MODULAR LATTICES OVER CM FIELDS

IVAN SUAREZ

Abstract. We study some properties of Arakelov-modular lattices, which are particular modular ideal lattices over CM fields. There are two main results in this paper. The first one is the determination of the number of Arakelov-modular lattices of fixed level over a given CM field provided that an Arakelov-modular lattice is already known. This number depends on the class numbers of the CM field and its maximal totally real subfield. This first part gives also a way to compute all these Arakelov-modular lattices. In the second part, we describe the levels that can occur for some multiquadratic CM number fields.

Introduction

This paper deals with ideal lattices over CM fields. A lattice is a free $\mathbb{Z}$-module of finite type, together with a positive definite symmetric bilineare form. In 1995, Quebbemann introduced the notion of modular lattice, i.e. a lattice which is similar to its dual (see [7] and [8]).The idea here is to combine this notion with the notion of ideal lattice, which is a lattice arising from a number field with a trace construction (see §1, and [3], [2]). This led to the introduction of Arakelov-modular lattices in [4]. In [4], we were mainly interested in Arakelov-modular lattices over cyclotomic fields. The purpose of this paper is to investigate the more general case of CM fields, and to give explicit results over multiquadratic fields.

After giving some definitions in Section 1, Section 2 is devoted to strongly Arakelov-modular lattices. In section 3, there are given the action of two groups (one of them being the class group) on the set of Arakelov-modular lattices of a given level which turn out to be transitive. Section 4 deals with the problem of finding Arakelov-modular lattices over multiquadratic fields.

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 type and $b : L_{\mathbb{R}} \times L_{\mathbb{R}} \to \mathbb{R}$ is a definite positive symmetric bilinear form on $L_{\mathbb{R}} := L \otimes_{\mathbb{Z}} \mathbb{R}$.

The *dual lattice* of the lattice (L, b) is the lattice (L^*, b), where

$$L^* = \{u \in L_{\mathbb{R}} \ : \ b(u, L) \subset \mathbb{Z}\}.$$

A lattice (L, b) is said to be *integral* if $L \subset L^*$. If moreover $b(u, u) \in 2\mathbb{Z}$ for each $u \in L$, then the lattice is said to be *even*.

Key words and phrases. Modular Lattices; CM Fields; Multiquadratic Fields.
The author gratefully acknowledge support from the Swiss National Science Fundation, grant No 200020-111814/1.
isuarez@univ-lemans.fr, EPFL, Lausanne, Switzerland.
2000 ***Mathematical Subject Classification.*** – 11R20, 11H06 .

Let L be an integral lattice. The *level* of the lattice L is the exponant of the group L^*/L. The level of a lattice is therefore the smallest integer ℓ such that the rescaled lattice $(L^*, \ell b)$ is integral.

Definition 1.1 (see [7])**.** A lattice (L, b) is said to be *modular* if

- (L, b) is even,
- $(L, b) \cong (L^*, \ell b)$, where ℓ is the level of the lattice.

Definition 1.2 (see [8])**.** Let (L, b) be a modular lattice of level ℓ. Define for each exact divisor $m||\ell$ (i.e. $m|\ell$ and $\gcd(m, \ell/m) = 1$) the lattice $L_m := \left(\frac{1}{m}L\right) \cap L^*$. Then the lattice (L, b) is said to be *strongly modular* if for each $m||\ell$, the two lattices (L_m, mb) and (L, b) are isometric.

1.2. **Ideal lattices.** (see also [3] and [2])

Let K be a CM-field, and let F be the maximal totally real subfield of K. Denote by $x \mapsto \overline{x}$ the complex conjugation. Recall that K is totally complex and that F is the fixed field by the conjugation (so we have $[K : F] = 2$).

Definition 1.3. An *ideal lattice* over K is a lattice $(\mathcal{I}, b)$, where

(i) $\mathcal{I}$ is a fractionnal ideal of K and
(ii) there exists a totally positive element $\alpha \in F$ such that $b(x, y) = \mathbf{Tr}_{K/\mathbb{Q}}(\alpha x\overline{y})$ for all $x, y \in \mathcal{I}$.

Notation: The ideal lattice $(\mathcal{I}, b)$ with $b(x, y) = \mathbf{Tr}(\alpha x\overline{y})$ will be denoted $(\mathcal{I}, \alpha)$.

Let $\mathcal{D}_K$ denote the different of $K/\mathbb{Q}$. If $(\mathcal{I}, \alpha)$ is an ideal lattice over K, its dual lattice is also an ideal lattice $(\mathcal{I}^*, \alpha)$ over K, where

$$\mathcal{I}^* = \alpha^{-1}\mathcal{D}_K^{-1}\overline{\mathcal{I}}^{-1}.$$

Let $(\mathcal{I}, \alpha)$ be an ideal lattice (over K). For each $\beta \in K^\times$, the multiplication by β induces an isometry between the ideal lattices $(\mathcal{I}, \alpha)$ and $\left(\beta\mathcal{I}, (\beta\overline{\beta})^{-1}\alpha\right)$. Two such ideal lattices are called *Arakelov-equivalent* (notation : $(\mathcal{I}, \alpha) \cong_A \left(\beta\mathcal{I}, (\beta\overline{\beta})^{-1}\alpha\right)$).

Definition 1.4. An even ideal lattice $(\mathcal{I}, \alpha)$ of level ℓ is said to be *Arakelov-modular* if the ideal lattices $(\mathcal{I}, \alpha)$ and $(\mathcal{I}^*, \ell\alpha)$ are Arakelov-equivalent.
An even ideal lattice $(\mathcal{I}, \alpha)$ of level ℓ is said to be *strongly Arakelov-modular* if for each $m||\ell$,

$$(\mathcal{I}_m, m\alpha) \cong_A (\mathcal{I}, \alpha).$$

2. Some properties of modular lattices

We keep in this section the notation of §1.2.

In [4], §3, it is shown that the existence of an Arakelov-modular lattice of level ℓ on K is equivalent to the existence of a totally positive element $\alpha \in F$, an ideal $\mathcal{I}$ and an element $\lambda \in K$ such that :

(i) $\lambda\overline{\lambda} = \ell$, and
(ii) $\alpha\mathcal{I}\overline{\mathcal{I}} = \lambda\mathcal{D}_K^{-1}$ (which is equivalent to $\lambda\mathcal{I}^* = \mathcal{I}$).

Moreover, the element λ can be chosen such that $\lambda^2 = \zeta\ell$ for some 2^r-th root of unity $\zeta \in K$. In that case, the following proposition gives the corresponding λ.

Proposition 2.1. *Let $\lambda \in K$ be an element satisfying $\lambda^2 = \zeta\ell$ for some primitive 2^r-th root of unity $\zeta \in K$. Then we have :*

(i) $\lambda = \pm\sqrt{\ell}$ *if* $r = 0$,
(ii) $\lambda = \pm\sqrt{-\ell}$ *if* $r = 1$,
(iii) $\lambda = \pm(1+\zeta^{-1})^{-1}\sqrt{(\zeta+\zeta^{-1}+2)\ell}$ *if* $r \geq 2$.

For strongly Arakelov-modular lattices, we have the following result (see [4], Proposition 3.3).

Proposition 2.2. *Let $(\mathcal{I}, \alpha)$ be an Arakelov-modular lattice over K. This lattice is strongly Arakelov-modular if and only if for each $m||\ell$, there exists $\beta_m \in \mathcal{O}_K$ such that:*

(i) $\beta_m\overline{\beta}_m = m$, *and*
(ii) $\beta_m\mathcal{O}_K = \overline{\beta_m\mathcal{O}_K}$.

Moreover, if the preceding conditions are satisfied, then the β_m's can be chosen such that $\beta_m^2 = \zeta_{(m)}m$, where $\zeta_{(m)}$ is some 2^{r_m}-th root of unity (depending on m).

Notice that if such a set of β_m exists in K, then all Arakelov-modular lattices of level ℓ over K are indeed strongly modular.

Proof. If such a set of β_m for $m||\ell$ exists, then [4], Proposition 3.3 shows that $(\mathcal{I}, \alpha)$ is strongly Arakelov-modular.

Conversely, if $(\mathcal{I}, \alpha)$ is strongly Arakelov-modular, then we can choose for each $m||\ell$ an element $\beta_m \in K$ such that $\left(\beta_m\mathcal{I}_m, (\beta_m\overline{\beta}_m)^{-1}m\alpha\right) = (\mathcal{I}, \alpha)$, where $\mathcal{I}_m = \left(\frac{1}{m}\mathcal{I}\right) \cap \mathcal{I}^*$. The ideal $\mathcal{I}_m$ can be explicitely determined as follow. Let's choose $\lambda \in \mathcal{O}_K$ such that $\lambda\overline{\lambda} = \ell$ and such that $\lambda\mathcal{I}^* = \mathcal{I}$ (such a λ exists thanks to the preceding remark). We have

$$\mathcal{I}_m = \left(\frac{1}{m}\mathcal{I}\right) \cap \mathcal{I}^* = (m^{-1}\mathcal{I}) \cap (\lambda^{-1}\mathcal{I}) = ((m^{-1}\mathcal{O}_K) \cap (\lambda^{-1}\mathcal{O}_K))\mathcal{I} = \mathfrak{b}_m^{-1}\mathcal{I},$$

where $\mathfrak{b}_m = m\mathcal{O}_K + \lambda\mathcal{O}_K$. Since $\lambda^2\mathcal{O}_K = \ell\mathcal{O}_K$ and since $m||\ell$, we get that $\mathfrak{b}_m^2 = m\mathcal{O}_K$. Moreover, the definition of β_m shows that $\beta_m\mathcal{I}_m = \beta_m\mathfrak{b}_m^{-1}\mathcal{I} = \mathcal{I}$, i.e. that $\beta_m\mathcal{O}_K = \mathfrak{b}_m$. Finally, since $(\beta_m\overline{\beta}_m)^{-1}m\alpha = \alpha$, we get that $\beta_m\overline{\beta}_m = m$ and we are done.

Finally, if β_m satisfies the conditions of the proposition, then $\beta_m/\overline{\beta}_m$ is a root of unity, from which the odd part can be removed, as in [4], Proposition 3.4 (since each n-th root of unity with n odd is a square). □

3. Classification of modular lattices over CM fields

Denote the set of Arakelov-modular lattices over K of level ℓ modulo Arakelov-equivalence by $\mathrm{AM}_K(\ell)$. Let $\mathrm{Cl}(K)$ denote the ideal class group of K and let E_K be the group of units of $\mathcal{O}_K$. Let $G = \mathbf{Gal}(K/F)$, and define $C_1 = \mathrm{Cl}(K)^G$, $C_2 := \{[\mathcal{J}] \in \mathrm{Cl}(K) \ : \ \exists\alpha \in K \text{ such that } \alpha\mathcal{J} = \overline{\alpha\mathcal{J}}\}$. It is easily checked that $C_2 = I_K^G/P_K^G \subset C_1$, where I_K (resp. P_K) is the group of ideals (resp. principal ideals) in K. In the following, we will assume that $\mathrm{AM}_K(\ell) \neq \emptyset$. We then call $A_\ell \subset F^\times$ the set of $\alpha \in F$ for which there exists an ideal $\mathcal{I}$ such that the ideal lattice $(\mathcal{I}, \alpha)$ is Arakelov-modular of level ℓ. The aim of this section is to describe $\mathrm{AM}_K(\ell)$.

Remark 3.1. The set A_ℓ is exactly the set of totally positive $\alpha \in F$ such that there exists an ideal $\mathcal{I}$ in K satisfying $\alpha^{-1}\lambda\mathcal{D}_K^{-1} = \mathcal{I}\overline{\mathcal{I}}$.

The class group of K acts on $\mathrm{AM}_K(\ell)$ as follow.

Let $[\mathcal{J}] \in \mathrm{Cl}(K)$ and let $[\mathcal{I}, \alpha] \in \mathrm{AM}_K(\ell)$. We can form the ideal lattice $[\mathcal{J}]\cdot[\mathcal{I}, \alpha] := [\mathcal{J}\overline{\mathcal{J}}^{-1}\mathcal{I}, \alpha]$, and it is easy to check that $[\mathcal{J}\overline{\mathcal{J}}^{-1}\mathcal{I}, \alpha] \in \mathrm{AM}_K(\ell)$. This gives an action of $\mathrm{Cl}(K)$ on $\mathrm{AM}_K(\ell)$.

The stabilisor of any ideal lattice of $\mathrm{AM}_K(\ell)$ is the group C_2. Indeed, if $[\mathcal{J}] \cdot [\mathcal{I}, \alpha] = [\mathcal{I}, \alpha]$, then there exists $\beta \in K$ such that $\mathcal{J}\overline{\mathcal{J}}^{-1}\mathcal{I} = \beta\mathcal{I}$ and $\beta\overline{\beta} = 1$. Hilbert Theorem 90 gives then the existence of $\gamma \in K$ such that $\beta = \gamma^{-1}\overline{\gamma}$, and we therefore get that $\gamma\mathcal{J} = \overline{\gamma\mathcal{J}}$, i.e. that $[\mathcal{J}] \in C_2$.

Let $[\mathcal{I}, \alpha] \in \mathrm{AM}_K(\ell)$. The orbit of the ideal lattice $[\mathcal{I}, \alpha]$ under $\mathrm{Cl}(K)$ in $\mathrm{AM}_K(\ell)$ is exactly the set of Arakelov-modular lattices of level ℓ which can be written $[\mathcal{I}', \alpha]$ for some ideal $\mathcal{I}'$. Therefore, we have a bijection $\mathrm{AM}_K(\ell)/\mathrm{Cl}(K) \cong A_\ell/\mathbf{N}_{K/F}(K)$.

In order to complete the description of $\mathrm{AM}_K(\ell)$, we will now be interested in $A_\ell/\mathbf{N}_{K/F}(K)$. First of all, recall that the Hasse norm theorem states that the following sequence is exact:

$$0 \to \widehat{H}^0(K/F, K^\times) \to \bigoplus_v \widehat{H}^0(K_v/F_v, K_v^\times) \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

In this exact sequence, the direct sum is taken over the set of places v of F, we have $\widehat{H}^0(K/F, K^\times) = F^\times/\mathbf{N}_{K/F}\,K^\times$, and the last application is the sum on coordinates. The field F_v denotes the completion of F at v, and K_v denotes the completion of K at some place above v.

Let $\lambda \in K$ be such that $\lambda\overline{\lambda} = \ell$. Each Arakelov-modular lattice $(\mathcal{I}, \alpha)$ of level ℓ over K satisfies

$$\lambda\mathcal{D}_K^{-1} = \alpha\mathcal{I}\overline{\mathcal{I}}.$$

Therefore, if $(\mathcal{I}, \alpha)$ and $(\mathcal{I}', \alpha')$ are two Arakelov-modular lattices of level ℓ, then $\alpha\mathcal{I}\overline{\mathcal{I}} = \alpha'\mathcal{I}'\overline{\mathcal{I}'}$. Since $\alpha/\alpha'\mathcal{O}_F$ is the norm of some ideal of K, the element α/α' maps to 1 via the map $\widehat{H}^0(K/F, K^\times) \to \widehat{H}^0(K_v/F_v, K_v^\times)$ for each place v which is unramified (since for local fields, the norm map is surjective on the units if the extension is unramified). Notice that α/α' also maps to 1 for each infinite place v, since α/α' is totally positive.

This says that $\alpha/\alpha' \in N$, where $N \subset \left(\bigoplus_v \widehat{H}^0(K_v/F_v, K_v^\times)\right) \cap \widehat{H}^0(K/F, K^\times)$ is the subgroup of elements which are local norm whenever v is infinite or unramified in K.

Conversely, if $\gamma \in K^\times$ maps to an element of N, then $\gamma \in F$ is totally positive. Moreover, γ is a norm locally whenever $\mathfrak{p}$ is a prime ideal which does not ramify in K/F. So we have the decomposition $\gamma\mathcal{O}_K = \mathcal{J}\overline{\mathcal{J}}$ for some ideal $\mathcal{J}$. Therefore, for each $\alpha \in A_\ell$, the element $\gamma\alpha$ is also in A_ℓ (see Remark 3.1). Notice that if $\gamma \in K^\times$ maps to $1 \in N$, then the Hasse norm Theorem implies that $\gamma\alpha$ and α are in the same class in $A_\ell/\mathbf{N}_{K/F}(K^\times)$. Therefore, we get the following proposition.

Proposition 3.2. *The subgroup* $N \subset \left(\bigoplus_v \widehat{H}^0(K_v/F_v, K_v^\times)\right) \cap \widehat{H}^0(K/F, K^\times)$ *acts freely and transitively on* $\mathrm{AM}_K(\ell)/\mathrm{Cl}(K)$.

This proposition allows us to compute $|\mathrm{AM}_K(\ell)|$.

First of all, let r be the number of ramified finite primes in K/F. We have

$$|N| = 1 + \binom{r}{2} + \binom{r}{4} + \cdots = 2^{r-1}.$$

Therefore, the number of Arakelov-modular lattices of level ℓ over K is

$$|\mathrm{AM}_K(\ell)| = 2^{r-1}|\operatorname{Cl}(K)/C_2|.$$

Let $G = \mathbf{Gal}(K/F)$ be the Galois group of K/F, and denote by I_K (resp. P_K) the ideal group of K (resp. the principal ideal group of K). The group C_2 is isomorphic to I_K^G/P_K^G. Fortunately, the order of this group is known (see for instance the proof of [6], Chap. 13, lemma 4.1). Actually, we have

Lemma 3.3.

$$|C_2| = \frac{e(K/F)h_F}{[K:F]|\widehat{H}^0(E_K)|}.$$

Here, $h_F = |\operatorname{Cl}(F)|$, and $e(K/F) = \prod_v e(v)$, where the product is taken over all the places of F, and where $e(v)$ is the local ramification degree at v. The group $\widehat{H}^0(E_K) = E_F/\mathbf{N}_{K/F}(E_K)$ can be computed as follow.

Write $e(K/F) = e_0(K/F)e_\infty(K/F)$, where

$$e_0(K/F) = \prod_{\mathfrak{p} \text{ finite}} e(\mathfrak{p}) \text{ and } e_\infty(K/F) = \prod_{v \text{ infinite}} e(v).$$

Since K is a CM-field, we have $[E_K : E_F\mu_K] = 1$ or 2, so $[\mathbf{N}_{K/F}(E_K) : \mathbf{N}_{K/F}(E_F\mu_K)] = [E_K : E_F\mu_K]$. Furthermore, since $\mathbf{N}_{K/F}(E_F\mu_K) = E_F^2$, we get that

$$|\widehat{H}^0(E_K)| = \frac{e_\infty(K/F)}{2[E_K : E_F\mu_K]}.$$

But $e_0(K/F) = e(K/F)/e_\infty(K/F) = 2^r$, so

$$|C_2| = 2^{r+1}[E_K : E_F\mu_K]h_F.$$

Finally, we obtain the following formula for $|\mathrm{AM}_K(\ell)|$.

Proposition 3.4. *If $\mathrm{AM}_K(\ell) \neq \emptyset$, we have*

$$|\mathrm{AM}_K(\ell)| = \begin{cases} \frac{h_K}{2h_F} & , \text{ if } [E_K : E_F\mu_K] = 1, \\ \frac{h_K}{4h_F} & , \text{ if } [E_K : E_F\mu_K] = 2. \end{cases}$$

The group C_2 is also easy to describe. We have the map $j_{K/F} : \operatorname{Cl}(F) \to \operatorname{Cl}(K)^G = C_1$ induced by the extension of ideals from F to K. Since K is a CM field, the kernel of $j_{K/F}$ has order 1 or 2, and of course $j_{K/F}(\operatorname{Cl}(F)) \subset C_2$. Moreover, since $C_2 = I_K^G/P_K^G$, it is easy to see that C_2 is actually generated by $\operatorname{im}(j_{K/F})$ and by the ramified primes in K/F (compare with Lemma 3.3).

Notice that we also get an isomorphism $\varphi : C_1/C_2 \to (\mathbf{N}_{K/F}(K^\times) \cap E_F)/\mathbf{N}_{K/F}E_K$, which can be defined as follow. Let $[\mathcal{J}] \in C_1$, and take $\beta \in K$ such that $\beta\mathcal{O}_K = \mathcal{J}^{-1}\overline{\mathcal{J}}$. Then $\beta\overline{\beta} \in \mathbf{N}_{K/F}(K^\times) \cap E_F$ is the desired element. It is easily seen that the kernel of this map is C_2. The surjectivity of this map will be checked later. This map comes from the following observation. The class $[\mathcal{J}] \in C_1$ is mapped to a totally positive

unit $u \in E_F^+$ such that for each class $[\mathcal{I}, \alpha] \in \mathrm{AM}_K(\ell)$, we have $[\mathcal{J}] \cdot [\mathcal{I}, \alpha] = [\mathcal{I}, u\alpha]$.

In order to show that φ is surjective, we will call I_K (resp. P_K) the group of ideals (resp. principal ideals) in K. The two following sequences are exact.

$$1 \to P_K \to I_K \to \mathrm{Cl}(K) \to 1$$
$$1 \to E_K \to K^\times \to P_K \to 1$$

From the first exact sequence, we get the long exact sequence in cohomology

$$H^0(\mathrm{Cl}(K)) \to H^1(P_K) \to H^1(I_K) = 1,$$

From the second exact sequence, we get

$$H^1(K^\times) = 1 \to H^1(P_K) \to \widehat{H}^0(E_K) \to \widehat{H}^0(K^\times),$$

which gives an isomorphism $H^1(P_K) \cong (\mathbf{N}_{K/F}(K^\times) \cap E_F)/\mathbf{N}_{K/F} E_K$. Now, the map $\tilde{\varphi} : C_1 \to (\mathbf{N}_{K/F}(K^\times) \cap E_F)$ is the composition of the two preceding maps, and $\tilde{\varphi}$ is therefore surjective.

4. Modular lattices over multiquadratic fields

Proposition 2.2 suggests us to look for ideal lattices over multiquadratic fields. We will begin our investigation with the case of biquadratic fields.

Lemma 4.1. *Let p and q be two distinct primes, and define $K = \mathbb{Q}(\sqrt{p}, \sqrt{-q})$. Then there exists a totally positive element $\alpha \in \mathbb{Q}(\sqrt{p})$ and an ideal $\mathcal{I}$ in K such that*

$$\sqrt{p}\mathcal{O}_K = \alpha \mathcal{I}\overline{\mathcal{I}}.$$

Proof. If $\left(\frac{-q}{p}\right) = 1$, then we have $\sqrt{p}\mathcal{O}_K = \mathfrak{P}\overline{\mathfrak{P}}$ for a prime ideal $\mathfrak{P}$ in K.

If $p = 2$ or if $p \equiv 1 \mod 4$, then there is a unit u in $\mathbb{Q}(\sqrt{p})$ of norm -1. Therefore, $\pm u\sqrt{p}$ is totally positive.

Finally, we must consider the case where $p \equiv 3 \mod 4$ and $\left(\frac{-q}{p}\right) = -1$. It is well known that the class number $h_{\mathbb{Q}(\sqrt{p})}$ of $\mathbb{Q}(\sqrt{p})$ is odd (see [5], Theorem 41). Let's take a prime number r satisfying the following conditions:

(i) $\left(\frac{p}{r}\right) = 1$,
(ii) $\left(\frac{-q}{r}\right) = 1$, and
(iii) $\left(\frac{-r}{p}\right) = 1$.

The Dirichlet theorem on primes in arithmetic progressions asserts that such a prime r exists if the three conditions are independent. The conditions (i) and (ii) are independent since $p \neq q$. In view of condition (i), the third condition asserts that $r \equiv 3 \mod 4$. It is therefore independent of condition (ii) unless $q = 2$. However, when $q = 2$, the conditions (ii) and (iii) are equivalent to asking that $r \equiv 3 \mod 8$. Therefore, a prime number r satisfying conditions $(i) - (iii)$ always exists.

Now, conditions (i) and (ii) imply that r is totally split in K. So let $\mathfrak{r}$ (resp. $\mathfrak{R}$) be a prime ideal in $\mathbb{Z}[\sqrt{p}]$ (resp. in $\mathcal{O}_K$) above r (resp. above $\mathfrak{r}$). Let d be the order of $\mathfrak{r}$ in $\mathrm{Cl}(\mathbb{Q}(\sqrt{p}))$ (recall that d is odd), and let ρ be a generator of $\mathfrak{r}^d$. We have $\mathbf{N}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\rho) = \pm r^d$. Now, condition (iii) implies that r is not a norm in $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, therefore, $\mathbf{N}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\rho) = -r^d$. If

we define $\alpha = \sqrt{p}\rho^{-1}$, and $\mathcal{I} = \mathfrak{R}^d$, then either α or $-\alpha$ is totally positive and $\sqrt{p}\mathcal{O}_K = \alpha\mathcal{I}\overline{\mathcal{I}}$. So the lemma is proved. □

Lemma 4.2. *Let p be a prime number, and let $K = \mathbb{Q}(\sqrt{p}, \sqrt{-1})$. Then there exists a totally positive element $\alpha \in \mathbb{Q}(\sqrt{p})$ and an ideal $\mathcal{I}$ in K such that $\sqrt{p}\mathcal{O}_K = \alpha\mathcal{I}\overline{\mathcal{I}}$ if and only if $p \not\equiv 3 \mod 4$.*

Proof. If $p = 2$ or if $p \equiv 1 \mod 4$, then there exists a unit u such that $u\sqrt{p}$ is totally positive.

If $p \equiv 3 \mod 4$, then the extension $\mathbb{Q}(\sqrt{p}, \sqrt{-1})/\mathbb{Q}(\sqrt{p})$ is unramified et each finite place. Therefore, class field theory tells us that the existence of a decomposition $\sqrt{p}\mathcal{O}_K = \alpha\mathcal{I}\overline{\mathcal{I}}$ is equivalent to the fact that $\sqrt{p}\mathbb{Z}[\sqrt{p}]$ belongs to the kernel of the Artin map. But since $p \equiv 3 \mod 4$, p is inert in $\mathbb{Q}(\sqrt{-1})$, so the ideal $\sqrt{p}\mathbb{Z}[\sqrt{p}]$ does not belong to the kernel of the Artin map. This conculdes the proof. □

We are now ready to investigate the existence of Arakelov-modular lattices over some multiquadratic fields.

Proposition 4.3. *Let $p_1, \cdots, p_n$ and q be $n+1$ distinct primes. Let $K = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n}, \sqrt{-q})$, and let ℓ be a square-free integer.*

The set $\mathrm{AM}_K(\ell)$ is not empty if and only if $q|\ell|qp_1 \cdots p_n$.

Proof. Assume that $\mathrm{AM}_K(\ell) \neq \emptyset$. There exists an integer $\lambda \in \mathcal{O}_K$ such that $\lambda^2 = \ell\zeta$, for some 2^r-th root of unity ζ. But K is a multiquadratic field and $\sqrt{-1} \notin K$, so we must have $\zeta = \pm 1$. Therefore we have $\lambda^2 = \pm\ell$, so that $\ell|qp_1 \cdots p_n$. Now, if $(\mathcal{I}, \alpha)$ is an Arakelov-modular lattice of level ℓ over K, then we have

$$\lambda\mathcal{D}_K^{-1} = \alpha\mathcal{I}\overline{\mathcal{I}}.$$

Therefore the ideal $\lambda\mathcal{D}_K^{-1}$ is an extension of an ideal over F. Since $\sqrt{-q}||\mathcal{D}_K$, this implies that $\sqrt{-q}||\lambda$, so that $q|\ell$.

Conversely, assume that $q|\ell|qp_1 \cdots p_n$. For each prime p_i, Lemma 4.1 shows that there exists a totally positive $\alpha_i \in F$ and an ideal $\mathcal{I}_i$ such that $\sqrt{p_i}\mathcal{O}_K = \alpha_i\mathcal{I}_i\overline{\mathcal{I}_i}$. Define λ such that $\lambda^2 = -\ell$. The ideal $\lambda\mathcal{D}_K^{-1}$ is a product of ideals which can be written $\sqrt{p_i}\mathcal{O}_K$ or $2\mathcal{O}_K$, and this ideal can therefore be written $\alpha\mathcal{I}\overline{\mathcal{I}}$ for some totally positive $\alpha \in F$. This shows the existence of an Arakelov-modular latticeof level ℓ over K, and thus completes the proof. □

Example 4.4. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{13}, \sqrt{-3})$. We have $|\mathrm{AM}_K(6)| = 96$. Moreover, a computation with PARI/GP ([1]) gives that some of the Arakelov 6-strongly modular lattices over K are extremal (i.e. of minimum 6). All of them have automorphism group of order $2^{10} \cdot 3^6 \cdot 5$, and may be isomorphic to the lattice described in [9].

Proposition 4.5. *Let $p_1, \cdots, p_n$ be distinct primes, and assume that $n \geq 2$. Let $K = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n}, \sqrt{-1})$.*

If one of the p_i's satisfies $p_i \equiv 3 \mod 4$, then $\mathrm{AM}_K(\ell) \neq \emptyset$ if and only if $\ell \mid 2p_1 \cdots p_n$.

If each p_i satisfies $p_i \not\equiv 3 \mod 4$, then $\mathrm{AM}_K(\ell) \neq \emptyset$ if and only if $\ell \mid p_1 \cdots p_n$.

Proof. Assume that $\mathrm{AM}_K(\ell) \neq \emptyset$. This implies that $\ell|\operatorname{disc}(K/F)$. Since ℓ is square-free, we get that either $\ell|2p_1 \cdots p_n$, if one of the p_i's satisfies $p_i \equiv 3 \mod 4$, or $\ell|p_1 \cdots p_n$ otherwise.

Conversely, let $F = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$ be the maximal totally real subfield of K. Assume first that $p_1 \equiv 3 \mod 4$. The extension K/F is then unramified at the finite places (since $\mathbb{Q}(\sqrt{p_1}, \sqrt{-1})/\mathbb{Q}(\sqrt{p_1})$ is unramified). Let $\Psi_{K/F} : \mathbf{I}_F \to \mathbf{Gal}(K/F)$ be the Artin map. The kernel of the Artin map is precisely the set of ideals whose transfer to K can be written $\alpha\mathcal{I}\overline{\mathcal{I}}$, for some totally positive element α. Now for each prime p_i, it is easy to see that either an even number of prime ideals divide $\sqrt{p_i}\mathcal{O}_F$, either $\sqrt{p_i}\mathcal{O}_F$ is a prime ideal which is totally plit in K/F (the latter case can only happen when $n = 2$). Since $F/\mathbb{Q}$ is a Galois extension, the value of $\Psi_{K/F}(\mathfrak{p}_i)$ does not depend on the choice of a prime ideal $\mathfrak{p}_i$ above p_i in F. Therefore, for each p_i, we have $\Psi_{K/F}(\sqrt{p}_i\mathcal{O}_F) = 1$, so each ideal $\sqrt{p_i}\mathcal{O}_K$ can be written $\alpha_i\mathcal{I}_i\overline{\mathcal{I}_i}$ for some totally positive element α_i. Similarly, it can be checked that $\Psi_{K/F}(((1+\sqrt{-1})\mathcal{O}_K) \cap \mathcal{O}_F) = 1$. The ideal $(1+\sqrt{-1})\mathcal{O}_K$ can thus also be written $\alpha\mathcal{I}\overline{\mathcal{I}}$, for some totally positive element α and some ideal $\mathcal{I}$ in K. Therefore, for each square-free $\ell | 2p_1 \cdots p_n$, there exists an Arakelov-modular lattice of level ℓ over K.

Assume now that each p_i satisfies $p_i \not\equiv 3 \mod 4$. Lemma 4.2 gives the existence of a decomposition $\sqrt{p_i}\mathcal{O}_K = \alpha_i\mathcal{I}_i\overline{\mathcal{I}_i}$ for each p_i. This gives the existence of an Arakelov-modular lattice of level ℓ over K for each square-free $\ell | p_1 \cdots p_n$, and thus completes the proof. □

The next proposition handles the case where $K = \mathbb{Q}(\sqrt{p}, \sqrt{-1})$.

Proposition 4.6. *Let p be a prime number, and let $K = \mathbb{Q}(\sqrt{p}, \sqrt{-1})$.*
If $p \not\equiv 3 \mod 4$, then $\mathrm{AM}_K(\ell) \neq \emptyset$ if and only if $\ell \in \{1,\ p\}$.
If $p \equiv 3 \mod 8$, then $\mathrm{AM}_K(\ell) \neq \emptyset$ if and only if $\ell = p$.
If $p \equiv 7 \mod 8$, then $\mathrm{AM}_K(\ell) \neq \emptyset$ if and only if $\ell \in \{2,\ p\}$.

Proof. If $p \not\equiv 3 \mod 4$, Lemma 4.2 gives that $\mathrm{AM}_K(\ell) \neq \emptyset$ for $\ell = 1,\ p$.

Assume now that $p \equiv 3 \mod 4$. The extension $\mathbb{Q}(\sqrt{p}, \sqrt{-1})/\mathbb{Q}(\sqrt{p})$ is unramified, so we have $\mathcal{D}_K = (2\sqrt{p})$. Therefore, there exists an Arakelov-modular lattices of level ℓ over K if and only if $\Psi_{K/F}((\lambda\mathcal{D}_K^{-1}) \cap F) = 1$. For $\lambda = \sqrt{p}$, we have $\Psi_{K/F}((\lambda\mathcal{D}_K^{-1}) \cap F) = \Psi_{K/F}(1/2\mathcal{O}_F) = 1$, so $\mathrm{AM}_K(p) \neq \emptyset$. Now, for $\ell \neq p$ we must compute $\Psi_{K/F}(\mathfrak{q})$ for the prime ideal $\mathfrak{q}$ of F above 2.

We have $2\mathcal{O}_F = \mathfrak{q}^2$. If $p \equiv 3 \mod 8$, then $\mathfrak{q}\mathcal{O}_K$ is a prime ideal, so $\Psi_{K/F}(\mathfrak{q}) = -1$. If $p \equiv 7 \mod 8$, then $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}\overline{\mathfrak{Q}}$, for a prime ideal $\mathfrak{Q}$ of $\mathcal{O}_K$, so $\Psi_{K/F}(\mathfrak{q}) = 1$. This gives the value of $\Psi_{K/F}((\lambda\mathcal{D}_K^{-1}) \cap F)$ for each $\ell | 2p$, and the proposition is proved. □

We are now interested in the case $K = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_r}, \sqrt{-q_1}, \cdots, \sqrt{-q_s})$, with p_i, $q_{,j}$ distincts primes and $s \geq 2$.

Proposition 4.7. *Assume that $K = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_r}, \sqrt{-q_1}, \cdots, \sqrt{-q_s})$ is defined as above. Assume also that $r + s \geq 3$, and let ℓ be a square-free integer.*

The set $\mathrm{AM}_K(\ell)$ is not empty if and only if $\ell | p_1 \cdots p_r q_1 \cdots q_s$.

Lemma 4.8. *Let $q_1 < q_2$ be two distinct primes. Let $K = \mathbb{Q}(\sqrt{-q_1}, \sqrt{-q_2})$, and let $F = \mathbb{Q}(\sqrt{q_1 q_2})$. The extension K/F is ramified if and only if $q_1 \equiv$*

$q_2 \equiv 1 \mod 4$ *or* $q_1 = 2$ *and* $q_2 \equiv 1 \mod 4$. *In the first case, the different is* (2) *and in the second case, the different is* $(\sqrt{-2})$.

Proof. The three fields between $\mathbb{Q}$ and K are $F_1 = \mathbb{Q}(\sqrt{-q_1})$, $F_2 = \mathbb{Q}(\sqrt{-q_2})$ and F. The extension K/F is unramified at the primes of odd norm. Therefore all the ramification in K/F comes from the dyadic ramification. If q_1 and q_2 are odd, we have $\mathcal{D}_{K/F} \neq \mathcal{O}_K$ if and only if $q_1 \equiv q_2 \equiv 1 \mod 4$, and in this case we have $\mathcal{D}_{K/F} = 2\mathcal{O}_K$. If $q_1 = 2$, the field extension K/F is ramified if and only if $-q_2 \equiv 3 \mod 4$, and in this case we have $\mathcal{D}_{K/F} = \sqrt{-2}\mathcal{O}_K$. □

Proof of Proposition 4.7. This time, we have $F = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_r}, \sqrt{q_1q_2}, \cdots, \sqrt{q_1q_s})$. Therefore, the different $\mathcal{D}_{K/F}$ can only be $\mathcal{O}_K$, $2\mathcal{O}_K$ or $\sqrt{\pm 2}\mathcal{O}_K$ (see Lemma 4.8). Moreover, if $\mathcal{D}_{K/F} \neq \mathcal{O}_K$, then there exists an ideal $\mathfrak{a}$ such that $\mathfrak{a}^2 = \mathcal{D}_{K/F}$. We are now interested in the ideals $\mathcal{I} = \sqrt{p_i}\mathcal{O}_F$ or $\mathcal{I} = (\sqrt{-q_j}) \cap F$. Since $[F : \mathbb{Q}] \geq 4$, we have either an even number of prime ideals dividing $\mathcal{I}$, or $\mathcal{I}$ is a prime ideal which splits in K. Therefore $\Psi_{K/F}(\mathcal{I}) = 1$ and $\mathcal{I}\mathcal{O}_K = \alpha_i\mathcal{J}_i\overline{\mathcal{J}_i}$ for some totally positive element $\alpha_i \in F$. This shows that for each ℓ dividing $p_1 \cdots p_r q_1 \cdots q_s$, we have $\mathrm{AM}_K(\ell) \neq \emptyset$. □

Example 4.9. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{-2}, \sqrt{-7})$. For $\ell = 6$ and for $\ell = 15$, we have $|\mathrm{AM}_K(\ell)| = 16$. A computation with PARI/GP gives us that for $\ell = 6$ and for $\ell = 15$, there is one extremal strongly Arakelov-modular lattice of level ℓ over K.

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. `PARI/GP`. *available at* `http://pari.math.u-bordeaux.fr/`.

[2] E. Bayer-Fluckiger. Lattices and Number Fields. *Contemporary Mathematics*, 241:69–84, 1999.

[3] E. Bayer-Fluckiger. Ideal Lattices. *in A Panorama of Number Theory or The View from Baker's Garden, edited by Gisbert Wustholz*, Cambridge Univ. Press, Cambridge:168–184, 2002.

[4] E. Bayer-Fluckiger and I. Suarez. Modular lattices over cyclotomic fields. *J. Number Theory*, 114 No. 2:394–411, 2005.

[5] A. Fröhlich and M.J. Taylor. *Algebraic Number Theory*, volume 27. Cambridge studies in advanced mathematics, 1991.

[6] S. Lang. *Cyclotomic Fields II*, volume GTM69. Springer Verlag, 1980.

[7] H.-G. Quebbemann. Modular Lattices in Euclidean Spaces. *Journal of Number Theory*, 54:190–202, 1995.

[8] H.-G. Quebbemann. Atkin-Lehner eigenforms and strongly modular lattices. *L'Enseignement Mathématique*, 43:55–65, 1997.

[9] R. Scharlau and R. Schulze-Pillot. Extremal lattices. *Matzat, B. Heinrich (ed.) et al., Algorithmic algebra and number theory. Selected papers from a conference, Heidelberg, Germany, October 1997.*, Berlin: Springer:139–170, 1999.

École Polytechnique Fédérale de Lausanne, Institut de MathÃĽmatiques Bernoulli, CH-1015 Lausanne, Switzerland

E-mail address: `isuarez@univ-lemans.fr`