'on trouve est que q est représenté par une puissance quatrième dans le groupe des classes de discriminant $-256p$ si, et seulement si, $\left(\frac{\varepsilon_p}{q}\right)_4 = 1$, et que alors q est représenté par une puissance huitième dans le groupe des classes de discriminant $-1024p$ si, et seulement si, $\left(\frac{\varepsilon_p}{q}\right)_8\left(\frac{q}{2}\right)_4 = 1$.

Bibliographie

[1] DIRICHLET-DEDEKIND, Vorlesungen über Zahlentheorie, 4ème Edition, Chelsea, New York, (1968).

[2] GAUSS, Disquisitiones Arithmeticae.

[3] F. HALTER-KOCH, Konstruktion von Klassenkörpern und Potenzrestkriterien für Quadratische Einheiten. Manuscripta Math., 54, 453-492 (1986).

[4] N. ISHII, On the eighth power residue of totally positive quadratic units. Preprint.

[5] A. SCHOLZ, Über die Lösbarkeit der Gleiching $t^2 - Du^2 = 4$. Math. Zeitschrift 39 (1935), 95-111.