Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Number Theory 114 (2005) 394–411

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Modular lattices over cyclotomic fields[☆]

Eva Bayer-Fluckiger*, Ivan Suarez

Departement de Mathematiques, Ecole Polytechnique Federale de Lausanne, CH-1015 Lausanne, Switzerland

Received 2 March 2004; revised 11 August 2004

Available online 1 February 2005

Communicated by J.S. Hsia

Abstract

This paper is concerned with modular lattices over cyclotomic fields. In particular, the notion of Arakelov modular ideal lattice is introduced. All the cyclotomic fields over which there exists an Arakelov modular lattice of given level are characterised.

Keywords: Lattices; Number fields; Modular forms

0. Introduction

This paper is concerned with integral lattices, i.e. finitely generated free abelian groups together with a positive definite integral bilinear form. Among integral lattices, unimodular ones play a very central role. A unimodular lattice is equal to its dual, and the theta series of even unimodular lattices are modular forms for the full modular group. Recently, H.-G. Quebbemann introduced the notion of *modular lattice*, i.e. a lattice which is similar to its dual (see [14–16]). The theta series of a modular lattice is a modular form for the group $\Gamma_0(\ell)$ (for some integer ℓ) which is a subgroup of the full modular group, and is also an eigenform of the Fricke operator (see [14]). H.-G.

[☆] The authors gratefully acknowledge support from the Swiss National Science Fundation, Grant No 200021-101918/1.

* Corresponding author. Fax: +41 693 42 50.

E-mail addresses: eva.bayer@epfl.ch (E. Bayer-Fluckiger), ivan.suarez@epfl.ch (I. Suarez).

URL: http://alg-geo.epfl.ch/~bayer/.

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2004.10.005

Quebbemann also observed that if a lattice satisfies a stronger condition (he called such a lattice a *strongly modular lattice*), then its theta series is also an eigenform for the Atkin–Lehner involutions (see [15,16]). This led to a definition of analytic extremality for modular and strongly modular lattices (see [17] or [8] for a survey).

An *ideal lattice* is an ideal of a number field K together with a bilinear form satisfying an invariance relation (see [3,5]). Ideal lattices correspond bijectively to Arakelov divisors over $\mathcal{O}_K$ (see [18]). We will investigate here how to use ideal lattices in order to construct modular lattices (similar attempts can be found in [1,4]). This will lead to the definition of an *Arakelov-modular lattice* on a CM-field K (see Section 1).

After giving some definitions, notation and basic facts in Sections 1 and 2, we will consider in Section 3 the CM-fields which contain an Arakelov-modular lattice. We will show that any Arakelov-modular lattice over a cyclotomic field is strongly modular (see Corollary 3.6). Then, fixing an integer ℓ, we will characterize all cyclotomic fields in which there exists an Arakelov-modular lattice of level ℓ (see Propositions 3.7 and 3.8 for the trace type case, and Proposition 3.13 or Theorem 3.14 for the general case). In Section 4, for a given CM-field K and a given Arakelov-modular lattice over K, we will give all the Arakelov-modular lattices of the same level which can be constructed over K (see Proposition 4.2). The last section contains some examples of modular lattices whose similarity is induced by the action of the Galois group of a Galois extension.

1. Definitions and notation

1.1. Modular lattices

A lattice is a pair (L, b), where L is a free $\mathbb{Z}$-module of finite rank, and $b : L_{\mathbb{R}} \times L_{\mathbb{R}} \to \mathbb{R}$ is a definite positive symmetric bilinear form (with $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$). We often write L instead of (L, b). Let $L^* = \{x \in L_{\mathbb{R}} : b(x, L) \subseteq \mathbb{Z}\}$ be the dual lattice of L. The lattice (L, b) is called *integral* (resp. *unimodular*) if $L \subseteq L^*$ (resp. if $L = L^*$). We say that a lattice (L, b) is *even* if $b(x, x)$ is even for all $x \in L$.

From now on, lattice will mean even lattice. Let a be a positive constant. The lattice ${}^{a}L$ will denote the rescaled lattice (L, ab). Let ℓ be a positive integer, and let m be a divisor of ℓ. We will say that m is an *exact divisor* of ℓ (notation : $m||\ell$) if $\ell = mm'$, where m and m' are coprime integers. For any exact divisor m of ℓ, we define $L^{*m} = \frac{1}{m}L \cap L^*$.

Definition 1.1. A lattice (L, b) is said to be *ℓ-modular* (or *modular of level ℓ*) if the lattices L and ${}^{\ell}(L^*)$ are isomorphic.

A lattice (L, b) is said to be *strongly modular* if $L \cong {}^{m}(L^{*m})$ for all $m||\ell$.

1.2. Ideal lattices

Let K be a CM-field and F be the maximal real subfield of K. Let $\mathcal{O}_K$ denote the ring of integers of K. An *ideal lattice* is a lattice $(\mathcal{I}, b)$, where $\mathcal{I}$ is a fractional $\mathcal{O}_K$-ideal and $b : \mathcal{I} \times \mathcal{I} \to \mathbb{R}$ is such that $b(\lambda x, y) = b(x, \overline{\lambda} y)$ for all $x, y \in \mathcal{I}$ and for all $\lambda \in \mathcal{O}_K$. This definition is equivalent to saying that there exists a totally positive $\alpha \in F_{\mathbb{R}}(= F \otimes \mathbb{R})$ such that $b(x, y) = \mathbf{Tr}(\alpha x \overline{y})$ (cf. [5, Proposition 1]). An ideal lattice $(\mathcal{I}, b)$ satisfying $b(x, y) = \mathbf{Tr}(\alpha x \overline{y})$ will be denoted $(\mathcal{I}, \alpha)$. From now on, we will only deal with ideal lattices $(\mathcal{I}, \alpha)$ which are integral and where $\alpha \in F$. Recall that the dual lattice of an ideal lattice $(\mathcal{I}, \alpha)$ is $\mathcal{I}^* = \alpha^{-1}\mathcal{D}_K^{-1}\overline{\mathcal{I}}^{-1}$, where $\mathcal{D}_K$ is the different of $K/\mathbb{Q}$. If 2 does not ramify in K/F, then any integral ideal lattice over K is even (see [6, Proposition 3.1]). The reader can refer to [3,5] to learn about basic facts concerning ideal lattices.

Let $(\mathcal{I}, \alpha)$ and $(\mathcal{I}', \alpha')$ be two ideal lattices. We say that these two lattices are *Arakelov-equivalent*, and we write $(\mathcal{I}, \alpha) \cong_A (\mathcal{I}', \alpha')$, if there exists $\beta \in K^\times$ such that $\mathcal{I}' = \beta\mathcal{I}$ and $\alpha' = (\beta\overline{\beta})^{-1}\alpha$. Notice that two ideal lattices are Arakelov-equivalent if and only if the corresponding Arakelov divisors are in the same class in the Arakelov class group (see [18, Sections 2 and 4]).

Definition 1.2. Let $(\mathcal{I}, \alpha)$ be an ideal lattice over K. We say that $(\mathcal{I}, \alpha)$ is *Arakelov-modular* of level ℓ if $(\mathcal{I}, \alpha) \cong_A (\mathcal{I}^*, \ell\alpha)$. Moreover, if $(\mathcal{I}, \alpha) \cong_A (\mathcal{I}^{*m}, m\alpha)$ for all $m || \ell$, the lattice $(\mathcal{I}, \alpha)$ is said to be *strongly Arakelov-modular* of level ℓ.

It is easy to see that Arakelov-modular lattices (resp. strongly Arakelov-modular lattices) are modular (resp. strongly modular).

2. Good divisors in cyclotomic fields

In this section, we introduce the notion of *good divisor* which will be needed in the sequel. Let K be a CM-field, and F be the maximal totally real subfield of K. Throughout this section, we suppose that at most one finite prime is ramified in K/F (K/F ramifies of course at all the infinite primes).

Proposition 2.1. *Let $p \in \mathbb{Z}$ be a prime number which does not ramify in $K/\mathbb{Q}$. Then p is a norm of K/F if and only if the prime ideals $\mathfrak{P}$ of K above p satisfy $\mathfrak{P} \neq \overline{\mathfrak{P}}$.*

Proof. Assume that all prime ideals $\mathfrak{P}$ above p satisfy $\overline{\mathfrak{P}} \neq \mathfrak{P}$. Assume first that K/F is unramified at all finite primes. In that case, we will show that p is a local norm at each prime. Actually, since p is totally positive, it is a local norm at the infinite primes. If $\mathfrak{q}$ is a prime ideal of F relatively prime to p, then p is a unit at $\mathfrak{q}$. But the extension $K_{\mathfrak{Q}}/F_{\mathfrak{q}}$ is unramified so p is a local norm at $\mathfrak{Q}$. If $\mathfrak{p}$ is a prime ideal of F above p, then $[K_{\mathfrak{P}} : F_{\mathfrak{p}}] = 1$ since $\overline{\mathfrak{P}} \neq \mathfrak{P}$. Therefore p is a local norm at each prime, and the Hasse Norm theorem gives us that p is a norm of K/F. Assume now that K/F is ramified at one prime. It only remains to check whether p is a local norm at the ramified finite prime, but this is given by the Hilbert reciprocity law.

Conversely, take $\mathfrak{P}$ a prime ideal over p such that $\mathfrak{P} = \overline{\mathfrak{P}}$. Let $N_{K_{\mathfrak{P}}/F_{\mathfrak{P}}} : K_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the local norm at $\mathfrak{P}$ and $\mathfrak{U}_{\mathfrak{P}}$ be the group of units of $F_{\mathfrak{P}}$. Then $K_{\mathfrak{P}}/F_{\mathfrak{P}}$ is unramified of degree 2, hence $N_{K_{\mathfrak{P}}/F_{\mathfrak{P}}}(K_{\mathfrak{P}}^\times) = \mathfrak{U}_{\mathfrak{P}}(K_{\mathfrak{P}}^\times)^2$, where $(K_{\mathfrak{P}}^\times)^2 = \{x^2 : x \in K_{\mathfrak{P}}^\times\}$ (see

[10], e.g. 36:16). Since the extension $K_{\mathfrak{P}}/\mathbb{Q}_p$ is unramified, p is a prime element in $K_{\mathfrak{P}}$ and does not belong to $\mathfrak{U}_{\mathfrak{P}}(K_{\mathfrak{P}}^{\times})^2$. Therefore p is not a norm of K/F. This concludes the proof. □

From now on K will be a *cyclotomic field*, $K = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. In this case, $F = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. We can assume that n is odd or $4|n$. The cyclotomic field K satisfies the assumptions we made at the beginning of this section, but there is a condition easier to check in this case.

Proposition 2.2. *Let p be a prime number not dividing n. Let $f = f_{K/\mathbb{Q}}$ be the residue class degree of p in $K/\mathbb{Q}$ (i.e. $f = \min\{f' : p^{f'} \equiv 1 \bmod n\}$). Then p is a norm of K/F if and only if one of the following is true*:

(1) *f is odd,*
(2) *f is even and $p^{\frac{f}{2}} \not\equiv -1 \bmod n$.*

Proof. We can apply Proposition 2.1, so this last proposition is equivalent to checking whether the canonical involution is in the decomposition group of $\mathfrak{P}$ over $\mathbb{Q}$. Recall that this decomposition group is defined as $\{\sigma \in \mathbf{Gal}(K/\mathbb{Q}) : \mathfrak{P}^{\sigma} = \mathfrak{P}\}$, we call it $\mathfrak{D}_{\mathfrak{P}}$. The prime $\mathfrak{P}$ is not ramified in $K/\mathbb{Q}$ because $p \nmid n$, so $\mathfrak{D}_{\mathfrak{P}}$ is cyclic generated by the Frobenius element $\sigma_{\mathfrak{P}}$. Recall that the canonical involution acts on ζ_n as $\overline{\zeta_n} = \zeta_n^{-1}$. The only element of order 2 of $\mathfrak{D}_{\mathfrak{P}}$ is $\sigma_{\mathfrak{P}}^{\frac{f}{2}}$ when f is even, and $\mathfrak{D}_{\mathfrak{P}}$ does not contain any element of order 2 when f is odd. Therefore p is not a norm of K/F if and only if f is even and

$$\zeta_n^{p^{\frac{f}{2}}} = \sigma_{\mathfrak{P}}^{\frac{f}{2}}(\zeta_n) = \zeta_n^{-1}$$

if and only if f is even and $p^{\frac{f}{2}} \equiv -1 \bmod n$. Hence the proposition is proved. □

We next introduce the notion of good divisor. Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field ($n \not\equiv 2 \bmod 4$), and p be a prime number dividing n.

Definition 2.3. Let p be a prime number dividing n and let $K = \mathbb{Q}(\zeta_n)$. The prime p is a *good divisor* of n if the different $\mathcal{D}_K$ of $K/\mathbb{Q}$ can be written $\mathcal{D}_K = \mathcal{I}\mathcal{J}\overline{\mathcal{J}}$, where $\mathcal{J}$ is a K-ideal over p and $\mathcal{I}$ is an ideal relatively prime to p.

An integer m is *good* for n if all the primes dividing m are good divisors of n.

Proposition 2.4. *Let p be a prime number dividing n. Write $n = p^r n'$, where p and n' are relatively prime.*

(1) *If p is odd, then p is a good divisor of n if and only if p is a norm of $\mathbb{Q}(\zeta_{n'})/\mathbb{Q}(\zeta_{n'} + \zeta_{n'}^{-1})$.*
(2) *If $p = 2$, then p is always a good divisor of n.*

Proof. Let $K' = \mathbb{Q}(\zeta_{n'})$ and $F' = \mathbb{Q}(\zeta_{n'} + \zeta_{n'}^{-1})$. If p is a norm of K'/F', then p is a good divisor of n. Conversely, assume p is odd, and p is a good divisor of n. Let $\mathfrak{P}$ be an ideal of K above p and denote $v_{\mathfrak{P}}$ the valuation at $\mathfrak{P}$. We have $v_{\mathfrak{P}}(\mathcal{D}_K) = p^{r-1}(pr - r - 1)$, so if we write $\mathcal{D}_K = \mathcal{I}\mathcal{J}\overline{\mathcal{J}}$, then $v_{\mathfrak{P}}(\mathcal{J}\overline{\mathcal{J}}) = p^{r-1}(pr - r - 1)$ is odd. Therefore $\mathfrak{P} \neq \overline{\mathfrak{P}}$ and $\mathfrak{P}' \neq \overline{\mathfrak{P}'}$, if $\mathfrak{P}' = \mathfrak{P} \cap K'$, since $\mathfrak{P}$ is totally ramified in K/K'. Hence p is a norm of K'/F'.

Assume now $p = 2$, so $r \geqslant 2$. If $\mathfrak{q}$ is a prime ideal of $\mathbb{Q}(\zeta_{2^r})$ above 2, then we can write $\mathcal{D}_{\mathbb{Q}(\zeta_{2^r})} = \mathfrak{q}^{2^{r-2}(r-1)}\overline{\mathfrak{q}}^{2^{r-2}(r-1)}$. Since $\mathcal{D}_K = \mathcal{D}_{\mathbb{Q}(\zeta_{2^r})}\mathcal{D}_{K'}$, we find that 2 is a good divisor of n. This completes the proof. □

Corollary 2.5. *Let p be an odd prime number dividing n. Write $n = p^r n'$, where* $\gcd(p, n') = 1$. *Let $f = \min\{f' : p^{f'} \equiv 1 \bmod n'\}$. Then p is a good divisor of n if and only if one of the following is true*:

(1) *f is odd,*

(2) *f is even and $p^{\frac{f}{2}} \not\equiv -1 \bmod n'$.*

3. Existence results

The aim of this section is to give existence conditions of Arakelov-modular lattices on a CM-field K. We keep the notations of Section 1.

Proposition 3.1. *There exists an Arakelov-modular lattice $(\mathcal{I}, \alpha)$ of level ℓ over K if and only if ℓ is a norm of K/F and if there exists a fractional ideal $\mathfrak{a}$ of K such that $\alpha^{-1}\lambda\mathcal{D}_K^{-1} = \mathfrak{a}\overline{\mathfrak{a}}$, where $\ell = \lambda\overline{\lambda}$, $\lambda \in K$.*

Proof. Let $\mathcal{D}_K$ be the different of $K/\mathbb{Q}$. Recall that the dual lattice of $(\mathcal{I}, \alpha)$ is $(\mathcal{I}^*, \alpha)$, where $\mathcal{I}^* = \alpha^{-1}\mathcal{D}_K^{-1}\overline{\mathcal{I}}^{-1}$. Assume first that the lattice $(\mathcal{I}, \alpha)$ is Arakelov-modular of level ℓ. Take $\beta \in K^*$ such that $(\mathcal{I}, \alpha) = (\beta\mathcal{I}^*, \ell\alpha(\beta\overline{\beta})^{-1})$. Hence $\ell = \beta\overline{\beta}$, and $\beta\mathcal{O}_K = \alpha\mathcal{I}\overline{\mathcal{I}}\mathcal{D}_K$. If we let $\mathfrak{a} = \mathcal{I}$ and $\lambda = \beta$, then these are the conditions required.

Conversely, take an ideal $\mathfrak{a}$ and an element $\lambda \in K^*$ satisfying the conditions of the proposition. Let us show that the ideal lattice $(\mathfrak{a}, \alpha)$ is Arakelov-modular. Notice first that we have $(\mathfrak{a}^*, \ell\alpha) = (\lambda^{-1}\mathfrak{a}, \lambda\overline{\lambda}\alpha)$, so it remains to prove that $(\mathfrak{a}, \alpha)$ is integral. Note then that λ is an integer. This follows from the equality $\lambda\mathcal{O}_K = \alpha\mathcal{D}_K\mathfrak{a}\overline{\mathfrak{a}}$ which implies that for all prime ideal $\mathfrak{P}$ of K, we have $v_{\mathfrak{P}}(\lambda) = v_{\overline{\mathfrak{P}}}(\lambda)$. So $v_{\mathfrak{P}}(\lambda) = \frac{1}{2}v_{\mathfrak{P}}(\ell) \geqslant 0$ for all finite prime $\mathfrak{P}$ of K, and λ is an integer. This implies that $\mathfrak{a} = \lambda\mathfrak{a}^* \subseteq \mathfrak{a}^*$, i.e. that $(\mathfrak{a}, \alpha)$ is integral. □

The next result asserts that we can restrict ourselves to finding Arakelov-modular lattices of level ℓ where ℓ is a square-free integer.

Proposition 3.2. *Let K be a CM-field, and ℓ be an integer. Assume there is an Arakelov-modular lattice $(\mathcal{I}, \alpha)$ of level ℓ over K. Write $\ell = \ell_1\ell_2^2$, where ℓ_1 is square-*

free. Then the rescaled lattice $(\mathcal{I}, \ell_2^{-1}\alpha)$ *is integral and is an Arakelov-modular lattice of level* ℓ_1.

Proof. Let $\mathcal{I}^*$ be the dual of $(\mathcal{I}, \alpha)$. Then $\ell_2\mathcal{I}^*$ is the dual lattice of $(\mathcal{I}, \ell_2^{-1}\alpha)$. Take $\lambda \in \mathcal{O}_K$ such that $\lambda\bar{\lambda} = \ell$ and $(\mathcal{I}, \alpha) = (\lambda\mathcal{I}^*, (\lambda\bar{\lambda})^{-1}\ell\alpha)$. Define $\lambda_1 = \lambda/\ell_2$. Then $\lambda_1\bar{\lambda}_1 = \ell_1$ and $\lambda_1\ell_2\alpha^{-1}\mathcal{D}_K^{-1} = \mathcal{I}\bar{\mathcal{I}}$. Proposition 3.1 completes the proof because it tells us that the lattice $(\mathcal{I}, \ell_2^{-1}\alpha)$ is Arakelov-modular of level ℓ_1. □

From now on, ℓ will always denote a square-free integer. We state now a result similar as the one in Proposition 3.1 concerning strongly Arakelov-modular lattices.

Proposition 3.3. *Let* K *be a CM-field and let* ℓ *be a square-free integer. Let* $(\mathcal{I}, \alpha)$ *be an Arakelov-modular lattice of level* ℓ *over* K. *Let* $\lambda \in \mathcal{O}_K$ *be such that* $\lambda\mathcal{I}^* = \mathcal{I}$ *and* $\lambda\bar{\lambda} = \ell$. *Assume that for each* $m||\ell$, *there is an integer* $\beta_m \in \mathcal{O}_K$ *such that*:

(1) $\beta_m\bar{\beta}_m = m$,
(2) $\beta_m\beta_{\ell/m} = \lambda$.

Then the lattice $(\mathcal{I}, \alpha)$ *is strongly Arakelov-modular of level* ℓ *over* K.

Proof. Let $m||\ell$, and let $\mathcal{J} = \mathcal{I}^{*m}$. We have $\mathcal{J} = \mathcal{I}^* \cap \left(\frac{1}{m}\mathcal{I}\right) = \left(\lambda^{-1}\mathcal{I}\right) \cap \left(\frac{1}{m}\mathcal{I}\right)$. Hence $\mathcal{J} = \mathcal{I}\left(\lambda^{-1}\mathcal{O}_K \cap m^{-1}\mathcal{O}_K\right) = \mathcal{I}(\lambda\mathcal{O}_K + m\mathcal{O}_K)^{-1}$. However, since $\bar{\beta}_m$ and $\beta_{\ell/m}$ are relatively prime, we have $\lambda\mathcal{O}_K + m\mathcal{O}_K = \beta_m\beta_{\ell/m}\mathcal{O}_K + \beta_m\bar{\beta}_m\mathcal{O}_K = \beta_m\mathcal{O}_K$. Finally, we check that $\mathcal{J} = \mathcal{I}\beta_m^{-1}$ and $(\mathcal{I}, \alpha) = (\beta_m\mathcal{J}, (\beta_m\bar{\beta}_m)^{-1}m\alpha)$. This equality shows that $(\mathcal{I}, \alpha) \cong_A (\mathcal{I}^{*m}, m\alpha)$ and thus completes the proof. □

Assume the condition of Proposition 3.1. Take an ideal $\mathfrak{a}$ of K such that $\lambda\mathcal{O}_K = \alpha\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_K$. The ideal $\lambda\mathcal{O}_K$ is therefore invariant under the canonical involution. Hence $u = \lambda/\bar{\lambda}$ is a unit for which all real and complex embeddings have norm 1, i.e. u is a root of unity. Let n be the order of u. Assume first that $n \not\equiv 0 \bmod 4$. In this case, either u or $-u$ is a square in $\mathcal{O}_K^\times$ (in fact, if u is of odd order, then $u = u^{n+1} = v^2$ with $v = u^{\frac{n+1}{2}}$, whereas if u is of even order, then $-u$ is of odd order). Hence either ℓ or $-\ell$ is then a square in K, and any prime dividing ℓ must ramify with an even ramification index in the extension $K/\mathbb{Q}$. Assume now that $n \equiv 0 \bmod 4$. As previously, we can remove the part which is prime to 2 in n. Therefore we have just proved the following:

Proposition 3.4. *Let* K *be a CM field. Assume that* $(\mathcal{I}, \alpha)$ *is an Arakelov-modular lattice of level* ℓ. *Then there exists* $\lambda \in K$ *and a* 2^r*th root of unity* $\zeta \in K$ *such that*:

- $\lambda^2 = \zeta\ell$,
- $\lambda\mathcal{I}^* = \mathcal{I}$.

Remark 3.5. In particular, if $\sqrt{-1} \notin K$, we must have either $\sqrt{\ell} \in K$, or $\sqrt{-\ell} \in K$.

Corollary 3.6. *Every Arakelov-modular lattice of level* ℓ *over a cyclotomic field is strongly Arakelov-modular*.

Proof. Let K be a cyclotomic field and let $(\mathcal{I}, \alpha)$ be an Arakelov-modular lattice of level ℓ over K. Let λ be such that $\lambda^2 = \varepsilon\ell$, with $\varepsilon \in \{\pm 1, \pm i\}$ (here, $i = \sqrt{-1}$). Proposition 3.4 tells us that $\lambda\mathcal{I}^* = \mathcal{I}$. Define $\beta_\ell = \lambda$. By Proposition 3.4, all the primes dividing ℓ must ramify in K, so for each $m||\ell$, either m or $-m$ must be a square in K if m is odd, and either im or $-im$ must be a square if m is even. Moreover, we can choose a family $(\beta_m)_{m||\ell}$ of integers of K such that $\beta_m^2 = i^{e(m)}m$ for some $e(m) \in \mathbb{Z}$ and such that this family satisfies the second condition of Proposition 3.3. Therefore the lattice $(\mathcal{I}, \alpha)$ is strongly Arakelov-modular, and the proposition is proved. □

Assume now that $K = \mathbb{Q}(\zeta_n)$ is a cyclotomic field in which all the primes dividing ℓ ramify. Let $\lambda \in K$ be such that $\lambda^2 = \varepsilon\ell$ (where $\varepsilon \in \{\pm 1, \pm i\}$).

Our first result concerns the existence of Arakelov-modular lattices of trace type over cyclotomic fields. Define $\ell_1, \ell_2 \in \mathbb{Z}$ in the following way:

- $\ell = \ell_1\ell_2$,
- if n is odd or divisible by 8, let ℓ_1 be the product of the primes dividing ℓ congruent to 1 modulo 4,
- if $n \equiv 4 \bmod 8$, let ℓ_2 be the product of the primes dividing ℓ congruent to 3 modulo 4.

We also define n' as the greatest divisor of n prime to ℓ (recall that we are assuming ℓ to be square-free).

Proposition 3.7. *With the above assumptions, there exists an Arakelov-modular lattice of level ℓ and of trace type over $K = \mathbb{Q}(\zeta_n)$ if and only if the three following conditions are satisfied*:

(i) *ℓ divides n,*
(ii) *ℓ_1 and n' are good for n and*
(iii) *if ℓ_1 is even, 2 is a norm of $\mathbb{Q}(\zeta_{\frac{n}{4}})/\mathbb{Q}(\zeta_{\frac{n}{4}} + \zeta_{\frac{n}{4}}^{-1})$.*

This last proposition generalizes Propositions 5 and 6 of [4].

Proof. For a prime ideal $\mathfrak{P}$ in K, $v_{\mathfrak{P}}$ will denote the valuation at $\mathfrak{P}$. Let $(\mathcal{I}, 1)$ be an Arakelov-modular lattice of level ℓ of K. By Proposition 3.4, all the primes dividing ℓ ramify in $K/\mathbb{Q}$, so $\ell|n$. Take $\lambda \in K$ such that $(\mathcal{I}, 1) = (\lambda\mathcal{I}^*, (\lambda\bar{\lambda})^{-1}\ell)$. We can assume that $\lambda^2 = \varepsilon\ell$, with $\varepsilon \in \{\pm 1, \pm i\}$. Using the fact that $\mathcal{I}^* = \mathcal{D}_K^{-1}\overline{\mathcal{I}}^{-1}$, we find that $\lambda\mathcal{O}_K = \mathcal{D}_K\mathcal{I}\overline{\mathcal{I}}$. Let $\mathfrak{P}$ be a prime ideal of K dividing ℓ_1 and let p be the prime of $\mathbb{Z}$ under $\mathfrak{P}$. If p is odd, then $v_{\mathfrak{P}}(\lambda) = \frac{1}{2}v_{\mathfrak{P}}(\ell)$, but $p \equiv 1 \bmod 4$, hence $v_{\mathfrak{P}}(p) \equiv 0 \bmod 4$, and $v_{\mathfrak{P}}(\lambda) \equiv 0 \bmod 2$. In this case, $v_{\mathfrak{P}}(\mathcal{D}_K)$ is odd, and $v_{\mathfrak{P}}(\lambda\mathcal{D}_K^{-1})$ is also odd. If $p = 2$, then $n \equiv 4 \bmod 8$ and $v_{\mathfrak{P}}(\lambda) = 1$. Since $v_{\mathfrak{P}}(\mathcal{D}_K^{-1})$ is even, $v_{\mathfrak{P}}(\lambda\mathcal{D}_K^{-1})$ is also odd. If $\mathfrak{P}$ is a prime dividing n', then $v_{\mathfrak{P}}(\lambda) = 0$, and $v_{\mathfrak{P}}(\mathcal{D}_K)$ is odd (unless $\mathfrak{P}$ is above 2, but in this case 2 is a good divisor of n). So when $\mathfrak{P}$ is a prime ideal dividing $\ell_1 n'$, $v_{\mathfrak{P}}(\lambda\mathcal{D}_K^{-1})$ is odd. Hence we must have $v_{\mathfrak{P}}(\mathcal{I}) \neq v_{\mathfrak{P}}(\overline{\mathcal{I}})$, i.e. $\mathfrak{P} \neq \overline{\mathfrak{P}}$. This shows that $\ell_1 n'$ must be good for n and that 2 must be a norm of $\mathbb{Q}(\zeta_{\frac{n}{4}})/\mathbb{Q}(\zeta_{\frac{n}{4}} + \zeta_{\frac{n}{4}}^{-1})$ whenever $2|\ell$ and $n \equiv 4 \bmod 8$.

Conversely, finding an Arakelov-modular lattice of level ℓ and of trace type over K is equivalent to finding a decomposition $\lambda\mathcal{D}_K^{-1} = \mathcal{I}\overline{\mathcal{I}}$, where $\lambda^2 = \varepsilon\ell$ ($\varepsilon \in \{\pm 1, \pm i\}$). Such a decomposition is possible if and only if $v_{\mathfrak{P}}(\lambda\mathcal{D}_K^{-1})$ is even whenever $\mathfrak{P} = \overline{\mathfrak{P}}$. If possible, take a prime ideal $\mathfrak{P}$ such that $v_{\mathfrak{P}}(\lambda\mathcal{D}_K^{-1})$ is odd and $\mathfrak{P} = \overline{\mathfrak{P}}$. The hypothesis on ℓ and on $\ell_1 n'$ implies that $\mathfrak{P}$ divides n and $\mathfrak{P}$ does not divide $\ell_1 n'$. So $\mathfrak{P}$ must divide ℓ_2. Let p be a prime of $\mathbb{Z}$ under $\mathfrak{P}$, and assume first that p is odd. Then $p \equiv 3 \bmod 4$ and $v_{\mathfrak{P}}(\lambda) = \frac{1}{2} v_{\mathfrak{P}}(\ell)$ is odd. Moreover $v_{\mathfrak{P}}(\mathcal{D}_K^{-1})$ is also odd, and $v_{\mathfrak{P}}(\lambda\mathcal{D}_K^{-1})$ is even, which leads to a contradiction. Assume now that $p = 2$. In this case, $v_{\mathfrak{P}}(\lambda)$ is even because we are assuming that $8|n$, and $v_{\mathfrak{P}}(\mathcal{D}_K)^{-1}$ is also even, which contradicts the fact that $v_{\mathfrak{P}}(\lambda\mathcal{D}_K^{-1})$ is odd. This completes the proof. □

We can rewrite the preceding proposition in the following way. For an integer n and a prime number p, we define n_p to be the greatest integer dividing n prime to p, and we define $f_p = [\mathbb{Z}[\zeta_{n_p}]/\mathfrak{P} : \mathbb{Z}/p]$, where $\mathfrak{P}$ is any prime ideal of $\mathbb{Z}[\zeta_{n_p}]$ above p.

Proposition 3.8. *Let n be an integer and ℓ be a square-free integer dividing n. There exists an Arakelov-modular lattice of level ℓ and of trace type over $\mathbb{Q}(\zeta_n)$ if and only if the three following conditions are satisfied*:

(i) *for all $p|\ell$, $p \equiv 1 \bmod 4$, we have either f_p is odd or $p^{\frac{f_p}{2}} \not\equiv -1 \bmod n_p$,*

(ii) *for all $p|n$, $p \not|\ell$, we have either $p = 2$, or f_p is odd or $p^{\frac{f_p}{2}} \not\equiv -1 \bmod n_p$,*

(iii) *if ℓ is even and $n \equiv 4 \bmod 8$, then we have either f_2 is odd or $2^{\frac{f_2}{2}} \not\equiv -1 \bmod n_2$.*

In particular, we can apply the preceding proposition to the unimodular case, by taking $\ell = 1$.

Corollary 3.9. *There exists a unimodular lattice of trace type over $\mathbb{Q}(\zeta_n)$ if and only if for all $p|n$, we have either $p = 2$, or f_p is odd or $p^{\frac{f_p}{2}} \not\equiv -1 \bmod n_p$.*

Example 3.10. Let $K = \mathbb{Q}(\zeta_{21})$ be the cyclotomic field generated by a 21st root of unity. Let $\ell = 3$. With the notations of Proposition 3.7, we have $\ell_1 = 1$ and $n' = 7$. We see that $7 \equiv 1 \bmod 3$, so 7 is a good divisor of 21. Moreover, 1 is a good divisor of any integer. Hence according to Proposition 3.7 there exists an Arakelov-modular lattice of level 3 and of trace type over K which is 12-dimensional. A computation in PARI/GP shows that the Arakelov-modular lattice obtained in this way is of minimum 4, and is therefore extremal. Since the class number of K is one, this is the only Arakelov-modular lattice of level 3 in K (cf Proposition 4.2). This lattice is the Coxeter–Todd lattice because it is the only extremal 3-modular lattice in dimension 12. Note that this construction is given in [6].

Example 3.11. Let $K = \mathbb{Q}(\zeta_{28})$ be the cyclotomic field generated by a 28th root of unity. Let $\ell = 14$. 2 is a norm of $\mathbb{Q}(\zeta_7)/\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ and 7 is a good divisor of 28, so Proposition 3.7 gives us an Arakelov-modular lattice of level 14 and of trace type over K which is 12-dimensional. A computation in PARI/GP shows that this lattice is of minimum 8, therefore it is an extremal lattice. Since the class number of K is one, there is only one Arakelov-modular lattice of level 14 in K (cf Proposition 4.2). This lattice is the lattice $L_2(7) \times D_8$ given on p. 64 of [11].

Example 3.12. Let $K = \mathbb{Q}(\zeta_{40})$ be the cyclotomic field generated by a 40th root of unity and let $\ell = 2$. We can also apply Proposition 3.7 to get a 2-modular lattice of trace type over K which is 16-dimensional. A computation in PARI/GP shows that this lattice is of minimum 4, and is therefore an extremal lattice. Since the class number of K is one, there is only one Arakelov-modular lattice of level 2 in K (cf Proposition 4.2). This is the Barnes–Wall lattice BW_{16} (see Theorem 4 of [14]).

Proposition 3.7 gives the list of all cyclotomic fields in which there exists an Arakelov-modular lattice of trace type. We now want to give the list of all cyclotomic fields in which there exists an Arakelov-modular lattice. First of all, notice that Lemma 2 of [4] gives all the cyclotomic fields generated by a p^rth root of unity (with p prime) in which there exists an Arakelov-modular lattice (cf. Theorem 3.15). So consider a cyclotomic field K whose extension K/F is unramified at the finite primes. We have $K = \mathbb{Q}(\zeta_n)$, where n is odd or divisible by 4 and where n is not a prime power. Moreover, the maximal real subfield of K is $F = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ and K/F is unramified at the finite primes. For a divisor d of n, we define $\zeta_d = \zeta_n^{\frac{n}{d}}$. The different of $K/\mathbb{Q}$ is then

$$\mathcal{D}_K = n \prod_{p|n,\, p \text{ prime}} (1 - \zeta_p)^{-1} \mathcal{O}_K.$$

For a divisor d of n, define $\gamma_d \in F$ to be

$$\gamma_d = \begin{cases} (1-\zeta_d)(1-\zeta_n)^{-\frac{n}{d}} & \text{if } \frac{n}{d} \text{ is odd,} \\ (1-\zeta_d)(1-\zeta_n)^{-\frac{n}{d}} \zeta_n^{\frac{n}{4}} & \text{otherwise.} \end{cases}$$

We see that for a prime $p|n$, the ideal $(1-\zeta_p)\mathcal{O}_K$ comes from the ideal of F generated by γ_p, hence $\mathcal{D}_K = \mathcal{D}_F = n \prod_{p|n} \gamma_p^{-1} \mathcal{O}_K$. Denote ρ the homomorphism from $(\mathbb{Z}/n\mathbb{Z})^*$ to the embeddings of K into $\mathbb{R}$ defined by

$$\rho(k)(\zeta_n) = \exp\left(\frac{2ik\pi}{n}\right).$$

A straightforward computation gives

$$\rho(k)(\gamma_d) = \begin{cases} 2^{-\frac{n}{d}+1}(-1)^{\frac{3d-3n}{2d}} \sin\left(\frac{\pi k}{d}\right) \sin\left(\frac{\pi k}{n}\right)^{-\frac{n}{d}} & \text{if } \frac{n}{d} \text{ is odd,} \\ 2^{-\frac{n}{d}+1}(-1)^{\frac{kd+3d-3n}{2d}} \sin\left(\frac{\pi k}{d}\right) \sin\left(\frac{\pi k}{n}\right)^{-\frac{n}{d}} & \text{otherwise (for } d \neq 2). \end{cases} \tag{1}$$

Let ℓ be a square-free integer dividing n. Let $\lambda \in K$ be such that $\lambda^2 = \varepsilon\ell$, with $\varepsilon \in \{\pm 1, \pm i\}$. Define ℓ_1, ℓ_2 and n' as in Proposition 3.7. We will say that a prime $p|n$ is *bad* for (n, ℓ) if either $p|\ell_1 n'$ and p is not a good divisor of n, or ℓ_1 is even and 2 is not a norm of $\mathbb{Q}(\zeta_{\frac{n}{4}})/\mathbb{Q}(\zeta_{\frac{n}{4}} + \zeta_{\frac{n}{4}}^{-1})$. Denote $n_{\text{bad}} = \prod p^r$, where p goes through the bad prime divisors for (n, ℓ), and where n/n_{bad} is relatively prime to n_{bad}. According to Proposition 3.7, n_{bad} is the largest divisor of n which prevents the existence of an Arakelov-modular lattice of level ℓ and of trace type over $\mathbb{Q}(\zeta_n)$. However if we define δ to be

$$\delta = \begin{cases} \prod_{p \ \text{bad}} \gamma_p & \text{if } n_{\text{bad}} \text{ is odd,} \\ \gamma_4 \prod_{p \ \text{bad},\ p \neq 2} \gamma_p & \text{otherwise,} \end{cases}$$

then there exists an ideal $\mathcal{I}$ of $K = \mathbb{Q}(\zeta_n)$ such that $\lambda n_{\text{bad}} \delta^{-1} \mathcal{D}_K^{-1} = \mathcal{I}\overline{\mathcal{I}}$ (see the proof of Proposition 3.7). Therefore if we can find a unit u having the same signature as δ, there will exists an Arakelov-modular lattice of level ℓ over K. In fact, we have the following:

Proposition 3.13. *Write $\delta\mathcal{O}_F = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and $\lambda\mathcal{D}_K = \mathfrak{Q}_1^{a_1} \cdots \mathfrak{Q}_s^{a_s}$ (where the $\mathfrak{p}_i$'s are prime $\mathcal{O}_F$-ideals and the $\mathfrak{Q}_i$'s are prime $\mathcal{O}_K$-ideals). With the above notation, the following conditions are equivalent.*

(i) *There exists an Arakelov-modular lattice of level ℓ over $K = \mathbb{Q}(\zeta_n)$.*
(ii) $\sum e_i \equiv 0 \bmod 2$.
(iii) $\sum a_i \equiv 0 \bmod 2$.

Proof. The conditions (ii) and (iii) are equivalent because all the $\mathfrak{p}_j$'s dividing $\delta\mathcal{O}_F$ are inert in K/F and $\lambda\mathcal{D}_K^{-1} n_{\text{bad}} \mathcal{I}\overline{\mathcal{I}} = \delta\mathcal{O}_K$. So the equivalence follows from the fact that n_{bad} is a square in K an that $v_{\mathfrak{P}}(\mathcal{I}\overline{\mathcal{I}}) + v_{\overline{\mathfrak{P}}}(\mathcal{I}\overline{\mathcal{I}}) \equiv 0 \bmod 2$.

Assume now (i), and let $(\mathcal{J}, \alpha)$ be an Arakelov-modular lattice of level ℓ over K. Let $\lambda \in K$ be such that $\lambda^2 = \varepsilon\ell$, with $\varepsilon \in \{\pm 1, \pm i\}$. Using an argument similar to the proof of Proposition 3.7, we see that there exists an ideal $\mathcal{I}$ of K such that $n_{\text{bad}} \delta^{-1} \lambda \mathcal{D}_K^{-1} = \mathcal{I}\overline{\mathcal{I}}$. The lattice $(\mathcal{J}, \alpha)$ is Arakelov-modular so $\alpha^{-1}\lambda\mathcal{D}_K^{-1} = \mathcal{J}\overline{\mathcal{J}}$ (see Proposition 3.4). Let I_F denote the group of ideals of F. Let $\Psi_{K/F}$ be the Artin map:

$$\Psi_{K/F} : I_F \longrightarrow \mathbf{Gal}(K/F) = \{\pm 1\}, \qquad \mathfrak{p} \mapsto \begin{cases} -1 & \text{if } \mathfrak{p} \text{ is inert in } K/F, \\ 1 & \text{otherwise.} \end{cases}$$

The extension K/F is ramified at all the infinite primes, and unramified at the finite primes, so class field theory tells us that $\delta\mathcal{O}_F = \frac{1}{n_{\text{bad}}} \alpha \mathcal{J}\mathcal{I}^{-1} \overline{\mathcal{J}\mathcal{I}^{-1}} \cap \mathcal{O}_F$ is in the kernel of the Artin map $\Psi_{K/F}$. But by the definition of δ, for all the prime ideals $\mathfrak{p}$ dividing $\delta\mathcal{O}_F$, $v_{\mathfrak{p}}(\delta)$ is odd and $\mathfrak{p}$ is inert in the extension K/F. So there must be an even number of distinct prime ideals dividing δ, and condition (ii) holds.

Assume now (ii), so that $\delta\mathcal{O}_F$ is in the kernel of the Artin map. Using an argument similar to the proof of Proposition 3.7, we see that there exists an ideal $\mathcal{I}$ of K such that $n_{\text{bad}}\delta^{-1}\lambda\mathcal{D}_K^{-1} = \mathcal{I}\overline{\mathcal{I}}$. By class field theory, there exists a totally positive element $\alpha \in F$ and an ideal $\mathcal{J}$ of K such that $\delta\mathcal{O}_F = \alpha\mathcal{J}\overline{\mathcal{J}} \cap \mathcal{O}_F$ (in fact, no finite prime ramifies in K/F, hence $N_{K/F}(\mathcal{J}) = \mathcal{J}\overline{\mathcal{J}} \cap \mathcal{O}_F$ for all ideals $\mathcal{J}$ of K). Therefore, $n_{\text{bad}}\alpha^{-1}\lambda\mathcal{D}_K^{-1} = \mathcal{I}\mathcal{J}\overline{\mathcal{I}\mathcal{J}}$, and Proposition 4.1 tells us that the lattice $(\mathcal{I}\mathcal{J}, n_{\text{bad}}^{-1}\alpha)$ is an Arakelov-modular lattice of level ℓ. This completes the proof. □

We are now interested in giving a more comprehensible condition equivalent to the conditions of Proposition 3.13. Recall that we have

$$\mathcal{D}_K = n\prod_{p|n}\gamma_p^{-1}\mathcal{O}_K, \text{ and } \lambda = \begin{cases} u\prod_{p|\ell}\gamma_p^{\frac{p-1}{2}} & \text{if } \ell \text{ is odd,}\\ u\gamma_4\prod_{p|\ell,\ p\ \text{odd}}\gamma_p^{\frac{p-1}{2}} & \text{otherwise,}\end{cases} \tag{2}$$

for some unit $u \in \mathcal{O}_K$. Assume first that $n = p^r q^s$ where p, q are odd primes (this discussion also applies to the case $n = 4q^s$, where we must replace γ_p with γ_4). For a prime ideal $\mathfrak{P}$ of K, we have $v_{\mathfrak{P}}(\gamma_p) = p^{p^{r-1}}$ (resp. $v_{\mathfrak{P}}(\gamma_4) = 1$) is odd. So $\sum_{\mathfrak{P}|p} v_{\mathfrak{P}}(\gamma_p)$ has the parity of the number of distinct prime ideals dividing p. Hence our aim is to know the parity of the number of distinct prime ideals above p. In fact, it is also the parity of the number of prime ideals of $\mathbb{Q}(\zeta_q)$ above p. Therefore, we can assume that $s = 1$. Let $f_p = \min\{f : p^f \equiv 1 \bmod q\}$. The number of prime ideals in $\mathbb{Q}(\zeta_q)$ above p is $g_p = \frac{q-1}{f_p}$. Suppose that $\left(\frac{p}{q}\right) = 1$ ($\left(\frac{p}{q}\right)$ is the Legendre symbol of p and q). Then p is a square modulo q and $f_p | \frac{q-1}{2}$. So $g_p = \frac{q-1}{f_p} = 2 \cdot \frac{q-1}{2f_p}$ is even. Suppose now that $\left(\frac{p}{q}\right) = -1$. Using the fact that $(\mathbb{Z}/q)^\times$ is cyclic, we see that $g_p = \frac{q-1}{f_p}$ is odd. Therefore, for $n = p^r q^s$, we have

$$\sum_{\mathfrak{P}|p} v_{\mathfrak{P}}(\gamma_p) \equiv \begin{cases} 0 \bmod 2 & \text{if } \left(\frac{p}{q}\right) = 1,\\ 1 \bmod 2 & \text{if } \left(\frac{p}{q}\right) = -1,\end{cases} \tag{3}$$

where the sum is taken on the prime ideals of $\mathbb{Q}(\zeta_n)$ above p.

Assume now that $n = 2^r q^s$. For a prime ideal $\mathfrak{P}$ above 2, $v_{\mathfrak{P}}(\gamma_4)$ is odd if and only if r $= 2$, and $v_{\mathfrak{P}}(\gamma_2)$ is always even. If $r \geqslant 3$, the exponent of $(\mathbb{Z}/2^r)^\times$ is 2^{r-2}, hence $g_q = \frac{2^{r-1}}{f_q}$ is even. So $\sum_{\mathfrak{Q}|q} v_{\mathfrak{Q}}(\gamma_q)$ is even in this case. Now if $r = 2$, the number of prime ideals in $\mathbb{Q}(i)$ above q is even if and only if $q \equiv 1 \bmod 4$, and the number of prime ideals in $\mathbb{Q}(\zeta_{q^s})$ above 2 is even if and only if $\left(\frac{2}{q}\right) = 1$ (this is formula (3) for $p = 2$).

Finally, assume that at least three distinct primes divide n. Let p be a prime dividing n and write $n = p^r n_p$, where $(n_p, p) = 1$. Let $f_p = \min\{f : p^f \equiv 1 \bmod n_p\}$. It is easy to see that the exponent of $\left(\mathbb{Z}/n_p\right)^\times$ divides $\frac{\varphi(n_p)}{2}$, hence f_p divides $\frac{\varphi(n_p)}{2}$. So the number of distinct prime ideals of $\mathbb{Q}(\zeta_n)$ above p is $g_p = \frac{\varphi(n_p)}{f_p}$ and is even. Hence, if at least three distinct primes divide n, then for all prime $p|n$, we have

$$\sum_{\mathfrak{P}|p} v_{\mathfrak{P}}(\gamma_p) \equiv 0 \bmod 2,$$

where the sum is taken on the prime ideals of $\mathbb{Q}(\zeta_n)$ above p.

Proposition 3.13 can now be restated as follow:

Theorem 3.14. *Let n be an integer such that $n \not\equiv 2 \bmod 4$ and such that n is not a prime power, and let ℓ be a square-free integer. Then there exists an Arakelov-modular lattice of level ℓ over $\mathbb{Q}(\zeta_n)$ if and only if $\ell \in \mathrm{Modular}(n)$, where $\mathrm{Modular}(n)$ is defined as follow (in the sequel, p and q are odd primes).*

1. *If $n = 4q^s$, with $q \equiv 1 \bmod 8$, then $\mathrm{Modular}(n) = \{1, 2, q, 2q\}$.*
2. *If $n = 4q^s$, with $q \equiv 3 \bmod 8$, then $\mathrm{Modular}(n) = \{2, q\}$.*
3. *If $n = 4q^s$, with $q \equiv 5 \bmod 8$, then $\mathrm{Modular}(n) = \{1, q\}$.*
4. *If $n = 4q^s$, with $q \equiv 7 \bmod 8$, then $\mathrm{Modular}(n) = \{q, 2q\}$.*
5. *If $n = 2^r q^s$ with $r \geqslant 3$, then $\mathrm{Modular}(n) = \{1, 2, q, 2q\}$.*
6. *If $n = p^r q^s$, with $p \equiv q \equiv 1 \bmod 4$, then $\mathrm{Modular}(n) = \{1, p, q, pq\}$.*
7. *If $n = p^r q^s$, with $p \equiv 1 \bmod 4$, $q \equiv 3 \bmod 4$ and $\left(\frac{p}{q}\right) = 1$, then $\mathrm{Modular}(n) = \{1, p, q, pq\}$.*
8. *If $n = p^r q^s$, with $p \equiv 1 \bmod 4$, $q \equiv 3 \bmod 4$ and $\left(\frac{p}{q}\right) = -1$, then $\mathrm{Modular}(n) = \{1, p\}$.*
9. *If $n = p^r q^s$, with $p \equiv q \equiv 3 \bmod 4$ and $\left(\frac{p}{q}\right) = 1$, then $\mathrm{Modular}(n) = \{q, pq\}$.*
10. *If at least three distinct primes divide n, then $\mathrm{Modular}(n)$ consists of all the square-free divisors of n.*

Proof. This proposition follows from formula (2) and from the discussion about the parity of the number of distinct prime ideals in $\mathbb{Q}(\zeta_n)$ above a given prime number $p|n$. □

In order to be complete, we will restate here the results corresponding to the prime power case which can be found in [4], Lemma 2.

Theorem 3.15. *Let $n = p^r$ be a prime power. Let ℓ be a square-free integer. Then there exists an Arakelov-modular lattice of level ℓ over $\mathbb{Q}(\zeta_n)$ if and only if $\ell \in \mathrm{Modular}(n)$, where $\mathrm{Modular}(n)$ is defined as follows:*

1. *If $p \equiv 1 \bmod 4$, then $\mathrm{Modular}(n) = \emptyset$.*
2. *If $p \equiv 3 \bmod 4$, then $\mathrm{Modular}(n) = \{p\}$.*
3. *If $n = 4$, then $\mathrm{Modular}(n) = \{1\}$.*
4. *If $n = 2^r$, $r \geqslant 3$, then $\mathrm{Modular}(n) = \{1, 2\}$.*

Proof. In [4], Lemma 2, the point 1 is already shown. In [4], Proposition 1, an Arakelov-modular lattice of level p (denoted $\mathcal{L}^p_{p^r}$) is exhibited in the field $\mathbb{Q}(\zeta_{p^r})$ for $p \equiv 3 \bmod 4$ and for $p = 2, r \geqslant 3$. Moreover, in $\mathbb{Q}(\zeta_{2^r})$, an unimodular lattice can be constructed because the different of $\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}$ is a square. Therefore it remains to prove that no unimodular lattice can be constructed over $\mathbb{Q}(\zeta_{p^r})$ for $p \equiv 3 \bmod 4$, and that there are no 2-modular lattices over $\mathbb{Q}(i)$.

This can be shown as in [4], Lemma 2. If $L = (\mathcal{I}, \alpha)$ is an ideal lattice over $\mathbb{Q}(\zeta_{p^r})$, then $\det(L) = N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\alpha\mathcal{I}^2)\mathrm{disc}_{\mathbb{Q}(\zeta_{p^r})}$. $N(\alpha)$ is a square (because α is totally real) and $\mathrm{disc}_{\mathbb{Q}(\zeta_{p^r})}$ is a square in the case $p^r = 4$ (resp. is not a square in the case $p \equiv 3 \bmod 4$. Therefore we can not have $\det(L) = 2$ (resp. $\det(L) = 1$) in the case $p^r = 4$ (resp. $p \equiv 3 \bmod 4$). This concludes the proof. □

If we apply Theorem 3.14 to $\ell = 1$, we find as a particular case Theorem 1.1,I,c) of [2], namely:

Corollary 3.16. *Assume that n is not a power of 2. Then there exists an unimodular lattice over $\mathbb{Q}(\zeta_n)$ if and only if at least two primes divide n and $\varphi(n)$ is divisible by 8.*

The three following examples will illustrate Theorem 3.14.

Example 3.17. Let $K = \mathbb{Q}(\zeta_{15})$ be the cyclotomic field generated by a 15th root of unity. Theorem 3.14, 8 tells us that there exists an Arakelov-modular lattice of level 5 over K. The different of $K/\mathbb{Q}$ is $\mathcal{D}_K = 15\delta^{-1}\mathcal{O}_K$, where $\delta = \gamma_3\gamma_5$ is defined as before (in this case, both 3 and 5 are bad for $(15, 5)$). We check that $5 = \lambda^2$, with $\lambda\mathcal{O}_K = \gamma_5^2\mathcal{O}_K$. Hence $15\lambda\delta^{-1}\mathcal{D}_K^{-1} = \gamma_5\overline{\gamma_5}\mathcal{O}_K$.

The sign of $\rho(k)(\delta)$ is the sign of $-\sin\left(\frac{\pi k}{3}\right)\sin\left(\frac{\pi k}{5}\right)$ for $0 < k < 15$. Apply the results of Section 4 of [2] (or use PARI/GP) to obtain a unit $u = -\frac{\zeta_{15}^2-\zeta_{15}^{-2}}{\zeta_{15}-\zeta_{15}^{-1}}$ such that the sign of $\rho(k)(u)$ is the sign of $\rho(k)(\delta)$ for all $0 < k < 8$, $\gcd(k, 15) = 1$. Finally, we get an Arakelov-modular lattice $(\mathcal{I}, \alpha)$ of level 5, where $\alpha = \frac{1}{15}u\delta$ and $\mathcal{I} = \gamma_5\mathcal{O}_K$. This is the only Arakelov-modular lattice of level 5 over K since $h_K = 1$ (see Proposition 4.2). A computation in PARI/GP tells us that this lattice is of minimum 4, and is therefore an extremal lattice. This lattice is the same lattice as the one constructed on p.16 of [17].

Example 3.18. Let $K = \mathbb{Q}(\zeta_{35})$ be the cyclotomic field generated by a 35th root of unity. Theorem 3.14, 8 tells us that there exists an Arakelov-modular lattice of level 5 over K. Both 5 and 7 are bad for $(35, 5)$, so the different of $K/\mathbb{Q}$ is $\mathcal{D}_K = 35\delta^{-1}\mathcal{O}_K$, where $\delta = \gamma_7\gamma_5$ is defined as before.

The sign of $\rho(k)(\delta)$ is the sign of $-\sin\left(\frac{\pi k}{5}\right)\sin\left(\frac{\pi k}{7}\right)$ for $0 < k < 35$. We can use the results of [2] to find a unit

$$u = -\frac{\zeta^3 - \zeta^{-3}}{\zeta - \zeta^{-1}}\,\frac{\zeta^9 - \zeta^{-9}}{\zeta - \zeta^{-1}}\,\frac{\zeta^{11} - \zeta^{-11}}{\zeta - \zeta^{-1}}\,\frac{\zeta^{12} - \zeta^{-12}}{\zeta - \zeta^{-1}}\,\frac{\zeta^{13} - \zeta^{-13}}{\zeta - \zeta^{-1}}$$

having the same signature as δ. Therefore we get an Arakelov-modular lattice $(\mathcal{I}, \alpha)$ of level 5, with $\alpha = \frac{1}{35}u\delta$ and $\mathcal{I} = \gamma_5\mathcal{O}_K$. The class number of K is $h_K = 1$, so there is exactly one Arakelov-modular lattice of level 5 over K (see Proposition 4.2). A computation under PARI/GP tells us that this ideal lattice is of minimum 8, and is therefore extremal. This lattice is the one given in p. 23 of [17].

Using the notation of Proposition 3.14, let P_F^+ be the set of ideals of F generated by totally positive elements and let $\mathrm{cl}^+(F) = I_F/P_F^+$ be the narrow class group of F. Let $\mathrm{cl}(K) = I_K/P_K$ be the class group of K. We have a map

$$\mathrm{cl}(K) \to \mathrm{cl}^+(F), \qquad \mathrm{cl}(\mathcal{I}) \mapsto \mathrm{cl}(\delta N_{K/F}(\mathcal{I})).$$

Proposition 3.13 tells us when the trivial class of $\mathrm{cl}^+(F)$ is in the image of this map.

Example 3.19. Let $K = \mathbb{Q}(\zeta_{56})$ be the cyclotomic field generated by a 56th root of unity. Theorem 3.14, 5 tells us that there exists an Arakelov-modular lattice of level 2 over K. As 7 is bad for $(56, 2)$, the different of $K/\mathbb{Q}$ is $\mathcal{D}_K = 7\delta^{-1}(\mathfrak{Q}\overline{\mathfrak{Q}})^8\mathcal{O}_K$, where $\delta = \gamma_7$ is defined as before, and $\mathfrak{Q}$ is a prime ideal of $\mathcal{O}_K$ above 2.

According to PARI/GP, there are no units of K having the same signature as δ. However, we know that the trivial class of $\mathrm{cl}^+(F)$ is in the image of the map defined above this example. The class group of K is of order 2 and is generated by $\mathfrak{Q}$, therefore the ideal $\gamma_7\mathfrak{Q}\overline{\mathfrak{Q}}$ must be generated by a totally positive element. In fact, this ideal is generated by the totally real element $\gamma_7\gamma_8$, whose signature is given by formula (1), so all that remains is to find a suitable unit. This can be done using PARI/GP. In this way, we find a 2-modular lattice of dimension 24 and of minimum 4.

4. Classification results

Given a CM field K and an Arakelov-modular lattice over K, this section deals with the problem of classifying all Arakelov-modular lattices which can be constructed over K. As we will see, this is possible under the hypothesis that at most one finite prime of F ramifies in K. Note that this is always the case for cyclotomic fields.

First, we assume that there exists an Arakelov-modular lattice of level ℓ and of trace type over K. If the extension K/F is ramified on at most one finite prime, then all Arakelov-modular lattices of level ℓ over K are Arakelov-equivalent to a lattice of trace type. This is the aim of the next Proposition:

Proposition 4.1. *Assume that there is an Arakelov-modular lattice of level ℓ and of trace type $(\mathcal{I}, 1)$ in K and also assume K/F is ramified on at most one finite prime. Let $(\mathcal{J}, \alpha)$ be an Arakelov-modular lattice of level ℓ. Then there exists an ideal $\mathcal{K}$ of K such that $(\mathcal{J}, \alpha) \cong_A (\mathcal{K}, 1)$.*

Proof. Assume first that no finite prime ramifies in the extension K/F. Let $\lambda \in K$ such that $\lambda\mathcal{I}^* = \mathcal{I}$ and $\lambda\mathcal{J}^* = \mathcal{J}$ (see Proposition 3.4). The first equality implies that

$\mathcal{I}\overline{\mathcal{I}} = \lambda\mathcal{D}_K^{-1}$, and the second one that $\alpha\mathcal{J}\overline{\mathcal{J}} = \lambda\mathcal{D}_K^{-1}$. Therefore we have

$$\alpha\mathcal{O}_K = (\mathcal{J}\overline{\mathcal{J}})^{-1}\mathcal{I}\overline{\mathcal{I}}. \tag{4}$$

We can now check that α is a local norm of K/F at each prime, to deduce via the Hasse norm Theorem that α is a global norm. Note that α is certainly a local norm at each infinite prime since α is totally positive. Let $\mathfrak{P}$ be a finite prime of K. $K_{\mathfrak{P}}/F_{\mathfrak{P}}$ is unramified, so if α is a unit at $\mathfrak{P}$, α is a norm of $K_{\mathfrak{P}}/F_{\mathfrak{P}}$. If α is not a unit at $\mathfrak{P}$, equality (4) tells us that $v_{\mathfrak{P}}(\alpha)$ is even whenever $\mathfrak{P} = \overline{\mathfrak{P}}$ (i.e. whenever $K_{\mathfrak{P}} \neq F_{\mathfrak{P}}$), so α is also a norm at $\mathfrak{P}$. Hence there exists $\delta \in K$ such that $\alpha = \delta\overline{\delta}$. The ideal $\mathcal{K} = \delta\mathcal{J}$ gives rise to an ideal lattice of trace type such that $(\mathcal{K}, 1) \cong_A (\mathcal{J}, \alpha)$. This completes the case in which K/F is unramified at the finite primes.

If only one finite prime $\mathfrak{Q}$ ramifies in K/F, a similar proof will work if we show that α is also a local norm at $\mathfrak{Q}$, and this is given by the Hilbert reciprocity law. □

Suppose that at most one finite prime of F ramifies in K. If moreover there exists an Arakelov-modular lattice of level ℓ over K, then we can explicitly describe all Arakelov-modular lattice of level ℓ which can be constructed over K. This is the purpose of the next proposition.

In order to state the next proposition, we introduce $\mathrm{cl}(K)$ the ideal class group of K, and we denote $\mathrm{cl}(K)^\tau$ the set of classes of $\mathrm{cl}(K)$ which contain an ideal fixed by $\mathbf{Gal}(K/F)$. If $\mathcal{J}$ is an ideal of K, we write $[\mathcal{J}]$ for its class in the ideal class group of K.

Let $\mathrm{AM}_K(\ell)$ be the set of classes of Arakelov-modular lattices of level ℓ over K modulo Arakelov-equivalence (cf Definition 1.2). The class of an ideal lattice $(\mathcal{I}, \alpha)$ in $\mathrm{AM}_K(\ell)$ is denoted by $[\mathcal{I}, \alpha]$. Assume $\mathrm{AM}_K(\ell) \neq \emptyset$ and choose $[\mathcal{I}, \alpha] \in \mathrm{AM}_K(\ell)$. Let Φ be the map

$$\Phi : \mathrm{cl}(K)/\mathrm{cl}(K)^\tau \to \mathrm{AM}_K(\ell), \qquad [\mathcal{J}] \mapsto [\mathcal{I}\mathcal{J}\overline{\mathcal{J}}^{-1}, \alpha].$$

Proposition 4.2. *With the above assumptions, Φ is bijective.*

Proof. We first introduce a notation : for $\gamma \in K$, and for an ideal lattice $(\mathcal{J}, \beta)$, we define $\gamma \cdot (\mathcal{J}, \beta) = (\gamma\mathcal{J}, (\gamma\overline{\gamma})^{-1}\beta)$. Recall that the lattices $(\mathcal{J}, \beta)$ and $\gamma \cdot (\mathcal{J}, \beta)$ are isometric.

First of all, define $\tilde{\Phi} : \mathrm{cl}(K) \to \mathrm{AM}_K(\ell)$ as above. If $\mathcal{J} = \beta\mathcal{O}_K$ is a principal ideal, then $(\mathcal{I}\mathcal{J}\overline{\mathcal{J}}^{-1}, \alpha) = (\beta/\overline{\beta}) \cdot (\mathcal{I}, \alpha)$, so $\tilde{\Phi}$ is well defined. Let $(\tilde{\mathcal{I}}, \tilde{\alpha})$ be an Arakelov-modular lattice of level ℓ over K. Let $\lambda \in \mathcal{O}_K$ such that $\lambda\mathcal{I}^* = \mathcal{I}$ and $\lambda\tilde{\mathcal{I}}^* = \tilde{\mathcal{I}}$ (see Proposition 3.4). A similar argument to the one used in the proof of Proposition 4.1 gives that $\tilde{\alpha} \in N_{K/F}(K)\alpha$. Hence by replacing $(\tilde{\mathcal{I}}, \tilde{\alpha})$ by $\gamma \cdot (\tilde{\mathcal{I}}, \tilde{\alpha})$, where $\tilde{\alpha} = \gamma\overline{\gamma}\alpha$, we can reduce the problem to the case $\alpha = \tilde{\alpha}$. We can now deduce that $\mathcal{I}\overline{\mathcal{I}} = \lambda\alpha^{-1}\mathcal{D}_K^{-1} = \tilde{\mathcal{I}}\overline{\tilde{\mathcal{I}}}$. Thus there exists an ideal $\mathcal{J}$ over K such that $\tilde{\mathcal{I}} = \mathcal{J}\overline{\mathcal{J}}^{-1}\mathcal{I}$. This proves that the map $\tilde{\Phi}$ is surjective.

Consider now $[\mathcal{J}] \in \ker \tilde{\Phi}$. We have $[\mathcal{I}\mathcal{J}\overline{\mathcal{J}}^{-1}, \alpha] = [\mathcal{I}, \alpha]$, so the ideal $\mathcal{J}\overline{\mathcal{J}}^{-1}$ is generated by an element $\beta \in K$ such that $\beta\overline{\beta} = 1$. We can now apply Hilbert's Theorem 90 to obtain an element $\gamma \in K$ such that $\gamma\mathcal{J} = \overline{\gamma\mathcal{J}}$. This last equality gives that $[\mathcal{J}]$ is in $\mathrm{cl}(K)^{\tau}$, and concludes then the proof. □

Thanks to Theorem 3.14, Proposition 4.2 can be applied to the case when K is a cyclotomic field. This is shown in the two following examples.

Example 4.3. Let $K = \mathbb{Q}(\zeta_{56})$ be the cyclotomic field generated by a 56th root of unity. Let $\ell = 7$ and apply Theorem 3.14, 5 to get an Arakelov-modular lattice of trace type and of level 7 over K. The class number of K is 2, so Proposition 4.2 tells us there are at most two Arakelov-modular lattices of level 7 over K. In fact, a computation in PARI/GP gives two Arakelov-modular lattices of level 7 over K, one of minimum 4 and the other of minimum 8. Neither of them is extremal.

Example 4.4. Let $K = \mathbb{Q}(\zeta_{80})$ be the cyclotomic field generated by a 80th root of unity. Let $\ell = 2$ and apply Theorem 3.14, 5 to get an Arakelov-modular lattice of trace type and of level 2 over K. The class number of K is 5, so Proposition 4.2 tells us there are at most five Arakelov-modular lattices of level 2 over K. In fact, a computation in PARI/GP gives two Arakelov-modular lattices of level 2 over K, one of minimum 4 and the other of minimum 6, the second one is therefore extremal. A computation with the Bernd Souvignier isometry program (see [12]) gives that this lattice is isomorphic to the lattice Q_{32}.

5. Action of the Galois group: examples

In this section, we primarily give some examples for the case in which the similarity is induced by the Galois group of $K/\mathbb{Q}$.

Assume that K is a CM-field and $K/\mathbb{Q}$ is Galois. Let ℓ be an integer (not assumed to be square-free). For any $\sigma \in \mathbf{Gal}(K/\mathbb{Q})$, the map $x \mapsto x^{\sigma}$ is an isometry from the ideal lattice $(\mathcal{I}, \alpha)$ to $(\mathcal{I}^{\sigma}, \alpha^{\sigma})$. Hence an ideal lattice $(\mathcal{I}, \alpha)$ whose class $[\mathcal{I}, \alpha]$ belongs to the same $\mathbf{Gal}(K/\mathbb{Q})$-orbit as $[\mathcal{I}^{*}, \ell\alpha]$ is ℓ-modular.

Proposition 5.1. *There exists an ideal lattice of trace type $(\mathcal{I}, 1)$ whose class $[\mathcal{I}, 1]$ belongs to the same* $\mathbf{Gal}(K/\mathbb{Q})$*-orbit as $[\mathcal{I}^{*}, \ell]$ if and only if there exists an ideal $\mathfrak{a}$ of K, a $\lambda \in K$ and an automorphism $\sigma \in$* $\mathbf{Gal}(K/\mathbb{Q})$ *such that $\ell = \lambda\overline{\lambda}$, $\lambda\mathfrak{a}^{\sigma} \subseteq \mathfrak{a}$ and $\lambda\mathcal{D}_K^{-1} = \mathfrak{a}\overline{\mathfrak{a}}^{\sigma}$.*

Proof. If $[\mathcal{I}, 1] = [(\mathcal{I}^{*})^{\sigma}, \ell^{\sigma}]$, take $\lambda \in K$ such that $(\mathcal{I}, 1) = (\lambda(\mathcal{I}^{*})^{\sigma}, \lambda\overline{\lambda}\ell^{\sigma})$. Then we get $\ell = \lambda\overline{\lambda}$ and $\lambda(\mathcal{I}^{*})^{\sigma} = \mathcal{I}$. We can now conclude using the identity $(\mathcal{I}^{*})^{\sigma} = (\mathcal{D}_K^{-1}\overline{\mathcal{I}}^{-1})^{\sigma} = \mathcal{D}_K^{-1}\overline{\mathcal{I}}^{-\sigma}$. Conversely, a straightforward computation gives us that $[\mathfrak{a}, 1] = [(\mathfrak{a}^{*})^{\sigma}, \ell]$, i.e. the lattice $(\mathfrak{a}, 1)$ is ℓ-modular. □

In fact, in the case of Proposition 5.1, ℓ need not be ramified in $K/\mathbb{Q}$ so that Proposition 3.4 is not true for such ideal lattices. The following two examples illustrate this fact.

Example 5.2. Let K be the cyclotomic field generated by a 40th root of unity. There exists prime ideals $\mathfrak{P}, \mathfrak{Q}$ of K and there exists an automorphism $\sigma \in \mathbf{Gal}(K/\mathbb{Q})$ such that $3\mathcal{O}_K = \mathfrak{P}\mathfrak{P}^\sigma\overline{\mathfrak{P}\mathfrak{P}^\sigma}$, $5\mathcal{O}_K = (\mathfrak{Q}\overline{\mathfrak{Q}})^4$. The different of $K/\mathbb{Q}$ is $\mathcal{D}_K = 4(\mathfrak{Q}\overline{\mathfrak{Q}})^3$. We want to construct a modular lattice of level 15 over K. If such a lattice exists, Proposition 3.7 tells us that this lattice would not be Arakelov-modular over K. Since K has class number 1, there exists $\lambda_3 \in K$ such that $\lambda_3\mathcal{O}_K = \mathfrak{P}\overline{\mathfrak{P}^\sigma}$. We have $\lambda_3\overline{\lambda_3} = 3u$, where u is a totally positive unit of K. By Proposition A.2 of [19], $u = v\overline{v}$ where v is a unit of K. Hence we can assume that $\lambda_3\overline{\lambda_3} = 3$. Define $\lambda = \lambda_3\sqrt{5}$, so that $\lambda\mathcal{O}_K = \mathfrak{P}\overline{\mathfrak{P}^\sigma}(\mathfrak{Q}\overline{\mathfrak{Q}})^2$. We can assume that $\mathfrak{Q}^\sigma = \mathfrak{Q}$ (by composing if necessary σ with an element of $\mathfrak{D}_{\mathfrak{P}} - \mathfrak{D}_{\mathfrak{Q}}$, for instance $\zeta_{40} \mapsto \zeta_{40}^3$). Hence $\lambda\mathcal{D}_K^{-1} = \mathfrak{P}\overline{\mathfrak{P}}^\sigma 4^{-1}(\mathfrak{Q}\overline{\mathfrak{Q}})^{-1} = \mathcal{I}\overline{\mathcal{I}}^\sigma$, where $\mathcal{I} = \mathfrak{P}2^{-1}\mathfrak{Q}^{-1}$. Proposition 5.1 gives the existence of a 15-modular ideal lattice. A computation under PARI/GP tells us that this lattice is of minimum 10, and is therefore extremal. A computation with the Bernd Souvignier isometry program (see [12]) gives that this lattice is isomorphic to the lattice $[SL_2(5)\ Y\ SL_2(9)]$ given in Theorem IV.1 of [9] (the Gram matrix can be found in [9], p.142).

Example 5.3. Let K be the cyclotomic field generated by a 40^{th} root of unity. We want to construct a 7-modular lattice over K. We have $\mathcal{D}_K = 4(\mathfrak{Q}\overline{\mathfrak{Q}})^3$ and $7\mathcal{O}_K = \mathfrak{P}\overline{\mathfrak{P}}\mathfrak{P}^\sigma\overline{\mathfrak{P}}^\sigma$, where $\mathfrak{P}, \mathfrak{Q}$ are prime ideals of K and $5\mathcal{O}_K = (\mathfrak{Q}\overline{\mathfrak{Q}})^4$. We can assume that $\mathfrak{Q}^\sigma = \mathfrak{Q}$ (by composing if necessary σ with $\zeta_{40} \mapsto \zeta_{40}^7$, which is an element of $\mathfrak{D}_{\mathfrak{P}} - \mathfrak{D}_{\mathfrak{Q}}$). Let λ be a generator of $\mathfrak{P}\overline{\mathfrak{P}^\sigma}$ (K is principal). By Proposition A.2 of [19], all totally positive units of F are in $N_{K/F}(U_K)$, where U_K is the group of units of $\mathcal{O}_K$. Therefore we can assume that $\lambda\overline{\lambda} = 7$. Let $\mathcal{I} = \frac{1}{2}\mathfrak{P}\mathfrak{Q}^{-3}$, and apply Proposition 5.1 to get a 7-modular ideal lattice over K. This lattice cannot be Arakelov-modular over any cyclotomic field because 7 does not ramify in any cyclotomic field of dimension 16 over $\mathbb{Q}$. A computation in PARI/GP tells us that this lattice is of minimum 6, and is therefore extremal. This lattice is the same lattice as the one exhibited in [17, p. 21].

References

[1] C. Batut, H.-G. Quebbemann, R. Scharlau, Computations of cyclotomic lattices, Exposition Math. 4 (1995) 175–179.

[2] E. Bayer-Fluckiger, Definite unimodular lattices having an automorphism of given characteristic polynomial, Comment. Math. Hely. 59 (1984) 509–538.

[3] E. Bayer-Fluckiger, Lattices and number fields, Contemp. Math. 241 (1999) 69–84.

[4] E. Bayer-Fluckiger, Cyclotomic modular lattices, J. Théorie Nombres Bordeaux 12 (2000) 273–280.

[5] E. Bayer-Fluckiger, Ideal lattices, in: G. Wustholz (Ed.), A Panorama of Number Theory or The View from Baker's Garden, Cambridge University Press, Cambridge, 2002, pp. 168–184.

[6] E. Bayer-Fluckiger, J. Martinet, Formes quadratiques liées aux algèbres semi-simples, J. Reine Angew. Math. 451 (1994) 51–69.

[8] G. Nebe, Gitter und Modulformen, Jahresber. Deutsch. Math.-Verein. 104 (3) (2002) 125–144.

[9] G. Nebe, W. Plesken, Finite rational matrix groups of degree 16, Mem. Am. Math. Soc. 116 (1995) 74–144.

[10] O.T. O'Meara, Introduction to Quadratic Forms, Springer, Berlin, 1963.

[11] W. Plesken, G. Nebe, Finite Rational Matrix Groups, Mem. Amer. Math. Soc. 116 (1995) 1–73.

[12] W. Plesken, B. Souvignier, Computing isometries of lattices, J. Symbolic Comput. 24 (1997) 327–334.

[14] H.-G. Quebbemann, Modular lattices in Euclidean spaces, J. Number Theory 54 (1995) 190–202.

[15] H.-G. Quebbemann, Atkin–Lehner eigenforms and strongly modular lattices, L'Enseigne. Math. 43 (1997) 55–65.

[16] H.-G. Quebbemann, A shadow identity and an application to isoduality, Abhandlungen Math. Sem. Univ. Hamburg 68 (1998) 339–345.

[17] R. Scharlau, R. Schulze-Pillot, Extremal lattices, in: B.H. Matzat (Ed.), Algorithmic Algebra and Number Theory, Selected Papers from a Conference, Heidelberg, Germany, October 1997, Springer, Berlin, 1999, pp. 139–170.

[18] R. Schoof, Computing Arakelov class groups, preprint.

[19] G. Shimura, On abelian varieties with complex multiplication, Proc. London Math. Soc. Ser. III. 34 (1977) 65–86.