MÉMOIRES DE LA S. M. F.

T. A. SPRINGER

Caractères quadratiques de groupes abéliens finis et sommes de Gauss

Mémoires de la S. M. F., tome 48 (1976), p. 103-115

<http://www.numdam.org/item?id=MSMF_1976__48__103_0>

Col. sur les Formes Quadratiques (1975, Montpellier)
Bull. Soc. Math. France
Mémoire 48, 1976, p. 103-115

CARACTERES QUADRATIQUES DE GROUPES ABELIENS FINIS ET SOMMES DE GAUSS

par

T. A. SPRINGER

Dans cette note on discute d'abord, au paragraphe 1, des propriétés générales (très élémentaires) des sommes de Gauss associées à un caractère quadratique sur un groupe abélien fini. Mentionnons, en particulier, la "formule de réciprocité" de 1.7.

Au paragraphe 2, nous donnons quelques exemples, et au paragraphe 3 on indique comment obtenir dans le contexte des sommes de Gauss, des lois de réciprocité, tel que celui de A. Weil [6] pour les formes quadratiques sur un corps de nombres. Des résultats analogues de Knebusch sont discutés brièvement dans [3, App. 4]. On indique aussi au paragraphe 3 comment la démonstration donnée par Siegel [4] de la loi de réciprocité dans un corps de nombres (de Hecke-Hasse) se transpose dans notre contexte.

1. Bicaractères et caractères quadratiques

1.1. Soit A un groupe abélien additif. Un bicaractère de A est une fonction $f : A \times A \to \mathbb{C}^*$ qui est multiplicative en chacune des variables si l'autre est constante. f est symétrique si $f(x,y) = f(y,x)$ pour tout $x,y \in A$.

Supposons f symétrique. Le noyau N_f de f est le sous-groupe

$$N_f = \{x \in A \mid f(x,A) = 1\} .$$

f est non-dégénéré si $N_f = 0$. Deux éléments $x,y \in A$ (ou deux sous-ensembles S,T de A) sont orthogonaux si $f(x,y) = 1$ (resp. $f(S,T) = 1$). Si B est un sous-groupe de A, on désigne par $B^{\perp}$ le sous-groupe orthogonal :

$$B^{\perp} = \{x \in A \mid f(x,B) = 1\} .$$

Un caractère quadratique de A est une fonction $\theta : A \to \mathbb{C}^*$ telle que $f_\theta : (x,y) \mapsto \theta(x+y)\,\theta(x)^{-1}\,\theta(y)^{-1}$ soit un bicaractère, c'est le bicaractère (symétrique) associé à θ. Le noyau N_θ de θ est celui de f_θ. La restriction de θ à N_θ est un caractère de N_θ, son noyau est le radical R_θ de θ. Nous dirons que θ est non-dégénéré si $R_\theta = 0$ et non-défectif si $N_\theta = 0$.

Soit θ un caractère quadratique de A et posons $f_\theta(x,y) = \langle x,y\rangle$, donc

$$\theta(x+y) = \theta(x)\,\theta(y)\,\langle x,y\rangle \tag{1}$$

On tire de (1)

(2) $$\theta(nx) = \theta(x)^n \langle x,x\rangle^{\frac{1}{2}n(n-1)} \qquad (n \in \mathbb{Z}) \ .$$

Le lemme suivant est une conséquence directe de (2). μ_d dénote le groupe des racines $d^{\text{ième}}$ de l'unité.

1.2. Lemme. Si $x \in A$ a ordre d, alors $\theta(x) \in \mu_d$ si d est impair et $\theta(x) \in \mu_{2d}$ si d est pair.

1.3. Lemme. Il existe des caractères $\chi : A \to \mathbb{C}^*$ et $\varepsilon : A \to \{1,-1\}$ tels que

(3) $$\theta(-x) = \chi(x)\,\theta(x)$$

(4) $$\theta(x)^2 = \varepsilon\chi(x)\,\langle x,x\rangle$$

Posons $\theta'(x) = \theta(-x)$, alors θ' est un caractère quadratique avec $f_{\theta'} = f_\theta$, d'où l'existence d'un caractère χ satisfaisant (3). On voit pareillement qu'il existe un caractère μ de A avec $\theta(x)^2 = \mu(x)\,\langle x,x\rangle$. Alors :

$$\mu(-x)\,\langle x,x\rangle = \theta(-x)^2 = \chi(x)^2\,\theta(x)^2 = \chi(x)^2\,\mu(x)\,\langle x,x\rangle \ ,$$

d'où l'on voit que $\varepsilon = \chi^{-1}\mu$ a les propriétés requises.

1.4. Dorénavant, nous supposerons A fini. Alors les valeurs de θ sont des racines de l'unité, d'après 1.2. La somme de Gauss $s(\theta\ ;\ A)$ est définie par

$$s(\theta\ ;\ A) = \sum_{x \in A} \theta(x) \ .$$

θ définit un caractère quadratique $\bar{\theta}$ du groupe A/R_θ et il est clair que

$$s(\theta\ ;\ A) = |R_\theta|\ s(\bar{\theta}\ ;\ A/R_\theta) \ .$$

1.5. Lemme. (i) Pour que $s(\theta\ ;\ A) \neq 0$ il faut et il suffit que $R_\theta = N_\theta$;
(ii) Si $s(\theta\ ;\ A) \neq 0$ on a $|s(\theta,A)| = |A|^{1/2}\,|R_\theta|^{1/2}$.

On a :

$$|s(\theta\ ;\ A)|^2 = \sum_{x,y \in A} \theta(x)\,\theta(y)^{-1} = \sum_{x,y \in A} \theta(x)\,\langle x,y\rangle^{-1} =$$

$$= |A| \sum_{x \in N_\theta} \theta(x) \ ,$$

ce qui implique les assertions du lemme.

1.6. Nous posons

$$\gamma(\theta\ ;\ A) = |A|^{-1/2}\,|R_\theta|^{-1/2}\ s(\theta\ ;\ A) \ .$$

D'après 1.5., on a $|\gamma(\theta\ ;\ A)| = 0$ ou 1.

Supposons θ non-défectif (alors $|\gamma(\theta\ ;\ A)| = 1$, d'après 1.5.). Si B est un sous-groupe de A et $B^\perp$ l'orthogonal (par rapport à f_θ), on a $(B^\perp)^\perp = B$ et $|B^\perp| = |A|\,|B|^{-1}$. Nous dirons que B est bon (pour θ) si $\theta|B \cap B^\perp = 1$. C'est le cas, par exemple, si $B \cap B^\perp = 0$ (B non-dégénéré) ou si $\theta|B = 1$ (B isotrope).

Le théorème suivant donne une formulation générale de la "formule de réciprocité des sommes de Gauss".

1.7. Théorème. Si B est un bon sous-groupe de A, alors

(5) $$\gamma(\theta\ ;\ A) = \gamma(\theta|B\ ;\ B)\ \gamma(\theta|B^{\perp}\ ;\ B^{\perp}) \quad .$$

On a :

$$s(\theta\ ;\ A)\ \overline{s(\theta|B^{\perp}\ ;\ B^{\perp})} = \sum_{\substack{x\in A \\ y\in B^{\perp}}} \theta(x)\ \theta(y)^{-1} = \sum_{\substack{x\in A \\ y\in B^{\perp}}} \theta(x)\ \langle x,y\rangle = |B^{\perp}|\ s(\theta|B\ ;\ B).$$

Comme $N_{\theta|B} = N_{\theta|B^{\perp}} = B \cap B^{\perp}$, il résulte de 1.5. (i), que $s(\theta|B\ ;\ B) \neq 0$, $s(\theta|B^{\perp}\ ;\ B^{\perp}) \neq 0$. La relation précédente et 1.5. (ii) impliquent alors 1.7.

Mentionnons explicitement quelques cas particuliers.

1.8. Corollaire. (i) Si B est un sous-groupe non dégénéré de A, alors $\theta|B$ et $\theta|B^{\perp}$ sont des caractères quadratiques non-défectifs de B et $B^{\perp}$, et on a (5).

(ii) Si B est un sous-groupe isotrope de A, alors :

$$\gamma(\theta\ ;\ A) = \gamma(\theta|B^{\perp}\ ;\ B^{\perp}) \quad .$$

1.9. Corollaire. Soit A_p la composante p-primaire de A. Alors A_p est un sous-groupe non-dégénéré de A, $\theta_p = \theta|A_p$ est un caractère quadratique non-défectif de A_p et on a

$$\gamma(\theta\ ;\ A) = \prod_p \gamma(\theta_p\ ;\ A_p) \quad .$$

Si B est un sous-groupe tel que $|B|$ et $|B^{\perp}|$ soient relativement premiers, il est clair que $B \cap B^{\perp} = 0$, par conséquent B est non-dégénéré. 1.9. résulte de cette remarque et de 1.8. (i).

Pour calculer $\gamma(\theta\ ;\ A)$ on peut se servir du résultat suivant (qui remonte à Minskowski).

Soit A un groupe abélien fini, soit f un bicaractère symétrique non-dégénéré de A. Nous dirons qu'un sous-groupe B est non-dégénéré pour f si $f|B$ l'est.

1.10. Proposition. Il existe une décomposition en somme directe $A = \bigoplus_h A_h$ où les A_h sont des sous-groupes non-dégénérés deux à deux orthogonaux, et de l'une des deux formes suivantes :

(a) un groupe cyclique,

(b) somme directe de deux 2-groupes cycliques de même ordre.

Il suffit de démontrer 1.10. dans le cas où A est un p-groupe. Nous raisonnons par récurrence sur A, le cas $|A| = p$ étant trivial. Soit p^e l'ordre maximal des éléments de A.

Supposons d'abord p impair. Si $f(x,x) \in \mu_{p^{e-1}}$ pour tout $x \in A$, on aurait $f(x,y)^2 \in \mu_{p^{e-1}}$ $(x,y \in A)$, d'où $f(p^{e-1}A,A) = 1$, une contradiction. Donc il existe $x \in A$ d'ordre p^e avec $f(x,x) \in \mu_{p^e} - \mu_{p^{e-1}}$. Soit B le sous-groupe cyclique engendré par x. Alors B est non-dégénérée, on a une décomposition orthogonale $A = B \oplus B^{\perp}$ et l'assertion résulte en appliquant l'hypothèse de récurrence à $B^{\perp}$.

Dans le cas $p = 2$, il reste à considérer le cas où $f(x,x) \in \mu_{2^{e-1}}$ pour tout $x \in A$. Soit $\zeta = e^{\pi i/2^{e-1}}$. On voit facilement qu'il existe $x,y \in A$ ayant ordre 2^e et tels que $f(x,y) = \zeta$. Alors $f(x,x) = \zeta^a$, $f(y,y) = \zeta^b$ où a et b sont pairs.

Si $mx + ny \in B \cap B^{\perp}$, alors :

$$ma + n \equiv m + bn \equiv 0 \pmod{2^e},$$

d'où $m \equiv n \equiv 0 \pmod{2^e}$. Par conséquent, B est la somme directe des groupes cycliques engendrés par x et y, et $B \cap B^{\perp} = 0$. L'assertion résulte encore par récurrence.

Soit maintenant θ un caractère quadratique non-défectif de A. Si les A_h sont comme dans 1.10, avec $f = f_\theta$, alors il résulte de 1.8. (i) et 1.10. que

$$\gamma(\theta\ ;\ A) = \prod_h \gamma(\theta|A_h\ ;\ A_h) \quad .$$

Ceci réduit le calcul de $\gamma(\theta\ ;\ A)$ (théoriquement, au moins) au cas où A a l'une des deux formes de 1.10.

2. Exemples

Dans ce numéro nous discuterons un nombre d'exemples.

2.1. Groupes cycliques.

Soit $A = \mathbb{Z}/n\mathbb{Z}$, soit θ un caractère quadratique non-défectif de A. Nous l'identifions à une fonction sur $\mathbb{Z}$, similairement pour f_θ. Posons $\zeta = e^{\pi i/n}$. Si $x,y \in \mathbb{Z}$ on a :

$$\langle x,y \rangle = \zeta^{2uxy} \quad ,$$

où $(u,x) = 1$. Alors $x \mapsto \theta(x)\,\zeta^{-ux^2}$ est un caractère et on voit qu'il existe $v \in \mathbb{Z}$ avec

$$\theta(x) = \zeta^{ux^2+vx} \quad . \tag{1}$$

Comme $\theta(x+n) = \theta(x)$, on a $un + v \equiv 0 \pmod 2$. (1) donne la forme générale d'un caractère quadratique non-défectif sur $\mathbb{Z}/n\mathbb{Z}$. Ecrivons $\theta = \theta_{u,v}$, $\gamma(u,v\ ;\ n) = \gamma(\theta_{u,v}\ ;\ \mathbb{Z}/n\mathbb{Z})$.

Si n est impair on a :

$$\gamma(u,v\ ;\ n) = \gamma(4u,2v\ ;\ n) \quad ,$$

et on constate facilement que

$$\gamma(4u,2v\ ;\ n) = \zeta^{-4uw^2}\ \gamma(4u,0\ ;\ n)\quad ,$$

où $4uw + v \equiv 0 \pmod{n}$. Or

$$\gamma(4u,0\ ;\ n) = n^{-1/2} \sum_{x=1}^{n} e^{4\pi i u x^2/n}\quad .$$

La somme est une somme de Gauss ordinaire, de valeur $(\frac{2u}{n})\ i^{(\frac{n-1}{2})^2}\ n^{1/2}$ [2, p. 153] (symbole de Jacobi).

Si n est pair on a

$$\gamma(u,v\ ;\ n) = \zeta^{-uw^2}\ \gamma(u,0\ ;\ n)\quad ,$$

où maintenant $uw + \frac{1}{2}\, v \equiv 0 \pmod{n}$, et

$$\gamma(u,0\ ;\ n) = \frac{1}{2}\, n^{-1/2} \sum_{x=1}^{2n} e^{2\pi i u x^2/2n}\quad .$$

C'est encore une somme de Gauss ordinaire.

2.2. Dans la situation de 2.1., soit $n = ab$ où $(a,b) = 1$. Posons $B = a\,\mathbb{Z}/n\,\mathbb{Z} \simeq \mathbb{Z}/b\,\mathbb{Z}$. Alors B est un sous-groupe non-dégénéré de A et $B^{\perp} = b\,\mathbb{Z}/n\,\mathbb{Z} \simeq \mathbb{Z}/a\,\mathbb{Z}$. Application de 1.7. donne la formule de réciprocité

$$\gamma(u,v\ ;\ n) = \gamma(au,v\ ;\ b)\ \gamma(bu,v\ ;\ a)\quad . \tag{2}$$

Si n est impair, $u = 2$ et $v = 0$, alors (2) implique la loi de réciprocité quadratique $(\frac{a}{b})\ (\frac{b}{a}) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$, si $a > 0$, $b > 0$.

2.3. Considérons maintenant le cas d'un groupe A du type (b) de 1.10. Soit θ un caractère quadratique non-défectif de A, tel que le bicaractère associé f_θ soit comme dans le dernièr alinéa de la démonstration de 1.10. Identifions θ à une fonction sur $\mathbb{Z} \times \mathbb{Z}$. Posons $|A| = 2^{2e}$, $\zeta = e^{\pi i/2^{e-1}}$. Il résulte de la démonstration de 1.10. que nous pouvons supposer que :

$$\theta(x,y) = \zeta^{ax^2+xy+by^2+cx+dy}\quad ,$$

où a et b sont pairs. Prenons d'abord $c = d = 0$, et écrivons $\tilde{\gamma}(a,b\ ;\ e) = \gamma(\theta\ ;\ A)$.

Si $e > 1$, le sous-groupe $B = 2^{e-1}A$ est isotrope (voir 1.6.), on a $B = 2A$. Application de 1.8. (ii) montre que :

$$\tilde{\gamma}(a,b\ ;\ e) = \tilde{\gamma}(a,b\ ;\ e-2)\quad (e \geqslant 2)\quad ,$$

d'où

$$\tilde{\gamma}(a,b\ ;\ e) = 1\quad (e\ \text{pair})$$

$$\tilde{\gamma}(a,b\ ;\ e) = (-1)^{ab}\quad (e\ \text{impair})\quad .$$

Dans le cas général, on réduit le calcul de $\gamma(\theta\ ;\ A)$ au cas $c = d = 0$ par une translation des variables, ce qui introduit un facteur supplémentaire.

2.4. Formes quadratiques sur un corps fini

Soit k un corps fini à q éléments, de caractéristique p. Nous désignons par χ le caractère de $\mathbb{F}_p$ avec $\chi(n \bmod p) = e^{2\pi in/p}$.

Soit V un espace vectoriel sur k, de dimension finie et Q une forme quadratique sur V. Alors

$$\theta(v) = \chi(\mathrm{Tr}_{k/\mathbb{F}_p} Q(v))$$

définit un caractère quadratique sur le groupe V. Nous supposerons θ non-défectif ce qui veut dire que Q est non-dégénérée si $p \neq 2$ et non défective si $p = 2$.

Soit d'abord $p \neq 2$. On désigne par τ_k le caractère non trivial d'ordre 2 de k^*. On a

$$\tau_k(x) = \tau_{\mathbb{F}_p}(N_{k/\mathbb{F}_p} x) ,$$

et

$$\tau_{\mathbb{F}_p}(n \bmod p) = \left(\frac{n}{p}\right) .$$

Soit $(e_1,\ldots,e_m)$ une base orthogonale de V par rapport à Q et posons $V_i = ke_i$. D'après 1.8. (i), on a :

$$\gamma(\theta ; V) = \prod_{i=1}^{m} \gamma(\theta|V_i ; V_i) ,$$

ce qui réduit la détermination de $\gamma(\theta ; V)$ au cas où $\dim V = 1$.

Supposons d'abord $k = \mathbb{F}_p$. Si $\dim V = 1$, le calcul des sommes de Gauss montre que :

$$\gamma(\theta ; V) = i^{(\frac{p-1}{2})^2} \cdot \tau_{\mathbb{F}_p}(Q(e_1)) ,$$

d'où dans le cas général

$$\gamma(\theta ; V) = i^{m(\frac{p-1}{2})^2} \tau_{\mathbb{F}_p}(\delta) ,$$

où $\delta = Q(e_1) \ldots Q(e_m)$.

Si k est quelconque et $\dim V = 1$, on voit que θ est le caractère quadratique défini par une forme quadratique $x \mapsto \mathrm{Tr}_{k/\mathbb{F}_p}(ax^2)$ sur k, considéré comme espace vectoriel sur $\mathbb{F}_p$. D'après ce qui précède, on aura :

$$\gamma(\theta ; V) = i^{d(\frac{p-1}{2})^2} \tau_{\mathbb{F}_p}(\delta_a) ,$$

où $d = [k : \mathbb{F}_p]$ et où δ_a est le déterminant de la forme bilinéaire $(x,y) \mapsto \mathrm{Tr}_{k/\mathbb{F}_p}(axy)$ sur k, par rapport à une base $(x_1,\ldots,x_d)$ de k sur $\mathbb{F}_p$. Alors :

$$\delta_a = N_{k/\mathbb{F}_p}(a)\, \xi^2 ,$$

où

$$\xi = \det (x_i^{q^{j-1}})_{1 \leqslant i,j \leqslant d} .$$

Or $\xi^q = (-1)^{d-1}\xi$, d'où

$$\tau_{\mathbb{F}_p}(\xi^2) = (-1)^{d-1} \quad .$$

Mettant tout cela ensemble on trouve finalement, dans le cas général

$$\gamma(\theta\ ;\ V) = i^{md(\frac{p-1}{2})^2+2m(d-1)}\ \tau_k(\delta) \quad ,$$

où $d = [k : \mathbb{F}_p]$, $m = \dim V$, $\delta = Q(e_1) \ldots Q(e_m)$. On notera que

$$\gamma(\theta\ ;\ V)^2 = \tau_k(-1)^m \quad .$$

2.5. Soit maintenant $p = 2$. La forme Q étant non-défective, $m = \dim V$ est pair. Soit $(e_i)_{1 \leqslant i \leqslant m}$ une base symplectique de V. Soit V_i $(1 \leqslant i \leqslant \frac{1}{2}m)$ le sous-espace engendré par e_i, $e_{i+1/2m}$. Alors :

$$\gamma(\theta\ ;\ V) = \prod_{i=1}^{1/2m} \gamma(\theta|V_i\ ;\ V_i) \quad ,$$

ce qui nous réduit au cas $\dim V = 2$.

Supposons $\dim V = 2$ et soit (e,f) une base symplectique. Alors :

$$Q(xe+yf) = ax^2+xy+by^2$$

où $a,b \in k$. On a :

$$\gamma(\theta\ ;\ V) = q^{-1} \sum_{x,y \in k} (-1)^{\mathrm{Tr}_{k/\mathbb{F}_2}(ax^2+xy+by^2)} \quad .$$

Comme :

$$\mathrm{Tr}_{k/\mathbb{F}_2}(x^2) = (\mathrm{Tr}_{k/\mathbb{F}_2}(x))^2 = \mathrm{Tr}_{k/\mathbb{F}_2}(x) \quad ,$$

on a aussi :

$$\gamma(\theta\ ;\ V) = q^{-1} \sum_{x,y \in k} (-1)^{\mathrm{Tr}_{k/\mathbb{F}_2}(a_1x+xy+b_1y)} \quad ,$$

où $a_1^2 = a$, $b_1^2 = b$. Un calcul facile montre alors que

$$\gamma(\theta\ ;\ V) = (-1)^{\mathrm{Tr}_{k/\mathbb{F}_2}(a_1b_1)} = (-1)^{\mathrm{Tr}_{k/\mathbb{F}_2}(ab)} \quad .$$

Ceci implique que dans le cas général on a :

$$\gamma(\theta\ ;\ V) = (-1)^{\mathrm{Tr}_{k/\mathbb{F}_2}(\Delta(Q))}$$

où $\Delta(Q)$ est l'invariant d'Arf de Q.

2.6. Soit M un groupe abélien de type fini, de rang m. Soit F une forme bilinéaire symétrique sur M, à valeurs dans Z, de déterminant impair.

$V = M/2M$ est un espace vectoriel sur $\mathbb{F}_2$. Nous écrivons $\bar{x} = x+2M$. On définit un caractère quadratique non-défectif sur V par

$$\theta(\bar{x}) = e^{\frac{1}{2}\pi i F(x,x)} \quad .$$

Nous allons déterminer $\gamma(\theta\ ;\ V)$.

Choisissons $a \in M$ tel que

$$F(x,x) \equiv F(x,a) \pmod 2 .$$

Alors $F(a,a) \equiv \det F + m-1 \pmod 4$ (voir par exemple [5, p. 10]), en particulier on aura $F(a,a) \equiv m \pmod 2$.

Posons

$$G(x,y) = F(x,y) + F(x,a)\,F(y,a) ,$$

alors $G(x,x) \equiv 0 \pmod 2$. Définissons une forme quadratique Q sur V par

$$Q(\bar{x}) \equiv \frac{1}{2} G(x,x) \pmod 2 .$$

Si Q est défective, il existe $b \in M-2M$ avec

$$F(x,b) + F(a,b)\,F(x,a) \equiv 0 \pmod 2 ,$$

ce qui n'est possible que si $b \equiv a \mod 2M$, m impair.

On a :

$$\gamma(\theta\ ;\ V) = 2^{-\frac{1}{2}m} \sum_{x \in M/2M} e^{\frac{1}{2}\pi i\,(G(x,x)-F(x,a)^2)} .$$

Si $a \in 2M$, on a $\gamma(\theta\ ;\ V) = (-1)^{\Delta(Q)}$, d'après 2.5. Soit maintenant $a \notin 2M$ et m pair. Choisissons $b \in M$ tel que $G(a,b) \equiv 1 \pmod 2$. Soit V_1 le sous-espace de V engendré par $\bar{a}$ et $\bar{b}$ et V_2 son orthogonal. D'après 1.8. (i) :

$$\gamma(\theta\ ;\ V) = \gamma(\theta|V_1\ ;\ V_1)\ \gamma(\theta|V_2\ ;\ V_2) ,$$

et d'après 2.5. :

$$\gamma(\theta|V_2\ ;\ V_2) = (-1)^{\Delta(Q|V_2)} .$$

$\gamma(\theta|V_1\ ;\ V_1)$ se trouve facilement par un calcul direct. On trouve finalement :

$$\gamma(\theta\ ;\ V) = (-1)^{\Delta(Q)} \quad \text{si } F(a,a) \equiv 0 \pmod 4 ,$$

$$\gamma(\theta\ ;\ V) = -i\,(-1)^{\Delta(Q)} \quad \text{si } F(a,a) \equiv 2 \pmod 4 .$$

Si $a \notin 2M$ et m est impair, écrivons $V = \mathbb{F}_2\,\bar{a} + V_1$, où maintenant : $V_1 = \{\bar{x} | F(x,a) \equiv 0 \pmod 2\}$. On trouve :

$$\gamma(\theta\ ;\ V) = e^{\frac{1}{4}\pi i}\,(-1)^{\Delta(Q|V_1)} \quad \text{si } F(a,a) \equiv 1 \pmod 4$$

$$\gamma(\theta\ ;\ V) = e^{-\frac{1}{4}\pi i}\,(-1)^{\Delta(Q|V_1)} \quad \text{si } F(a,a) \equiv 3 \pmod 4$$

3. Invariants de formes quadratiques sur certains corps

3.1. Soit A un anneau de Dedekind avec la propriété que les quotients pour un idéal maximal soient des corps finis. Soit K le corps des quotients de A. Fixons un caractère complexe χ du groupe additif de K, tel que $\chi|A = 1$. On suppose que l'ensemble des $x \in K$ tels que $\chi(xA) = 1$ soit un idéal fractionnaire. C'est alors l'inverse $\underline{d}^{-1}$ d'un idéal $\underline{d} = \underline{d}_\chi$ de A (<u>la différente</u> de χ).

Soit V un espace vectoriel de dimension finie sur K et Q une forme quadratique sur V. On désigne par $(,)$ la forme bilinéaire associée, on la suppose non-dégénérée.

Soit L un A-réseau dans V tel que $Q(L) \subset A$. Posons :

$$L' = \{x \in V \mid (x,L) \subset A\} ,$$

c'est encore un réseau et $L \subset L' \subset \underline{d}^{-1}L'$. Le groupe $\underline{d}^{-1}L'/L$ est fini. Nous définissons un caractère θ_L sur ce groupe par

$$\theta_L(x+L) = \chi(Q(x)) .$$

Le bicaractère associé f_{θ_L} est donné par :

$$f_{\theta_L}(x+L,y+L) = \chi((x,y)) ,$$

d'où l'on voit que θ_L est non-défectif.

Le résultat suivant généralise quelque peu ce qui est établi dans [3, p. 128].

3.2. Proposition. *$\gamma(\theta_L ; \underline{d}^{-1}_{\chi}L'/L)$ est indépendant du choix de L.*

Il suffit de montrer que ce nombre ne change pas si L est remplacé par un sous-réseau L_1. Alors $L' \subset L'_1$ et $\underline{d}^{-1}L'/L_1$ est un sous-groupe de $\underline{d}^{-1}L'_1/L_1$. L'orthogonal de $\underline{d}^{-1}L'/L_1$ par rapport à $f_{\theta_{L_1}}$ est L/L_1, ce qui implique que $\underline{d}^{-1}L'/L_1$ est l'orthogonal d'un sous-groupe isotrope de $\underline{d}^{-1}L'_1/L_1$. Alors, 1.8. (ii), montre que :

$$\gamma(\theta_{L_1} ; \underline{d}^{-1}_{\chi}L'_1/L_1) = \gamma(\theta_{L_1}/\underline{d}^{-1}_{\chi}L'/L_1 ; \underline{d}^{-1}_{\chi}L'/L_1) .$$

On voit facilement que le second membre égale $\gamma(\theta_L ; \underline{d}^{-1}_{\chi}L'/L)$, d'où la proposition.

Posons $\gamma(Q) = \gamma_\chi(Q) = \gamma(\theta_L ; \underline{d}^{-1}_{\chi}L'/L)$, c'est légitime d'après 3.2.

3.3. Proposition. (i) *On a* $\gamma_\chi(Q_1 \oplus Q_2) = \gamma_\chi(Q_1)\,\gamma_\chi(Q_2)$, $\gamma_\chi(-Q) = \gamma_\chi(Q)^{-1}$;

(ii) *γ_χ définit un caractère du groupe de Witt des formes quadratiques de K.*

3.4. Soit $\operatorname{char} K \neq 2$ et soit $(e_i)_{1 \leqslant i \leqslant m}$ une base orthogonale de V. Posons $V_i = Ke_i$. D'après 3.3. (i), on a :

$$\gamma_\chi(Q) = \prod_{i=1}^{m} \gamma_\chi(Q|V_i) ,$$

ce qui réduit la détermination de $\gamma_\chi(Q)$ au cas $V = K$. On a alors $Q(x) = ax^2$ (ce que nous écrivons $Q = \langle a \rangle$).

Soit $V = K$, $Q = \langle a \rangle$ et posons $L = \underline{a}$, un idéal (fractionnaire) tel que $a\underline{a}^2 \subset A$. Alors $L' = (2a\underline{a})^{-1}$ et $\underline{d}^{-1}L'/L \sim (2a\underline{a}\underline{d})^{-1}/\underline{a}$. Si $\underline{i}$ est un idéal de A nous posons $N\underline{i} = |A/\underline{i}|$. Alors on a :

(1) $$\gamma_\chi(\langle a\rangle) = N(2a\underline{\underline{a}}^2\underline{\underline{d}})^{-\frac{1}{2}} \sum_{(2a\underline{\underline{a}}\underline{\underline{d}})^{-1}/\underline{\underline{a}}} \chi(ax^2)$$

(sommation sur un système de représentants des classes de $(2a\underline{\underline{a}}\underline{\underline{d}})^{-1}$ modulo $\underline{\underline{a}}$).

3.5. Considérons le cas où $A = \mathbb{Z}$ et où le caractère de $\mathbb{Q}/\mathbb{Z}$ est défini par

$$\chi_{\mathbb{Q}}(x) = e^{2\pi i x}$$

On a $\underline{\underline{d}} = \mathbb{Z}$. Posons $\gamma_{\mathbb{Q}} = \gamma_{\chi_{\mathbb{Q}}}$. Alors (1) donne :

$$\gamma_{\mathbb{Q}}(\langle a\rangle) = |2a|^{-\frac{1}{2}} \sum_{x=1}^{2|a|} e^{2\pi i x^2/4a} .$$

D'après les formules pour les sommes de Gauss [2, p. 153] on trouve :

$$\gamma_{\mathbb{Q}}(\langle a\rangle) = e^{1/4\,\pi i \operatorname{sgn} a}$$

ce qui implique

$$\gamma_{\mathbb{Q}}(Q) = e^{1/4\,\pi i \operatorname{sgn} Q} ,$$

où $\operatorname{sgn} Q$ est la signature réelle de la forme quadratique Q.

3.6. Soit maintenant A l'anneau des entiers d'un corps de nombres K, de degré fini sur $\mathbb{Q}$. Le caractère de K/A est défini par

$$\chi_K(x) = \chi_{\mathbb{Q}}(\mathrm{Tr}_{K/\mathbb{Q}}\, x) .$$

La différente est alors la différente $\underline{\underline{d}}_{K/\mathbb{Q}}$ du corps K. Posons $\gamma_K = \gamma_{\chi_K}$.

Si $a \in K$ et si v est une place réelle de K, on dénote par $\operatorname{sgn}_v a$ le signe de a dans la complétion de K définie par v. Si Q est une forme quadratique sur K, $\operatorname{sgn}_v Q$ a une signification analogue.

On voit immédiatement que :

$$\gamma_K(\langle a\rangle) = \gamma_{\mathbb{Q}}(Q_1) ,$$

où Q_1 est la forme quadratique sur le $\mathbb{Q}$-espace vectoriel K définie par :

$$Q_1(x) = \mathrm{Tr}_{K/\mathbb{Q}}(ax^2) .$$

Il résulte alors de (2) que

(3) $$\gamma_K(\langle a\rangle) = e^{\frac{1}{4}\pi i \sum_v \operatorname{sgn}_v a}$$

par conséquent :

$$\gamma_K(Q) = e^{\frac{1}{4}\pi i \sum_v \operatorname{sgn}_v Q} .$$

Soit alors a un nombre totalement positif de K et u une unité de A. Il résulte de (1) et (3) que ($\underline{\underline{a}}$ étant comme dans 3.4.) :

$$\sum_{(2a\underline{\underline{a}}\underline{\underline{d}})^{-1}/\underline{\underline{a}}} \chi_K(uax^2) = i^{-M(u)} \sum_{(2a\underline{\underline{a}}\underline{\underline{d}})^{-1}/\underline{\underline{a}}} \chi_K(ax^2) ,$$

où $M(u)$ est le nombre des places réelles v avec $\operatorname{sgn}_v u = -1$. Ceci est lié à un résultat d'Armitage [1].

3.7. Soit encore K un corps de nombres et A son anneau des entiers. Si $\underline{p}$ est un idéal premier de A, on dénote par $K_{\underline{p}}$ la complétion correspondante de K et par $A_{\underline{p}}$ l'anneau des entiers de $K_{\underline{p}}$. Il existe une bijection :

$$K/A \xrightarrow{\sim} \bigoplus_{\underline{p}} K_{\underline{p}}/A_{\underline{p}} \tag{4}$$

($\underline{p}$ parcourant l'ensemble des idéaux premiers de A). Si χ est un caractère (quelconque) comme dans 3.1., l'isomorphisme (4) lui associe un caractère $\chi_{\underline{p}}$ de $K_{\underline{p}}$, qui a les propriétés de 3.1. (pour $K_{\underline{p}}$ et $A_{\underline{p}}$).

Soit Q une forme quadratique non-dégénérée sur le K-espace vectoriel V. On dénote pour $Q_{\underline{p}}$ la forme induite sur $V_{\underline{p}} = K_{\underline{p}} \otimes_K V$.

3.8. Théorème. $\gamma_\chi(Q) = \prod_p \gamma_{\chi_{\underline{p}}}(Q_{\underline{p}})$.

Soit L comme dans 3.1. et posons $L_{\underline{p}} = A_{\underline{p}} \otimes_A L$, c'est un $A_{\underline{p}}$-réseau dans $V_{\underline{p}}$. Si $\underline{d}_{\underline{p}}$ est la différente de $\chi_{\underline{p}}$, le groupe fini $\underline{d}^{-1}L'/L$ est la somme directe orthogonale de sous-groupes isomorphes aux $\underline{d}_{\underline{p}}^{-1}L'/L$ et l'assertion résulte de 1.8. (i).

Si en outre $\chi = \chi_K$ nous posons $\gamma_{K_{\underline{p}}} = \gamma_{(\chi_K)_{\underline{p}}}$. La formule de 3.8. devient alors :

$$\gamma_K(Q) = \prod_{\underline{p}} \gamma_{K_{\underline{p}}}(Q_{\underline{p}}) \quad .$$

C'est la loi de réciprocité de Weil (voir [6 , p. 133]). Le premier membre a été déterminé ci-dessus. Les facteurs du second membre s'obtiennent, en principe, par des calculs locaux. Nous n'y insistons pas.

3.9. Soit encore K un corps de nombres. (1) et (3) donnent alors le calcul de certaines sommes de Gauss. Nous allons en déduire quelques autres formules. Nous prenons $\chi = \chi_K$ dans (1).

Soit $a \in A$ premier à 2, et choisissons $c \in K$ totalement positif tel que $c\,\underline{d}$ soit un idéal entier, premier à $2aA$ (où $\underline{d} = \underline{d}_{K/\mathbb{Q}}$). En appliquant (1) avec $a^{-1}c$ au lieu de a et $\underline{a} = aA$, il résulte de (3) que :

$$N(2ac\underline{d})^{-\frac{1}{2}} \sum_{(2c\underline{d})^{-1}/aA} \chi_K(a^{-1}cx^2) = e^{\frac{1}{4}\pi i \sum_v \operatorname{sgn}_v a} \quad .$$

Posons :

$$\sigma_c(a) = N(a\underline{cd})^{-\frac{1}{2}} \sum_{(\underline{cd})^{-1}/aA} \chi_K(a^{-1}cx^2) \quad ,$$

$$\sigma_c'(a) = N(aA)^{-\frac{1}{2}} \sum_{A/aA} \chi_K(a^{-1}cx^2) \quad ,$$

$$\tau_c(a) = N(2A)^{-\frac{1}{2}} \sum_{A/2A} \chi_K(\tfrac{1}{4}acx^2) \quad .$$

Il résulte de 1.8. (i), appliqué au caractère quadratique sur le groupe $(2\underline{cd})^{-1}/aA$ défini par $x \mapsto \chi_K(a^{-1}cx^2)$ et au sous-groupe $(\underline{cd})^{-1}/aA$ que :

$$\sigma_c(a)\,\tau_c(a) = e^{\frac{1}{4}\pi i \sum_v \operatorname{sgn}_v a} \quad . \tag{5}$$

Soient maintenant $a,b \in A$ tels que $a,b,2$ soient premiers entre eux et prenons c totalement positif tel que $\underline{cd}$ soit un idéal entier premier à $2ab$. Soit $(\frac{a}{b})$ le symbole de Jacobi.

En appliquant maintenant 1.8. (i), au caractère quadratique sur $(\underline{cd})^{-1}/ab\,A$ défini par $x \mapsto \chi_K(a^{-1}b^{-1}cx^2)$ et au sous-groupe $b(\underline{cd})^{-1}/abA$ on trouve :

$$\sigma_c(ab) = (\tfrac{a}{b})(\tfrac{b}{a})\,\sigma_c(a)\,\sigma_c'(b) \quad .$$

Il en résulte que :

$$\sigma_c'(b) = \sigma_c(b)\,\sigma_c(1)^{-1} \quad ,$$

d'où

$$(\tfrac{a}{b})(\tfrac{b}{a}) = \sigma_c(ab)\,\sigma_c(a)^{-1}\,\sigma_c(b)^{-1}\,\sigma_c(1) \quad ,$$

et (5) donne :

$$(\tfrac{a}{b})(\tfrac{b}{a}) = (-1)^{\sum_v \frac{\operatorname{sgn}_v a-1}{2}\cdot\frac{\operatorname{sgn}_v b-1}{2}}\,\tau_c(ab)^{-1}\tau_c(a)\tau_c(b)\tau_c(1)^{-1} \quad . \tag{6}$$

Or $\tau_c(a)$ est un nombre $\gamma(\theta\,;V)$ comme dans 2.6. (6) est la loi de réciprocité quadratique dans K.

Si $a \equiv b \equiv 1 \pmod{2A}$, le second membre se calcule plus explicitement, d'après Siegel [4].

Si $y \in A$, il existe $u(y) \in A$ tel que

$$\operatorname{Tr}_{K/\mathbb{Q}}(cx^2y) \equiv \operatorname{Tr}_{K/\mathbb{Q}}(cxu(y)) \pmod{2},$$

pour tout $x \in A$, et on a :

$$\operatorname{Tr}_{K/\mathbb{Q}}(cu(x)u(y)) \equiv \operatorname{Tr}_{K/\mathbb{Q}}(xy) \pmod{2}$$

(ceci résulte de [loc. cit., p. 347]).

Soit $a \equiv b \equiv 1 \pmod{2}$, et posons $a = 1+2a'$, $b = 1+2b'$. Un calcul facile montre que :

$$\tau_c(a) = e^{-\frac{1}{4}\pi i \operatorname{Tr}_{K/\mathbb{Q}}(cu(a')^2)}\,\tau_c(1) \quad ,$$

d'où :

$$\tau_c(ab)\,\tau_c(a)^{-1}\,\tau_c(b)^{-1}\,\tau_c(1) = e^{-\pi i\,\mathrm{Tr}_{K/\mathbb{Q}}(cu(a')u(b'))} = (-1)^{\mathrm{Tr}_{K/\mathbb{Q}}(a'b')}.$$

Ceci donne la formule de Hasse

$$(\tfrac{a}{b})(\tfrac{b}{a}) = (-1)^{\sum_v \frac{\mathrm{sgn}_v a-1}{2}\,\frac{\mathrm{sgn}_v b-1}{2} + \mathrm{Tr}_{K/\mathbb{Q}}(\frac{a-1}{2}\,\frac{b-1}{2})}.$$

REFERENCES

[1] J.V. ARMITAGE, On a Theorem of Hecke in Number Fields and Function Fields, Inv. Math. 2 (1967), 238-246.

[2] E. LANDAU, Vorlesunger über Zahlentheorie, Bd. 1, Leipzig, 1927.

[3] J. MILNOR and D. HUSEMOLLER, Symmetric bilinear forms, Erg. Math. Bd. 73, Springer-Verlag, 1973.

[4] C.L. SIEGEL, Uber das quadratische Reziprozitätsgesetz in algebraischen Zahlkörpern, dans : Gesammelte Abhandlungen, Springer-Verlag, 1966, Bd. 3, 334-349.

[5] T.A. SPRINGER, Note on quadratic forms in characteristic 2, Nieuw Archief v. Wiskunde (3) X (1962), 1-10.

[6] A. WEIL, Sur certains groupes d'opérateurs unitaires, Acta Math. 111 (1964), 143-211.

Mathematisch Instituut
Der Risjksuniversiteit te Utrecht

UTRECHT

PAYS-BAS