COMPUTATIONS OF CYCLOTOMIC LATTICES

C. Batut, H.-G. Quebbemann, R. Scharlau

Abstract

We study even modular lattices of level ℓ and dimension $2(p-1)$, p prime, which arise from the ideal class group of the p-th cyclotomic extension of $\mathbb{Q}(\sqrt{-\ell})$. After giving the basic theory we concentrate on Galois-invariant ideals, obtain computational results on minimal vectors and isometries, and identify several old or new extremal lattices.

1 Introduction

In this paper (a sequel to [BB], [Q1], [Q2]) we mainly deal with a family of lattices in euclidean spaces which are related to Craig's $A_{p-1}^{(m)}$. Our lattice $B_{n,\ell}^{(m)}$ has dimension $n = 2(p-1)$, contains the tensor product of $A_{p-1}^{(m)}$ with the ring of integers in $\mathbb{Q}(\sqrt{-\ell})$, and is hermitian-unimodular over this ring (therefore similar to its $\mathbb{Z}$-dual, with determinant ℓ^{p-1}). Like $A_{p-1}^{(m)}$ it admits a simple description as a cyclotomic ideal which displays the affine-linear group $\mathbb{F}_p^+ \rtimes \mathbb{F}_p^*$ as a group of automorphisms. Our family, however, includes more prominent individuals: there are $E_8 = B_{8,1}^{(1)}$, $K_{12} = B_{12,3}^{(1)}$, $\Lambda_{24} = B_{24,1}^{(2)}$, but also Plesken and Nebe's $[2.M_{12}.2]_{20} = B_{20,2}^{(2)}$ and $[2.M_{22}.2]_{20} = B_{20,7}^{(2)}$ (the latter appears to give the highest "isodual Hermite number" known for $n = 20$, and it is one of two "extremal" lattices of minimum 8 we know). On the other hand, our lattices are harder to analyze than Craig's: we cannot give a general lower bound on the minimum, nor theoretically decide eutaxy when $\ell > 3$. Information on these and related questions will be obtained for $p \leq 29$ by machine computations using PARI.

Part of the work on this paper was done during stays of the second author at the University of Bordeaux to which he expresses his gratitude for its hospitality.

2 Unimodular cyclotomic lattices over imaginary-quadratic fields

Let ℓ be a square-free positive integer, $K = \mathbb{Q}(\sqrt{-\ell})$, and $\mathcal{O}_K$ the ring of integers in K. Given a positive definite hermitian space (V, h) of dimension k over K, we also consider it as an inner product space of dimension $n = 2k$ over $\mathbb{Q}$ for

[0]*Key words and phrases:* lattice, integral quadratic form, Craig lattice, hermitian lattice, modular lattice, extremal lattice, isodual Hermite number, cyclotomic ideal.

1991 Mathematics Subject Classification: 11E12; 11H55, 11R18, 11-04.

$$x \cdot y = c\,\mathrm{Tr}_{K/\mathbb{Q}}\, h(x,y), \quad c = \begin{cases} 1 & \ell \equiv 3 \pmod 4 \\ 1/2 & \text{otherwise} \end{cases} \tag{2.1}$$

Then, if Λ is an $\mathcal{O}_K$-lattice on V, its hermitian dual lattice Λ_h^* is $\sqrt{-\ell}\Lambda^*$, where Λ^* denotes the euclidean dual. We shall deal with lattices satisfying

$$\Lambda = \Lambda_h^*, \quad \text{and} \quad x \cdot x \in 2\mathbb{Z} \quad \text{for all} \quad x \in \Lambda. \tag{2.2}$$

(Of course, for $\ell \equiv 3 \pmod 4$ the first condition here implies the second one.) As a euclidean lattice such a Λ is even and isometric to $\sqrt{\ell}\Lambda^*$, therefore of determinant ℓ^k.

Let p be an odd prime not dividing ℓ, and ζ a non-trivial p-th root of unity over K. We put $F = K(\zeta)$ and remark that $[F : K] = p - 1$. Consequently, if p divides the order of the isometry group $\mathrm{Aut}_h\Lambda$ for a lattice Λ as above, part of V must be a nonzero F-vector space, and therefore $p - 1$ is at most equal to k. We shall deal with the case $k = p - 1$, and then can assume (cf. [Fe], Section 9)

$$V = F, \quad h(x,y) = \mathrm{Tr}_{F/K}(\delta x\overline{y}), \quad \Lambda = \mathcal{I} \tag{2.3}$$

where δ is a totally positive element in $F^+ = F \cap \mathbb{R}$ and $\mathcal{I}$ is a fractional ideal of F. Note that $\Lambda_h^* = (\delta\overline{\mathcal{I}}\mathcal{D}_{F/K})^{-1}$ where $\mathcal{D}_{F/K} = (1-\zeta)^{p-2}$ is the different. To satisfy (2.2) we therefore require that

$$p\delta\mathcal{I}\overline{\mathcal{I}} = (1-\zeta). \tag{2.4}$$

Actually (2.4) is equivalent to (2.2) because the absence of dyadic ramification in F/F^+ guaranties that Λ is even ([BM], Section 3).

Proposition 1 *Condition (2.4) can be satisfied (with $\delta \in F^+$ totally positive) if and only if we have*

$$\left(\frac{-\ell}{p}\right) = 1 \tag{2.5}$$

Proof. The extension F/F^+ is unramified at all finite primes, and so class field theory tells us that the left-hand side of (2.4) is in the kernel of the Artin map. In other words, for (2.4) to hold $(1-\zeta)$ must be decomposed in F, and so p decomposed in K. Conversely, if this is satisfied, we can write

$$(1-\zeta) = \mathcal{P}\overline{\mathcal{P}} \ \text{ with a prime ideal } \mathcal{P} \text{ in } \mathcal{O}_F, \tag{2.6}$$

and then (2.4) holds with $\delta = 1/p$ and $\mathcal{I} = \mathcal{P}$. ■

From now on we assume (2.5) and fix $\mathcal{P}$ as in (2.6). In order to satisfy (2.4) with $\delta = 1/p$, we may also put $\mathcal{I} = \mathcal{J}\overline{\mathcal{J}}^{-1}\mathcal{P}$ where $\mathcal{J}$ is any nonzero fractional ideal of F. This will turn out to be already the most general case. Namely, let $cl(\mathcal{J})$ denote the ideal class of $\mathcal{J}$, and $Cl(F)$ the class group; put $G = Gal(F/K)$. The K-isometry class of the lattice Λ will be denoted by $[\Lambda]$.