Journal de Théorie des Nombres
de Bordeaux **12** (2000), 273–280

Cyclotomic modular lattices

par Eva BAYER-FLUCKIGER

Dedicated to Jacques Martinet

Résumé. Beaucoup de réseaux intéressants peuvent être obtenus en tant que *réseaux idéaux* sur des corps cyclotomiques : certains résaux de racines, le réseau de Coxeter–Todd, le réseau de Leech, etc. La plupart de ces réseaux sont *modulaires* au sens de Quebbemann. Le but de cet article est de déterminer les corps cyclotomiques sur lesquels il existe un réseau idéal modulaire. On étudie aussi une famille de réseaux particulièrement simple, les réseaux idéaux de *type trace*. L'article donne une liste complète des réseaux idéaux modulaires de type trace réalisés sur des corps cyclotomiques.

Abstract. Several interesting lattices can be realised as *ideal lattices* over cyclotomic fields : some of the root lattices, the Coxeter-Todd lattice, the Leech lattice, etc. Many of these are *modular* in the sense of Quebbemann. The aim of the present paper is to determine the cyclotomic fields over which there exists a modular ideal lattice. We then study an especially simple class of lattices, the ideal lattices of *trace type*. The paper gives a complete list of modular ideal lattices of trace type defined on cyclotomic fields.

Introduction

Let $K = \mathbf{Q}(\zeta_m)$ be the cyclotomic field of the m–th roots of unity. Many interesting lattices can be constructed as ideal lattices over K. For instance, the root lattice E_8 for $m = 15, 20$ and 24, the Coxeter–Todd lattice K_{12} for $m = 21$, the Leech lattice Λ_{24} for $m = 35, 39, 52, 56$ and 84,...(see for instance [5], [7], [10], [8], [9], [3], [1], [2]). In other words, these lattices can be written under the form $b : I \times I \to \mathbf{Z}$, $b(x, y) = \mathrm{Tr}(\alpha x\overline{y})$, for some ideal I of K and some totally positive $\alpha \in K^*$, $\overline{\alpha} = \alpha$, where $x \mapsto \overline{x}$ denotes complex conjugation. If $\alpha = 1$, then the lattice is said to be of *trace type*. Several of these lattices are *unimodular*, or more generally *modular* in the sense of Quebbemann (see §1). The aim of the present note is to show that

Manuscrit reçu le 15 octobre 2000.

if m is not a power of a prime which is congruent to 1 modulo 4, then there exists a modular ideal lattice over K. This is done in §2 and §3. One can also characterize the cyclotomic fields K over which there exists a modular ideal lattice of trace type, and even give a complete list of these lattices, cf. §4–6.

I would like to thank the Mathematical Sciences Research Institute, Berkeley, for its hospitality and support during the preparation of this paper.

1. Definitions and notation

Let m be a positive integer, let ζ_m be a primitive m–th root of unity, and let $K = \mathbf{Q}(\zeta_m)$ be the corresponding cyclotomic field. We may suppose without loss of generality that m is odd or divisible by 4. Let us denote by $x \mapsto \overline{x}$ the complex conjugation of K. Let $F = \mathbf{Q}(\zeta_m + \zeta_m^{-1})$ be the fixed field of the complex conjugation (in other words, the maximal real subfield of K). Let $O = \mathbf{Z}[\zeta_m]$ be the ring of integers of K. Let $\mathcal{D}_K$ be the different of K. Set $n = [K : \mathbf{Q}] = \varphi(m)$.

Recall that an *integral lattice* is a pair (L, b), where L is a free $\mathbf{Z}$–module of finite rank, and $b : L \times L \to \mathbf{Z}$ is a positive definite symmetric bilinear form. Such a lattice is said to be *even* if $b(x,x) \equiv 0 \pmod 2$ for all $x \in L$. In this paper, all lattices will be supposed integral. We often write L instead of (L, b). The *dual* of the lattice (L, b), denoted by (L^*, b), is by definition $L^* = \{x \in L \otimes_{\mathbf{Z}} \mathbf{Q} \mid b(x, L) \subset \mathbf{Z}\}$.

The following is a special case of the notion of *ideal lattice*, cf. [6].

Definition 1. An *ideal lattice* is a pair (I, b), where I is a (fractional) O–ideal, and $b : I \times I \to \mathbf{Z}$ a lattice such that $b(\lambda x, y) = b(x, \overline{\lambda} y)$ for all $x, y \in I$ and for all $\lambda \in O$.

It is easy to see that this is equivalent to asking that there exists a totally positive $\alpha \in F$ such that $b(x, y) = \mathrm{Tr}(\alpha x \overline{y})$, where $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbf{Q}}$ is the trace. Such a lattice is said to be of *trace type* if $\alpha = 1$. In other words :

Definition 2. An *ideal lattice of trace type* is a pair (I, b), where I is a (fractional) O–ideal, and $b : I \times I \to \mathbf{Z}$ is given by $b(x, y) = \mathrm{Tr}(x\overline{y})$.

Note that the lattices constructed by Craig [8], [9] are of trace type.

Let ℓ be a positive integer. A lattice (L, b) is said to be *ℓ–modular* if there exists a similarity $\sigma : L \otimes_{\mathbf{Z}} \mathbf{Q} \to L \otimes_{\mathbf{Z}} \mathbf{Q}$ with multiplier ℓ such that $\sigma(L^*) = L$. We say that (L, b) is *modular* if it is ℓ–modular for some ℓ. These notions were introduced by Quebbemann, cf. [11]. It is easy to see that if (L,b) is ℓ–modular, then $\det(b) = \ell^{n/2}$, where $n = \mathrm{rank}(L)$. In particular, n is even unless ℓ is the square of an integer. If $n = 2k$ and if (L,b) is even, then it is shown in [11] that the theta series of (L,b) is a modular form of weight k over $\Gamma_0(\ell)$ and an eigenform of the Fricke operator. Any *unimodular* lattice (that is, a lattice (L,b) with $\det(b) = 1$) is modular with $\ell = 1$. Note that if $\ell = 1$, then $\Gamma_0(\ell) = \mathrm{PSL}_2(\mathbf{Z})$, so we recover the well–known fact that the theta series of an even, unimodular lattice is modular over $\mathrm{PSL}_2(\mathbf{Z})$, cf. for instance [12].

2. Some constructions of modular lattices

The aim of this section is to give some constructions of modular ideal lattices over certain cyclotomic fields $\mathbf{Q}(\zeta_m)$. This will then be used to show a more general result in §3. Note that the constructions given here are special cases of those of §5.

2.1. The prime power case. Here, we take $m = p^r$ where p is a prime and r a positive integer. Suppose that either $p = 2$ and $r \geq 3$, or $p \equiv 3 \pmod 4$ and $r \geq 1$. Let us denote by P the unique prime ideal of O above p. Let $\mathcal{D}_K$ be the different of K. Then $\mathcal{D}_K = P^a$, with $a = p^{r-1}(pr - r - 1)$. We have $n = [K : \mathbf{Q}] = p^{r-1}(p-1)$.

We construct a p–modular ideal lattice as follows. Set $s = \frac{p^{r-1}(p-1)-2a}{4}$. Let $I = P^s$, and let $b : I \times I \to \mathbf{Z}$ be given by $b(x,y) = \mathrm{Tr}(x\overline{y})$.

Notation. We denote the ideal lattice constructed above by $\mathcal{L}^p_{p^r}$.

Proposition 1. *Let p be a prime number and let r be a positive integer. Suppose that either $p = 2$ and $r \geq 3$, or $p \equiv 3 \pmod 4$ and $r \geq 1$. The lattice $\mathcal{L}^p_{p^r}$ is an even, p–modular ideal lattice of trace type over $K = \mathbf{Q}(\zeta_{p^r})$. It has rank $p^{r-1}(p-1)$ and determinant $p^{\frac{p^{r-1}(p-1)}{2}}$.*

Proof. Let $\mathcal{L}^p_{p^r}$ be given by (I,b) as above. Note that $I^* = I^{-1}\mathcal{D}^{-1}$. Let $\sigma : K \to K$ be defined by multiplication with $\sqrt{-p}$. Then $\sigma(I^*) = I$, and σ is a similarity of b with multiplier p. It remains to check that b is even. If p is odd, then this is a consequence of [5, Proposition 2.12]. If $p = 2$, then a straightforward computation shows that b is even. Hence (I,b) is an even p–modular ideal lattice.

Remark 1. If $p \equiv 3 \pmod 4$, then the ideal lattice $\mathcal{L}^p_{p^r}$ is isomorphic to the orthogonal sum of p^{r-1} copies of the Craig lattice $A^{\frac{p-1}{4}}_{p-1}$, the copies being permuted by a primitive p^{r-1}-st root of unity. See for instance [1] for a description of the Craig lattices as ideal lattices. If $p = 2$ and $r \geq 3$, then

$\mathcal{L}^p_{p^r}$ is isomorphic to 2^{r-3} copies of the root lattice D_4, the copies being permuted by a primitive 2^{r-3}-rd unity.

2.2. The composite case. Let p and q be odd prime numbers with $p \equiv q \equiv 3 \pmod 4$. Suppose that $(\frac{q}{p}) = 1$, where $(\frac{q}{p})$ denotes the Legendre symbol. Let r and s be two positive integers. Let $m = p^r q^s$, and let K be the cyclotomic field $K = \mathbf{Q}(\zeta_m)$.

We have $\mathcal{D} = J_1 J \overline{J}$, where J_1 is above p and $J\overline{J}$ above q. Indeed, we have $(\frac{-p}{q}) = (\frac{-1}{q})(\frac{p}{q}) = (-1)(-1) = 1$. Hence q splits in $\mathbf{Q}(\sqrt{-p})$, and so the extension of q to K is of the form $J\overline{J}$. This implies that the different is of the form described above. Let P be the unique prime ideal above p in $\mathbf{Z}[\zeta_{p^r}]$, and let $\widetilde{P}$ be the extension of P to O (this is not necessarily a prime ideal). Then $J_1 = \widetilde{P}^a$, where $a = p^{r-1}(pr - r - 1)$. Set $s = \frac{p^{r-1}(p-1)-2a}{4}$. Let $I_1 = \widetilde{P}^s$, and $I = I_1 J_2^{-1}$. Let $b : I \times I \to \mathbf{Z}$ be given by $b(x,y) = \mathrm{Tr}(x\overline{y})$.

Notation. We denote the ideal lattice constructed above by $\mathcal{L}^p_{p^r q^s}(J)$.

Proposition 2. *Let p and q be odd prime numbers with $p \equiv q \equiv 3 \pmod 4$. Suppose that $(\frac{q}{p}) = 1$, where $(\frac{q}{p})$ denotes the Legendre symbol. Let r and s be two positive integers. Let $m = p^r q^s$, and let K be the cyclotomic field $K = \mathbf{Q}(\zeta_m)$. Then the lattice $\mathcal{L}^p_m(J)$ constructed above is an even, p–modular ideal lattice of trace type over K. It has rank $\varphi(m)$ and determinant $p^{\frac{\varphi(m)}{2}}$.*

Proof. Let $\mathcal{L}^p_m(J)$ be given by (I, b) as above. Let $\sigma : K \to K$ be given by multiplication with $\sqrt{-p}$. Then a straightforward computation shows that $\sigma I^* = I$. Clearly σ is a similarity with multiplier p. Therefore (I, b) is a p–modular ideal lattice, and it is clearly of trace type. By [5, Proposition 2.12], it is even.

Example 1. Let $K = \mathbf{Q}(\zeta_{21})$, and let Q be one of the two prime ideals above 7. Set $J = Q^5$. We then obtain the 3–modular ideal lattice $\mathcal{L}^3_{21}(J)$ of rank 12. It is shown in [7] that this lattice is isomorphic to the Coxeter–Todd lattice K_{12}.

3. Modular ideal lattices

In this section, we characterize the cyclotomic fields over which there exist modular ideal lattices.

Theorem 1. *There exists a modular ideal lattice if and only if m is not a power of a prime p with $p \equiv 1 \pmod 4$.*

The proof is based on the following lemmas :

Lemma 1. *Suppose that m is not a prime power. Then there exists a unimodular ideal lattice if and only if $\varphi(m) \equiv 0 \pmod 8$.*

Proof. See [3, Proposition 1.8].

Lemma 2. *Suppose that $m = p^r$ with p prime. Then there exists a modular ideal lattice if and only if $p \not\equiv 1 \pmod 4$.*

Proof. If $m = 2$ or 4, then the unit lattice is a unimodular ideal lattice. Hence we may assume that either p is an odd prime, $p \equiv 3 \pmod 4$, or $p = 2$ and $r \geq 3$, and Proposition 1 shows the existence of a p–modular lattice $\mathcal{L}^p_{p^r}$ in this case.

Conversely, suppose that p is a prime and $p \equiv 1 \pmod 4$. Let us show that in this case, no modular ideal lattice exists. Let us denote by d_K the absolute value of the discriminant of K. Note that if $b : I \times I \to \mathbf{Z}$, $b(x,y) = \mathrm{Tr}(\alpha x \overline{y})$ is an ideal lattice, then $\det(b) = \mathrm{N}(\alpha) N(I)^2 d_K$. As $\alpha \in F$, the factor $\mathrm{N}(\alpha)N(I)^2$ is a square. We have $d_K = p^a$ with $a = p^{r-1}(pr - r - 1)$. Then a is an odd integer, so d_K is not a square. This implies that $\det(b)$ cannot be a square. On the other hand, if b is a modular lattice, then $\det(b) = \ell^{n/2}$ for some integer ℓ. The hypothesis $p \equiv 1$ (mod) 4) implies that $n/2$ is an even integer. Therefore $\det(b)$ is a square. This leads to a contradiction, hence there is no modular ideal lattice.

Lemma 3. *Suppose that $m = p^r q^s$ with p and q prime numbers such that $p \equiv q \equiv 3 \pmod 4$. Then there exists a modular ideal lattice.*

Proof. By quadratic reciprocity, we have $(\frac{p}{q}) = -(\frac{q}{p})$. Hence one of these must be equal to 1. Suppose that $(\frac{q}{p}) = 1$. Then Proposition 2 of §2 shows the existence of a p–modular ideal lattice.

Proof of Theorem 1. Therorem 1 follows immediately from Lemmas 1.–3. Indeed, if $m = p^r$ or $2p^r$ for some prime p, then we apply Lemma 2. If $m = p^r q^s$ with p and q prime numbers such that $p \equiv q \equiv 3 \pmod 4$, then apply Lemma 3. In all other cases, $\varphi(m)$ is divisible by 8, so we may apply Lemma 1.

Corollary 1. *Suppose that m is not a power of a prime p such that $p \equiv 1 \pmod 4$, and that $m \neq 2, 4$. Then there exists an even modular lattice.*

Proof. Indeed, if m is not a power of 2, then any ideal lattice is even by [5, Proposition 2.12]. Suppose that $m = 2^r$, $r \geq 3$. Then by Proposition 1 there exists an even 2–modular lattice.

4. Modular ideal lattices of trace type

The aim of this section is to characterize the cyclotomic fields for which there exists a modular ideal lattice *of trace type*. We keep the notation of the preceding sections, in particular $K = \mathbf{Q}(\zeta_m)$ is the cyclotomic field of the m–th roots of unity. Recall that m is odd, or divisible by 4, and that we denote by $\mathcal{D}_K$ the different of K.

Definition 3. Let p be a prime divisor of m. We say that *p is a norm of m* if we have $\mathcal{D}_K = I J \overline{J}$ for some integral O–ideals I and J such that J is above p and I is prime to p.

The following propositions give some simple sufficient conditions for a prime p to be a norm of m.

Proposition 3. *Let p be an odd prime divisor of m. If at least one of* (i) *or* (ii) *below holds, then p is a norm of m.*

(i) *There exists an odd prime divisor q of m such that $q \equiv 3 \pmod 4$, and $(\frac{p}{q}) = 1$.*

(ii) *m is divisible by 4, and $p \equiv 1 \pmod 4$.*

Proposition 4. *Suppose that m is divisible by* 4*. Then* 2 *is a norm of m.*

Proof of Propositions 3 and 4. The statements follow from the decomposition properties of prime numbers in cyclotomic fields. For instance, let us check that a prime satisfying hypothesis (i) of Proposition 3 is a norm of m. Let q be a prime number as in (i). As $q \equiv 3 \pmod 4$, we have $\mathbf{Q}(\sqrt{-q}) \subset K$. If $p \equiv 1 \pmod 4$, then $(\frac{q}{p}) = 1$. We have $(\frac{-q}{p}) = (\frac{-1}{p})(\frac{q}{p}) = 1$. Therefore p splits in $\mathbf{Q}(\sqrt{-q})$, hence it is a norm in m. If $p \equiv 3 \pmod 4$, then $(\frac{q}{p}) = -(\frac{p}{q}) = -1$. We have $(\frac{-q}{p}) = (\frac{-1}{q})(\frac{q}{p}) = (-1)(-1) = 1$, the prime p splits in $\mathbf{Q}(\sqrt{-q})$ and hence p is a norm in m. The other verifications are of a similar nature.

Definition 4. Let m' be a divisor of m. We say that *m' is a norm of m* if all the prime divisors of m' are norms of m.

Theorem 2. *Let $\ell = 1$ or a prime number p, with $p \not\equiv 1 \pmod 4$. Let $m = \ell^r m'$, with m' prime to ℓ. Then there exists an ℓ–modular ideal lattice of trace type if and only if m' is a norm of m.*

This will be proved in §6, after introducing some more constructions of modular ideal lattices in §5.

5. More constructions of modular ideal lattices

In this section, we will show that under the hypothesis of Theorem 2, one can explicitly construct ℓ–modular ideal lattices of trace type. Moreover, if $\ell = 1$ or a prime number, these are all ℓ–modular ideal lattices of trace type.

Let $\ell = 1$. Suppose that m is a norm of m. Then by Propositions 3 and 4, we have $\mathcal{D}_K = J\overline{J}$ for some O–ideal J. Set $I = J^{-1}$, and let $b : I \times I \to \mathbf{Z}$ be given by $b(x, y) = \mathrm{Tr}(x\overline{y})$.

Notation. Let us denote by $\mathcal{L}^1_m(J)$ the lattice constructed above.

Proposition 5. *Suppose that m is a norm of m. Then $\mathcal{L}^1_m(J)$ is a unimodular ideal lattice of trace type. If moreover m is not a power of 2, then it is an even lattice.*

Proof. It is clear that $\mathcal{L}^1_m(J)$ is a unimodular ideal lattice of trace type. If m is not a power of 2, then this lattice is even by [5, Proposition 2.12].

Suppose now that $\ell = p$ is a prime number, with $p \not\equiv 1 \pmod 4$. Let $m = p^r m'$, where m' is prime to p. Suppose that m' is a norm of m. Then by Propositions 3 and 4, we have $\mathcal{D}_K = J_1 J\overline{J}$, where J_1 is above p, and J is some O–ideal prime to J_1. Let us denote by P the unique prime ideal of $\mathbf{Q}(\zeta_{p^r})$ above p, and let $\widetilde{P}$ the extension of P to O. Then $J_1 = \widetilde{P}^a$, where $a = p^{r-1}(pr - r - 1)$. Set $s = \frac{p^{r-1}(p-1)-2a}{4}$. Let $I_1 = \widetilde{P}^s$, and $I = I_1 J^{-1}$. Let $b : I \times I \to \mathbf{Z}$ be given by $b(x, y) = \mathrm{Tr}(x\overline{y})$.

Notation. Let us denote by $\mathcal{L}^p_m(J)$ the ideal lattice constructed above.

Proposition 6. *Let $m = p^r m'$, with p prime, such that $p \not\equiv 1 \pmod 4$, and m' prime to p. Suppose that m' is a norm of m. Then $\mathcal{L}^p_m(J)$ is a p–modular ideal lattice of trace type over the cyclotomic field $K = \mathbf{Q}(\zeta_m)$. Moreover, if m is not a power of 2, then this lattice is even.*

Proof. Let $\mathcal{L}^p_m(J)$ be given by (I, b) as above. Let $\sigma : K \to K$ be given by multiplication with $\sqrt{-p}$. Then a straightforward computation shows that $\sigma I^* = I$. Clearly σ is a similarity with multiplier p. Therefore (I, b) is a p–modular ideal lattice, and it is clearly of trace type. If m is not a power of 2, then this lattice is even by [5, Proposition 2.12].

Remark. Note that the lattices of 2.1. and 2.2. are special cases of $\mathcal{L}^p_m(J)$.

This construction can be used to obtain several known lattices, for instance Craig's construction in [9] of the Leech lattice over $\mathbf{Q}(\zeta_{39})$ is of the form $\mathcal{L}^1_{39}(J)$ for some ideal J.

6. Characterization of modular ideal lattices of trace type

Theorem 2 of §5 follows from the following characterization of modular ideal lattices of trace type.

Theorem 3. *Let $\ell = 1$ or a prime number p such that $p \not\equiv 1 \pmod 4$. Let $m = \ell^r m'$, with m' prime to ℓ. Suppose that m' is a norm of m. Then $\mathcal{L}^{\ell}_m(J)$ is an ℓ–modular ideal lattice of trace type over $\mathbf{Q}(\zeta_m)$. Conversely, any ℓ–modular ideal lattice of trace type is of the form $\mathcal{L}^{\ell}_m(J)$ for some ideal J.*

Proof. By Propositions 5 and 6, the lattice $\mathcal{L}^{\ell}_m(J)$ is an ℓ–modular ideal lattice of trace type. Conversely, it is clear that any modular lattice of trace type and of determinant a power of ℓ is of the form $\mathcal{L}^{\ell}_m(J)$ for some ideal J. This concludes the proof of Theorem 3.

Proof of Theorem 2. The existence part follows immediately from Theorem 3. Conversely, by Propositions 3 and 4 a lattice of the shape $\mathcal{L}^{\ell}_m(J)$ can only exist if m' is a norm of m. By Theorem 3 these are the only ℓ–modular ideal lattices of trace type, hence the proof of Theorem 2 is complete.

References

[1] C. BACHOC, C. BATUT, *Etude Algorithmique de Réseaux Construits avec la Forme Trace.* Exp. Math. **1** (1992), 184–190.

[2] C. BATUT, H.-G. QUEBBEMANN, R. SCHARLAU, *Computations of Cyclotomic Lattices.* Exp. Math. **4** (1995), 175–179.

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

[4] E. BAYER–FLUCKIGER, *Lattices, cyclic group actions and number fields.* In preparation.

[5] E. BAYER–FLUCKIGER, *Lattices and number fields.* Comtemp. Math. **241** (1999), 69–84.

[6] E. BAYER–FLUCKIGER, *Ideal lattices.* To appear.

[7] E. BAYER–FLUCKIGER, J. MARTINET, *Réseaux liés à des algèbres semi–simples.* J. reine angew. Math. **415** (1994), 51–69.

[8] M. CRAIG, *Extreme forms and cyclotomy. Mathematika* **25** (1978), 44–56.

[9] M. CRAIG, *A cyclotomic construction of Leech's lattice.* Mathematika **25** (1978), 236–241.

[10] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, Masson (1996).

[11] H.-G. QUEBBEMANN, *Modular Lattices in Euclidean Spaces.* J. Number Theory **54** (1995), 190–202.

[12] J.-P. SERRE, *Cours d'arithmétique.* P.U.F. (1970).

Eva BAYER–FLUCKIGER
UMR 6623 du CNRS
Laboratoire de Mathématiques de Besançon
16, route de Gray
25030 Besançon
France
E-mail : bayer@math.univ-fcomte.fr