JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

EVA BAYER-FLUCKIGER

Réseaux unimodulaires

Journal de Théorie des Nombres de Bordeaux 2^e série, tome 1, n° 1 (1989), p. 189-196

<http://www.numdam.org/item?id=JTNB_1989__1_1_189_0>

Séminaire de Théorie des Nombres,
Bordeaux, **1**,*189–196(1989)*

Réseaux unimodulaires.

par EVA BAYER-FLUCKIGER

Résumé — Soit f un produit de polynômes cyclotomiques. Existe-t-il une forme bilinéaire symétrique entière, unimodulaire et définie positive ayant une isométrie de polynôme caractéristique f ? Ce travail donne une réponse partielle à cette question.

Abstract — *Let f be a product of cyclotomic polynomials. Does there exist an integral, unimodular and positive definite symmetric bilinear form that has an isometry with characteristic polynomial f ? The present paper gives a partial answer to this question.*

1 - Isométries parfaites

Le point de départ de ce travail est une question de Claude Weber, motivée par la théorie des noeuds [4], [5] :

Soit L un $\mathbf{Z}$-module libre de rang n, et soit $S : L \times L \to \mathbf{Z}$ une forme bilinéaire ϵ-symétrique ($\epsilon = 1$ ou -1) unimodulaire et paire (c'est-à-dire $S(x,x) \equiv 0 \ (mod 2)$ pour tout $x \in L$).

Question 1 :

Existe-t-il une forme bilinéaire unimodulaire $A : L \times L \to \mathbf{Z}$ telle que $S(x,y) = A(x,y) + \epsilon A(y,x)$ pour tout $x, y \in L$?

Michel Kervaire a étudié cette question [5]. Lorsque $\epsilon = -1$, la réponse est affirmative. Si $\epsilon = 1$ et S est indéfinie, Kervaire a montré que la réponse est encore positive sauf si $n = 2$. Il a utilisé pour cela la classification des formes bilinéaires symétriques entières, unimodulaires et indéfinies [6], [9]. Pour aborder le cas où S est symétrique et défini, il a introduit la notion d'isométrie parfaite :

DÉFINITION. *Un isomorphisme de $\mathbf{Z}$-modules $t : L \to L$ est une isométrie de S si $S(tx,ty) = S(x,y)$ pour tout $x, y \in L$. Une isométrie $t : L \to L$ de S est appelée isométrie parfaite si $(1-t) : L \to L$ est un isomorphisme.*

Manuscrit reçu le 16 mai 1989.

LEMME 1. *[5] Il existe une forme bilinéaire unimodulaire $A : L \times L \to \mathbb{Z}$ telle que $S(x,y) = A(x,y) + \epsilon A(y,x)$ pour tout $x, y \in L$ si et seulement si S a une isométrie parfaite.*

DÉMONSTRATION:

Etant donné A, on définit $t : L \to L$ par

$$A(tx, y) = -\epsilon A(y, x).$$

On vérifie que t est bien une isométrie de S, et que $S(x,y) = A((1-t)x, y)$. Comme A est unimodulaire, $1 - t$ est un isomorphisme. Réciproquement, si t est une isométrie parfaite de S, posons $A(x,y) = S((1-t)^{-1}x, y)$. On vérifie que $S(x,y) = A(x,y) + \epsilon A(y,x)$. Une démonstration détaillée se trouve dans [5], page 178.

Remarque

Le lemme et sa démonstration sont inspirés par la théorie des noeuds [5].

On peut donc reformuler la question 1 comme suit :

Question 2 :

Est-ce que S admet une isométrie parfaite ?

Supposons désormais *S symétrique et définie positive.* Comme S est paire, il est bien connu que le rang de S est divisible par 8 (voir par exemple [9], chapitre V, Corollaire 2). Rappelons qu'il existe une unique classe d'isomorphisme de formes bilinéaires symétriques unimodulaires de rang 8, notée Γ_8. Il y en a deux de rang 16, une indécomposable notée Γ_{16} et la somme orthogonale de deux copies de Γ_8. Pour $n = 24$, Niemeier a démontré qu'il existe exactement 24 classes d'isomorphisme de telles formes [7]. L'une de ces formes, appelée forme de Leech, a une propriété particulière :

DÉFINITION. *Le minimum de S est le plus petit entier non nul m tel qu'il existe $x \in L$ avec $S(x,x) = m$.*

La forme de Leech est de minimum 4, alors que les formes de Niemeier sont de minimum 2.

DÉFINITION. *On appelle réseau une forme bilinéaire symétrique entière et définie positive.*

Kervaire [5] a donné une réponse complète à la Question 2 pour les réseaux de rang au plus 24. Le réseau Γ_8 a une isométrie parfaite, Γ_{16} n'en a pas. Parmi les réseaux unimodulaires de rang 24, 10 ont une isométrie parfaite (dont le réseau de Leech), 14 n'en ont pas. Kervaire a aussi obtenu des résultats concernant des réseaux de rang arbitrairement grand et de minimum 2 (voir [5]).

On dit qu'un réseau est *indécomposable* s'il n'est pas isomorphe à une somme orthogonale de réseaux non triviaux. Le résultat suivant est une conséquence du Théorème 1 et de la Proposition 2 (voir 2) :

PROPOSITION 1. *Il existe une infinité de classes d'isomorphisme de réseaux unimodulaires, indécomposables et de minimum au moins* 4 *qui ont une isométrie parfaite.*

Soit (L, S) un réseau et soit $t : L \to L$ une isométrie de S. Soit f le polynôme caractéristique de t. Alors t est parfaite si et seulement si $f(1) = \pm 1$. Au lieu de chercher des réseaux ayant une isométrie parfaite, on peut se poser une question plus précise et s'intéresser aux réseaux ayant une isométrie de polynôme caractéristique donné. Ceci fera l'objet du paragraphe suivant.

2. Réseaux unimodulaires ayant une isométrie de polynôme caractéristique donné

Soit f un polynôme unitaire à coefficients entiers. Un *f-réseau* est un réseau ayant une isométrie de polynôme caractéristique f. Le groupe des isométries d'un réseau est fini. Donc s'il existe un f-réseau, alors f est un produit de polynômes cyclotomiques. Notons ϕ_m le polynôme cyclotomique correspondant aux racines $m^{\text{ièmes}}$ de l'unité.

THÉORÈME 1 [2]. :

Soit $f = \phi_m^n$. Alors

1) Si m est une puissance de 2, alors il existe un f-réseau unimodulaire.

2) Si m n'est pas une puissance de 2, alors il existe un f- réseau unimodulaire si et seulement si le degré de f est divisible par 8, et $f(1)f(-1)$ est un carré.

PROPOSITION 2 [2].

Soit $f = \phi_m$, avec m sans facteur carré. Alors tout f-réseau est indécomposable. Si m n'est pas un nombre premier et si $deg(f) > 8$, alors tout f-réseau est de minimum au moins 4.

DÉMONSTRATION DE LA PROPOSITION 1:

Soit $m = pqr$, avec p, q et r des nombres premiers impairs distincts. Posons $f = \phi_m$. Alors $deg(f) = (p-1)(q-1)(r-1)$, donc $deg(f)$ est divisible par 8. On a $f(1) = f(-1) = 1$. Les conditions du théorème 1 sont remplies, il existe donc un f-réseau unimodulaire (L, S). Soit $t : L \to L$ une isométrie de S de polynôme caractéristique f. On a $f(1) = 1$, donc t est parfaite. La proposition 2 entraîne que (L, S) est indécomposable et de minimum au moins 4.

On dit que deux polynômes $f, g \in \mathbb{Z}[X]$ sont *premiers entre eux* s'il existe $h, k \in \mathbb{Z}[X]$ avec $fh + gk = 1$.

LEMME 2 ([2], REMARK (1.3)).

La somme orthogonale d'un f-réseau et d'un g-réseau est un (fg)-réseau. Réciproquement, si f et g sont premiers entre eux alors tout (fg)-réseau se décompose en la somme orthogonale d'un f-réseau et d'un g-réseau.

Il est bien connu que ϕ_n et ϕ_m ne sont pas premiers entre eux si et seulement si $n = p^r m$, où p est un nombre premier et r un nombre entier. Par exemple, ϕ_{p^n} et ϕ_{p^m} ne sont pas premiers entre eux si p est un nombre premier. Le théorème 1 montre que si p est un nombre premier impair, alors il n'existe pas de ϕ_{p^n}- réseau unimodulaire.

PROPOSITION 3. *Soit p un nombre premier impair, et posons $f = \phi_{p^n}\phi_{p^m}$ où n et m sont des nombres entiers positifs. Les propriétés suivantes sont équivalentes :*

(a) Il existe un f-réseau unimodulaire

(b) $deg(f)$ est divisible par 8

(c) $p \equiv 1 \pmod 4$ ou $n + m \equiv 1 \pmod 2$.

DÉMONSTRATION: L'équivalence de (b) et de (c) résulte de propriétés élémentaires des polynômes cyclotomiques. Si (L, S) est un f-réseau unimodulaire, alors S est pair (cf. [2], démonstration du lemme (1.4)). Donc le

rang de L est divisible par 8. Mais $rang(L) = deg(f)$. Donc (a) entraîne (b). Il reste à montrer que (c) entraîne (a). La démonstration de ce fait sera donnée dans le 5, après quelques préliminaires sur les formes de torsion.

3 - Formes de torsion

Soit C un groupe (dans la suite, nous prendrons pour C le groupe trivial ou le groupe cyclique infini C_∞). Une forme $\mathbf{Z}$- bilinéaire symétrique $S : G \times G \to \mathbf{Q}/\mathbf{Z}$ sur un groupe abélien fini G est *non dégénérée* si l'homomorphisme $\hat{S} : G \to Hom_Z(G, \mathbf{Q}/\mathbf{Z})$, défini par $\hat{S}(x)(y) = S(x,y)$, est un isomorphisme. Si on a de plus $S(tx,ty) = S(x,y)$ pour tout $x, y \in G$ et $t \in C$, alors (G,S) est appelée une *C-forme de torsion*. La *somme orthogonale* de deux formes de torsion (G,S) et (G',S') est par définition $(G \oplus G', S \oplus S')$, où $(S \oplus S')(x+x', y+y') = S'(x',y')$. Si $t \in C$, on pose $t(x,x') = (tx, tx')$.

Soit (G,S) une forme de torsion. Pour tout sous-groupe H de G, posons $H^\perp = \{x \in G \mid S(x,y) = 0 \text{ pour tout } y \in H\}$. On dit que (G,S) est *neutre* s'il existe un sous-groupe U de G tel que $U^\perp = U$, et $t(U) = U$ pour tout $t \in C$. Deux formes de torsion (G,S) et (G',S') sont *isomorphes* s'il existe un isomorphisme de Z-modules $f : G \to G'$ tel que $t \circ f = f \circ t$ pour tout $t \in C$, et $S'(fx, fy) = S(x,y)$ pour tout $x, y \in G$.

Soit $G(\mathbf{Q}/\mathbf{Z}, C)$ le groupe de Grothendieck des classes d'isomorphisme des C-formes de torsion par rapport à la somme orthogonale. Soit $W(\mathbf{Q}/\mathbf{Z}, C)$ le quotient de $G(\mathbf{Q}/\mathbf{Z}, C)$ par le sous-groupe engendré par les formes neutres. Ce groupe est appelé *groupe de Witt* des C-formes de torsion. Si C est le groupe trivial, on pose $W(\mathbf{Q}/\mathbf{Z}, C) = W(\mathbf{Q}/\mathbf{Z})$. On dit que deux formes de torsion sont *équivalentes* si elles sont dans la même classe de $W(\mathbf{Q}/\mathbf{Z}, C)$. Il est facile de vérifier que (G,S) et (G',S') sont équivalents si et seulement s'il existe des formes neutres (N,T) et (N',T') telles que $(G,S) \oplus (N,T) \tilde{=} (G',S') \oplus (N',T')$.

Le lemme suivant est bien connu :

LEMME 3 [8], (5.1.3). *Soit (G,S) une forme de torsion, et soit H un sous-groupe de G tel que $H \subset H^\perp$ et $t(H) = H$ pour tout $t \in C$. Alors (G,S) et $(H^\perp/H, S)$ sont équivalentes.*

4. Construction de f-réseaux unimodulaires

Soit (M,S) un f-réseau, et soit $t : M \to M$ une isométrie de S de polynôme caractéristique f. Soit $V = M \otimes_{\mathbf{Z}} \mathbf{Q}$. On obtient $S : V \times V \to \mathbf{Q}$ et $t : V \to V$ par extension des scalaires. Posons $M' = \{x \in V \mid S(x,y) \in \mathbf{Z}$

pour tout $y \in M\}$. On a $t(M') = M'$. Soit $G = M'/M$. On obtient une forme symétrique $S : G \times G \to \mathbf{Q}/\mathbf{Z}$ et une isométrie $t : G \to G$ de cette forme. Alors (G, S) est une $C = C_\infty$-forme de torsion. Supposons que (G, S) soit neutre. Il existe alors un sous-groupe U de G tel que $U^\perp = U$ et $t(U) = U$. Notons $p : M' \to G = M'/M$ la projection. Soit $L = p^{-1}(U)$. Alors $L' = L$ et $t(L) = L$. Donc L est un f-réseau unimodulaire.

5. Démonstration de la Proposition 3

Soit $(e_1, \cdots, e_p)$ la base standard de $\mathbf{R}^p$. On munit $\mathbf{R}^p$ du produit scalaire canonique $e_i.e_j$. Soit

$$A = \mathbf{Z}A_{p-1} = \{\sum a_i e_i \mid a_i \in \mathbf{Z} \ \sum a_i = 0\}$$

le réseau de rang $p-1$ engendré par le système de racines A_{p-1} (voir par exemple [7], 4). On a $A'/A \tilde{=} \mathbf{Z}/p\mathbf{Z}$. Notons rA la somme orthogonale de r copies de A. Posons $M_n = p^{n-1}A$. La base canonique du $\mathbf{R}^p$ contenant la $j^{\text{ème}}$ copie de A sera notée $(e_1^j, \cdots e_p^j)$. Soit $t_n : M_n \to M_n$ l'isométrie de M_n définie par

$$t_n(e_i^j) = e_i^{j+1} \text{ si } j \neq p^{n-1}, \ t_n(e_i^{p^{n-1}}) = e_{i+1}^1$$

où i est un indice modulo p. Alors le polynôme caractéristique de t_n est ϕ_{p^n}. Soit M la somme orthogonale de M_n et de M_m, muni de l'isométrie $t = t_n \oplus t_m$. Alors M est un $\phi_{p^n}\phi_{p^m}$-réseau.

Posons $G_n = M_n'/M_n$. La C_∞-forme de torsion (G_n, S_n) associée à M_n est la somme orthogonale de p^{n-1} copies de

$$T : \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$$

$$T(x, y) = -\frac{1}{p}xy$$

(voir [7], §4), munie de l'isométrie $t_n : G_n \to G_n$.

Dans $W(\mathbf{Q}/\mathbf{Z})$, la somme orthogonale de 4 copies de T est toujours nulle, et celle de 2 copies de T l'est si et seulement si $p \equiv 1 \ (mod\ 4)$. Donc dans $W(\mathbf{Q}/\mathbf{Z})$, la classe de la forme de torsion (G_n, S_n) est égale à celle de

$$T_n = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$$

$$T_n(x, y) = -\frac{\epsilon}{p}xy$$

où $\epsilon \equiv p^{n-1}$ $(mod\ 4)$.

Remarquons que la C_∞- forme de torsion (G_n, S_n) s'identifie à l'anneau de groupe $\mathbf{F}_p C_{p^n-1}$ (où $\mathbf{F}_p$ est le corps fini à p éléments et C_r est le groupe cyclique d'ordre r) muni de l'opposée de la forme standard. Soit $I = (t_n - 1)(G_n)$, l'idéal d'augmentation de cet anneau de groupe. Posons $k = \frac{n-1}{2}$, et $U = I^k$. Alors $U \subset U^\perp = I^{k-1}$. Par le lemme 3, les C_∞-formes de torsion (G_n, S_n) et $(U^\perp/U, S_n)$ sont équivalentes. On a $U^\perp/U \tilde{=} \mathbf{Z}/p\mathbf{Z}$ et l'isométrie induite par t_n est l'identité. Donc (G_n, S_n) est équivalente à T_n en tant que C_∞-formes de torsion.

Soit $(G, S) = (G_n, S_n) \oplus (G_m, S_m)$ la C_∞-forme de torsion associée à M. Cette forme est donc équivalente à $T_n \oplus T_m$. Si $p \equiv 1(mod 4), T_n \oplus T_m$ est neutre. Si $p \equiv 3$ $(mod\ 4)$, alors $T_n \oplus T_m$ est neutre si et seulement si $n + m$ est impair. Donc l'hypothèse (c) entraîne que (G, S) est neutre. La construction du 4 nous fournit donc un $\phi_{p^n}\phi_{p^m}$-réseau unimodulaire.

Remarque

Au cours d'une étude de la forme trace d'une extension cyclique d'ordre p^2 dans laquelle p est totalement ramifié [1], Christine Bachoc et Boas Erez obtiennent des $\phi_p\phi_{p^2}$-réseaux unimodulaires. Le système des racines de leurs réseaux est pA_{p-1}, tout comme celui des $\phi_p\phi_{p^2}$-réseaux construits dans la démonstration ci-dessus.

Bibliographie

[1] C. BACHOC et B. EREZ *Forme trace et ramification.* (à paraître).

[2] E. BAYER-FLUCKIGER *Definite unimodular lattices having an automorphism of given characteristic polynomial*, Comment. Math. Helv. **59** (1984), 509–538.

[3] E. BAYER-FLUCKIGER *Unimodular lattices.* (en préparation).

[4] J-C. HAUSMAN (éditeur) *Problems in knot theory.*, Proceedings of a conference on knot theory, Plans-sur-Bex 1977 Lecture Notes Math **685**. Springer Verlag, 1978, 309–311.

[5] M. KERVAIRE *Formes de Seifert et fromes quadratiques entières*, L'enseignement Math. **31** (1985), 173–186.

[6] J. MILNOR, D. HUSEMOLLER *Symetric bilinear forms*, Ergebnisse Math. **73**. Springer Verlag (1973).

[7] H-V. NIEMEIER *Definite quadratische Formen der Diskriminante 1 und Dimension 24*, J. Number Theory **5** (1973), 142–178.

[8] W. SCHARLAU *Quadratic and hermitian forms*, Grundlehren Math. Wiss. **270**. Springer Verlag (1985).

[9] J-P. SERRE *Cours d'arithmétique*, Presses Universitaires de France (1970).

Mots clefs: Formes quadratiques entières.

U.A. 741 du C.N.R.S.
Laboratoire de Mathématiques
Faculté des Sciences de Besançon
25030 Besançon Cedex, FRANCE.