AUTOMORPHISMS OF EVEN UNIMODULAR LATTICES OVER NUMBER FIELDS

MARKUS KIRSCHMER

Abstract. We describe the powers of irreducible polynomials occurring as characteristic polynomials of automorphisms of even unimodular lattices over number fields. This generalizes results of Gross & McMullen and Bayer-Fluckiger & Taelman.

1. Introduction

Even unimodular lattices over the integers correspond to regular quadratic forms over $\mathbb{Z}$. Hence they play an important role. Gross and McMullen [6] give necessary conditions for an irreducible polynomial $S \in \mathbb{Z}[t]$ to be the characteristic polynomial of an automorphism of an even unimodular $\mathbb{Z}$-lattice. They speculate that these conditions are sufficient. This conjecture was proved recently by Bayer-Fluckiger and Taelman [2] not only in the case that S is irreducible but also for powers of irreducible polynomials. The purpose of this note is to extend the characterization of Bayer-Fluckiger and Taelman to any algebraic number field K with ring of integers $\mathfrak{o}$.

To state the main result, some notation is necessary. Let $\Omega(K)$ be the set of all places of K. For $v \in \Omega(K)$ let K_v be the completion of K at v. If v is finite, we denote by $\mathfrak{o}_v$ the ring of integers of K_v. Let $\Omega_2(K)$ be the set of all even places of K, i.e. the finite places over 2. For $v \in \Omega_2(K)$ let e_v be the ramification index of K_v and let $\Delta_v \in \mathfrak{o}_v^*$ be a unit of quadratic defect $4\mathfrak{o}$, see Definition 3.3 for details. Further, let $\Omega_r(K)$ denote the set of real places of K. Given a polynomial $S \in \mathfrak{o}[t]$ and $v \in \Omega_r(K)$, let $2m_v(S)$ be the number of complex roots of $S \in K_v[t]$ which do not lie on the unit circle.

Theorem A. *Let n be a positive integer. For $v \in \Omega_r(K)$ let (r_v, s_v) be a pair of non-negative integers such that $r_v + s_v = 2n$. Let $P \in \mathfrak{o}[t]$ be a monic irreducible polynomial different from $t \pm 1$ and let S be a power of P such that $\deg(S) = 2n$. Then there exists an even unimodular $\mathfrak{o}$-lattice L such that K_vL has signature (r_v, s_v) for all $v \in \Omega_r(K)$, and some proper automorphism of L with characteristic polynomial S if and only if the following conditions hold.*

- (C1) *S is reciprocal, i.e. $t^{2n}S(1/t) = S(t)$.*
- (C2) *$m_v(S) \le \min(r_v, s_v)$ and $m_v(S) \equiv r_v \equiv s_v \pmod 2$ for all $v \in \Omega_r(K)$.*
- (C3) *The fractional ideals $S(1)\mathfrak{o}$ and $S(-1)\mathfrak{o}$ are squares.*
- (C4) *$(-1)^n S(1)S(-1) \cdot K_v^{*,2} \in \{K_v^{*,2},\ \Delta_v \cdot K_v^{*,2}\}$ for all $v \in \Omega_2(K)$.*
- (C5) *$(-1)^{s_v} S(1)S(-1) \in K_v$ is positive for all $v \in \Omega_r(K)$.*

2010 *Mathematics Subject Classification.* 11H56.
Key words and phrases. Even unimodular lattices, Automorphisms.

(C6) *The cardinalities of the sets*

$$\{v \in \Omega_r(K) \mid n(n-1) \not\equiv s_v(s_v-1) \pmod 4\}$$
$$\{v \in \Omega_2(K) \mid e_v \text{ is odd and } (-1)^n S(1)S(-1) \notin K_v^{*,2}\}$$

have the same parity.

The outline of the proof of Theorem A is the same as in [2]. The $\mathfrak{o}$-lattice L will be constructed as a trace lattice of a suitable hermitian lattice of rank 1. Using the local-global principle for Brauer groups, [2] gives a criterion for the existence of such a global hermitian lattice with prescribed local structure. This reduces the proof of the theorem to the problem of finding a suitable even unimodular $\mathfrak{o}$-lattice over all local fields. [2] solves the latter problem completely for non-dyadic local fields but not for dyadic local fields other than $\mathbb{Q}_2$. The main contribution of this note is to fill this gap.

For $K = \mathbb{Q}$, one can recover [2, Theorem A] from Theorem A, cf. Remark 4.1. In this case it is well known that $r_\infty \equiv s_\infty \pmod 8$. This congruence does not hold for arbitrary algebraic number fields K. For example, let $K = \mathbb{Q}(\sqrt{6})$ and let L be the even unimodular $\mathfrak{o}$-lattice with Gram matrix

$$\begin{pmatrix} 2 & 1-\sqrt{6} \\ 1-\sqrt{6} & 6 \end{pmatrix} .$$

The determinant of this matrix is the fundamental unit $2\sqrt{6}+5$. Moreover, L is totally positive definite, i.e. it has signature $(2,0)$ at the two infinite places of K.

The paper is organized as follows. Section 2 recalls some facts about bilinear spaces and unimodular lattices. In Section 3, we answer the question whether a quadratic space over a local field admits an even unimodular lattice with given characteristic polynomial. Finally, the last section gives a proof of Theorem A.

2. Definitions, notation and basic facts

Let K be a field of characteristic different from 2.

A bilinear space (V,Φ) is a finite-dimensional vector space V over K equipped with a non-degenerate, symmetric, bilinear form $\Phi\colon V \times V \to K$. In this paper, the dimension of V is assumed to be even, say $2n$. Let $B = (b_1, \dots, b_{2n})$ be a basis of V. Then

$$\mathcal{G}(B) = (\Phi(b_i, b_j)) \in K^{2n\times 2n}$$

is called the Gram matrix of B. The determinant $\det(V,\Phi)$ of (V,Φ) is the determinant of $\mathcal{G}(B)$ viewed as an element of $K^*/K^{*,2}$. Further, $\operatorname{disc}(V,\Phi) = (-1)^n \cdot \det(V,\Phi)$ is called the discriminant of (V,Φ). Given any place v of K, we denote by $V_v := V \otimes_K K_v$ the completion of V at v.

The orthogonal and special orthogonal groups of (V,Φ) are

$$\begin{aligned} \mathrm{O}(V,\Phi) &= \{\varphi \in \mathrm{GL}(V) \mid \Phi(\varphi(x),\varphi(y)) = \Phi(x,y) \text{ for all } x,y \in V\} , \\ \mathrm{SO}(V,\Phi) &= \mathrm{O}(V,\Phi) \cap \mathrm{SL}(V) . \end{aligned}$$

Given any anisotropic vector $v \in V$ (i.e. $\Phi(v,v) \neq 0$), the reflection

$$\tau_v\colon V \to V \; w \mapsto w - 2\frac{\Phi(v,w)}{\Phi(v,v)} \cdot v \tag{2.1}$$

defines an element of $\mathrm{O}(V,\Phi)$. The reflections generate $\mathrm{O}(V,\Phi)$ and the spinor norm is the unique group homomorphism

$$\theta\colon \mathrm{O}(V,\Phi) \to K^*/K^{*,2}$$

such that $\theta(\tau_v) = \Phi(v,v)\cdot K^{*,2}$ for all anisotropic vectors $v \in V$.

Lemma 2.1. *Let (V,Φ) be a bilinear space over K of even rank. Let S be the characteristic polynomial of some $\alpha \in \mathrm{SO}(V,\Phi)$. Then*

$$\theta(\alpha) = S(-1)\cdot K^{*,2} \quad \textit{and} \quad \theta(-\mathrm{id}_V) = \det(V,\Phi)\,.$$

Proof. Let V have rank $2n$. Zassenhaus' method to compute spinor norms [9, equation (2.1)] yields

$$\theta(\alpha) \equiv \det((\mathrm{id}_V+\alpha)/2) \equiv 2^{-2n}\det(\mathrm{id}_V+\alpha) \equiv S(-1) \pmod{K^{*,2}}\,.$$

The second congruence is [9, Equation (2.3)]. □

The following result is well known, see for example [1, Corollary 5.2] or [6, Proposition A.3].

Lemma 2.2. *Let (V,Φ) be a bilinear space over K of even rank. Let S be the characteristic polynomial of some $\alpha \in \mathrm{SO}(V,\Phi)$. If $S(\pm 1) \neq 0$ then $\det(V,\Phi) = S(1)S(-1)$.*

Proof. Lemma 2.1 yields

$$\det(V,\Phi) \equiv \theta(-\mathrm{id}_V) \equiv \theta(\alpha)\theta(-\alpha) \equiv S(1)S(-1) \pmod{K^{*,2}}\,,$$

since θ is a group homomorphism. □

Assume now that K is the field of fractions of a Dedekind ring $\mathfrak{o}$. Further let L be an $\mathfrak{o}$-lattice in (V,Φ), i.e. a finitely generated $\mathfrak{o}$-module L in V such that $KL = V$. The ideal generated by $\{\Phi(x,x) \mid x \in L\}$ is called the norm of L and is denoted by $\mathfrak{n}(L)$. The dual $L^\# := \{x \in V \mid \Phi(x,L) \subseteq \mathfrak{o}\}$ is also an $\mathfrak{o}$-lattice. If $L = L^\#$, then L is said to be unimodular. If in addition $\mathfrak{n}(L) \subseteq 2\mathfrak{o}$, then L is called even unimodular. In particular, if $2 \in \mathfrak{o}^*$ then any unimodular lattice is even.

We say that two $\mathfrak{o}$-lattices in V are properly isometric if they are in the same orbit under $\mathrm{SO}(V,\Phi)$. The stabilizer of a lattice L in V under $\mathrm{SO}(V,\Phi)$ is the proper automorphism group of L.

The proof of Theorem A is based on the construction of a suitable bilinear space using one-dimensional hermitian spaces. We recall this setup quickly.

Let E_0 be an étale K-algebra and let E be an étale E_0-algebra which is a free E_0-module of rank 2. There exists a unique K-linear involution σ on E which fixes E_0. Every $\lambda \in E_0^*$ gives rise of a bilinear form

$$b_\lambda\colon E\times E \to K,\ (x,y)\mapsto \mathrm{Tr}_{E/K}(\lambda x\sigma(y))$$

over K, where $\mathrm{Tr}_{E/K}\colon E \to K$ denotes the usual trace map. Multiplication by any $\alpha \in E^*$ with $\alpha\sigma(\alpha) = 1$ induces an isometry on (E,b_λ). The isometry class of the bilinear space (E,b_λ) only depends on the class of λ in

$$\mu(E,\sigma) := E_0^*/\{x\sigma(x) \mid x \in E^*\}\,.$$

Suppose that E is a field. By [2, Lemma 5.3], there exists a short exact sequence

$$1 \longrightarrow \mu(E,\sigma) \xrightarrow{\beta} \mathrm{Br}(E_0) \longrightarrow \mathrm{Br}(E)\,, \tag{2.2}$$

which identifies $\mu(E,\sigma)$ with the relative Brauer group $\mathrm{Br}(E/E_0)$.

3. Automorphisms of even unimodular lattices over local fields

Let K be a non-archimedean local field of characteristic 0 with ring of integers $\mathfrak{o}$ and uniformizer π. We assume the residue class field $\mathfrak{o}/\pi\mathfrak{o}$ to be finite. Further, let $\operatorname{ord}\colon K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation of K. The field K is said to be dyadic if $\operatorname{ord}(2) > 1$.

Given a non-degenerate bilinear space (V, Φ) over K with Gram matrix $\operatorname{diag}(a_1, \dots, a_n)$, set

$$c(V, \Phi) := \prod_{i<j} (a_i, a_j)$$

where $(\_,\_)$ denotes the Hilbert symbol of K. The integer $c(V, \Phi)$ is the Hasse-Witt invariant of (V, Φ) and does not depend on the chosen Gram matrix, see for instance [5, Lemma 2.2].

Theorem 3.1. *Let (V, Φ) be a bilinear space over K. Suppose L is an even unimodular $\mathfrak{o}$-lattice in V. If $\varphi \in \mathrm{SO}(V, \Phi)$ such that $\varphi(L) = L$, then $\theta(\varphi) \in \mathfrak{o}^* K^{*,2}$.*

Proof. The result is due to Kneser [7, Satz 3] for non-dyadic fields K. The dyadic case is solved by Beli in [3, Lemma 3.7 and Lemma 7.1]. □

Let E, E_0 and σ be as in Section 2. Let $\alpha \in E$ such that $\alpha\sigma(\alpha) = 1$ and $\sigma(\alpha) \neq \alpha$. Further, let S be the characteristic polynomial of α over K.

Proposition 3.2. *Suppose $S(1)$ and $S(-1)$ are non-zero and assume that one of the following conditions holds:*

- *K is non-dyadic and $\operatorname{ord}(S(1)) \equiv \operatorname{ord}(S(-1)) \equiv 0 \pmod 2$.*
- *K is dyadic and $\operatorname{ord}(S(1)) \equiv \operatorname{ord}(S(-1)) \pmod 2$.*

Then there exists some $\lambda \in \mu(E, \sigma)$ such that (E, b_λ) contains an α-stable unimodular $\mathfrak{o}$-lattice.

Proof. See Propositions 7.1 and 7.2 of [2]. □

Suppose now that K is dyadic. Then $2\mathfrak{o} = \pi^e\mathfrak{o}$ for some integer $e \geq 1$. In the unramified case, i.e. $e = 1$, Bayer-Fluckiger and Taelman give the analogous result of Proposition 3.2 for even unimodular lattices. We extend this classification to any ramification index e. The result is heavily based on O'Meara's classification of unimodular lattices over $\mathfrak{o}$, which we recall briefly.

Definition 3.3. The quadratic defect of $a \in K$ is

$$\mathfrak{d}(a) = \bigcap_{b \in K} (a - b^2)\mathfrak{o}\,.$$

We will make use of the following facts about the quadratic defect of units.

Lemma 3.4. *Let $a \in \mathfrak{o}^*$.*

1. *$\mathfrak{d}(a)$ only depends on the square class of a and $\mathfrak{d}(1) = (0)$.*
2. *There exists some element $b \in \mathfrak{o}$ such that $1 + b$ is in the square class of a and $\mathfrak{d}(a) = \mathfrak{d}(1 + b) = b\mathfrak{o}$.*
3. *There exists some unit $\Delta \in \mathfrak{o}^*$ of quadratic defect $4\mathfrak{o}$. Then $K(\sqrt{\Delta})$ is the unique unramified quadratic extension of K. In particular, Δ is unique up to unit squares.*

Proof. See Section 63A of [8], in particular 63:1a–63:5. □

For the remainder of this section, we fix some unit $\Delta \in \mathfrak{o}^*$ of quadratic defect $4\mathfrak{o}$. Without loss of generality, $\Delta = 1 + 4\delta$ for some unit $\delta \in \mathfrak{o}^*$. Note that $(a, \Delta) = (-1)^{\mathrm{ord}(a)}$, cf. [8, 63:11a].

Definition 3.5. Let L be a unimodular $\mathfrak{o}$-lattice in a bilinear space (V, Φ).

(1) The determinant $\det(L)$ of L is the determinant of any Gram matrix of L, viewed as an element in $\mathfrak{o}^*/\mathfrak{o}^{*,2}$.
(2) The abelian group $\mathfrak{g}(L) = \{\Phi(x, x) \mid x \in L\}$ is called the norm group of L and the norm $\mathfrak{n}(L)$ is the fractional $\mathfrak{o}$-ideal generated by $\mathfrak{g}(L)$. An element $a \in \mathfrak{g}(L)$ is called a norm generator of L if it generates the ideal $\mathfrak{n}(L)$.
(3) The weight $\mathfrak{w}(L)$ is defined as

$$\mathfrak{w}(L) = \pi\mathfrak{m}(L) + 2\mathfrak{o} ,$$

where $\mathfrak{m}(L)$ denotes the largest fractional $\mathfrak{o}$-ideal contained in $\mathfrak{g}(L)$.

By [8, Paragraph 93A], the norm and weight of a unimodular $\mathfrak{o}$-lattice L satisfy

$$2\mathfrak{o} \subseteq \mathfrak{w}(L) \subseteq \mathfrak{n}(L)$$

and $\mathfrak{w}(L) = 2\mathfrak{o}$ whenever $\mathrm{ord}(\mathfrak{n}(L)) + \mathrm{ord}(\mathfrak{w}(L))$ is even. Based on the above invariants, OMeara classified the isometry classes of unimodular $\mathfrak{o}$-lattices:

Theorem 3.6 (O'Meara)**.** *Let L_1, L_2 be unimodular $\mathfrak{o}$-lattices in the same bilinear space (V, Φ). Then L_1 and L_2 are isometric if and only if*

$$\mathfrak{g}(L_1) = \mathfrak{g}(L_2) .$$

Moreover, $\mathfrak{g}(L_i) = a_i\mathfrak{o}^2 + \mathfrak{w}(L_i)$ where a_i denotes a norm generator of L_i.

Proof. See [8, Theorem 93:16 and 93:4]. □

Using the above classification, one can write down Gram matrices for all isometry classes of unimodular $\mathfrak{o}$-lattices explicitly. To this end, let $\mathbb{H}$ be an hyperbolic plane, i.e. an $\mathfrak{o}$-lattice with Gram matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} .$$

Given any integer $r \geq 0$, we denote by $\mathbb{H}^r$ the orthogonal sum of r copies of $\mathbb{H}$.

Lemma 3.7. *Let L be a unimodular $\mathfrak{o}$-lattice of rank $2n$ with norm generator a and weight $\pi^b\mathfrak{o}$. Further, let $(-1)^n \det(L) = 1 + \alpha$ with $\mathfrak{d}((-1)^n \det(L)) = \alpha\mathfrak{o}$. Then L is isomeric to one of the following lattices.*

$$L_1 = \begin{pmatrix} a & 1 \\ 1 & -\alpha/a \end{pmatrix} \perp \mathbb{H}^{n-1} \quad \text{where } \pi^b = \mathfrak{d}(-\alpha)/a + 2\mathfrak{o},$$

$$L_2 = \begin{pmatrix} a & 1 \\ 1 & -\alpha/a \end{pmatrix} \perp \begin{pmatrix} \pi^b & 1 \\ 1 & 0 \end{pmatrix} \perp \mathbb{H}^{n-2} \quad \text{where } b < e,$$

$$L_3 = \begin{pmatrix} a & 1 \\ 1 & -(\alpha - 4\delta)/a \end{pmatrix} \perp \begin{pmatrix} \pi^b & 1 \\ 1 & -4\delta/\pi^b \end{pmatrix} \perp \mathbb{H}^{n-2} .$$

The second and third case only occur if $\mathrm{ord}(a) + b$ is odd. Moreover,

$$c(KL_i) = \begin{cases} +(1+\alpha, (-1)^{n-1}a)(-1,-1)^{n(n-1)/2} & \text{if } i = 1, 2, \\ -(1+\alpha, (-1)^{n-1}a)(-1,-1)^{n(n-1)/2} & \text{if } i = 3. \end{cases}$$

Proof. See [8, Examples 93:17 and 93:18] for details. The computation of the Hasse-Witt invariants follows by induction on n from [5, Lemma 2.3] and a lengthy computation with Hilbert symbols. The weight of L_1 can be computed using the method given in [8, Section 94]. $\square$

Corollary 3.8. *Let L be an even unimodular $\mathfrak{o}$-lattice. Then $\operatorname{rank}(L) = 2n$ is even and L is isometric to either*

$$\mathbb{H}^n \quad or \quad \begin{pmatrix} 2 & 1 \\ 1 & -2\delta \end{pmatrix} \perp \mathbb{H}^{n-1}\,. \tag{3.1}$$

In the first case, $\operatorname{disc}(KL) = 1$ and $c(KL) = (-1,-1)^{n(n-1)/2}$. In the second case, $\operatorname{disc}(KL) = \Delta$ and $c(KL) = (-1)^e \cdot (-1,-1)^{n(n-1)/2}$.

Proof. It is well known that L is an orthogonal sum of unary and binary sublattices, cf. [8, 93:15]. Since unary lattices are not even unimodular, the rank of L must be even, say $2n$. Theorem 3.6 shows that 2 is a norm generator of L because $\mathfrak{n}(L) = \mathfrak{w}(L) = 2\mathfrak{o}$. The result now follows from Lemma 3.7. $\square$

Lemma 3.9. *Let L be a unimodular lattice of rank $2n$ over $\mathfrak{o}$ with norm generator a and weight $\pi^b\mathfrak{o}$. Suppose that KL contains an even unimodular lattice. Then one of the following conditions holds.*

1. $\operatorname{disc}(KL) = 1$, $b = e$ *and* $L \cong \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \perp \mathbb{H}^{n-1}$.
2. $\operatorname{disc}(KL) = \Delta$, $b = e$, $\operatorname{ord}(a) + b$ *is even and*
$$L \cong \begin{pmatrix} a & 1 \\ 1 & -4\delta/a \end{pmatrix} \perp \mathbb{H}^{n-1}\,.$$
3. $\operatorname{disc}(KL) = 1$, $\operatorname{ord}(a) + b$ *is odd*, $b < e$ *and*
$$L \cong \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \perp \begin{pmatrix} \pi^b & 1 \\ 1 & 0 \end{pmatrix} \perp \mathbb{H}^{n-2}\,.$$
4. $\operatorname{disc}(KL) = \Delta$, $\operatorname{ord}(a) + b$ *is odd*, $\operatorname{ord}(a) + e$ *is even*, $b < e$ *and*
$$L \cong \begin{pmatrix} a & 1 \\ 1 & -4\delta/a \end{pmatrix} \perp \begin{pmatrix} \pi^b & 1 \\ 1 & 0 \end{pmatrix} \perp \mathbb{H}^{n-2}\,.$$
5. $\operatorname{disc}(KL) = \Delta$, $\operatorname{ord}(a) + b$ *is odd*, $b + e$ *is even*, $b < e$ *and*
$$L \cong \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \perp \begin{pmatrix} \pi^b & 1 \\ 1 & -4\delta/\pi^b \end{pmatrix} \perp \mathbb{H}^{n-2}\,.$$

Proof. By Corollary 3.8 either $\operatorname{disc}(KL) = 1$ and $c(KL) = (-1,-1)^{n(n-1)/2}$ or $\operatorname{disc}(KL) = \Delta$ and $c(KL) = (-1)^e \cdot (-1,-1)^{n(n-1)/2}$. The result now follows from Lemma 3.7. $\square$

The following result generalizes [2, Theorem 8.1].

Theorem 3.10. *Let (V, Φ) be a bilinear space of rank $2n$ over K. Let G be a subgroup of $\operatorname{SO}(V, \Phi)$. Then V contains a G-stable even unimodular $\mathfrak{o}$-lattice if and only if the following conditions hold:*

1. *(V, Φ) contains a G-stable unimodular $\mathfrak{o}$-lattice.*
2. *(V, Φ) contains an even unimodular $\mathfrak{o}$-lattice.*
3. *$\theta(G) \subseteq \mathfrak{o}^* K^{*,2}$.*

Proof. The first two conditions are certainly necessary. The necessity of the third condition follows from Theorem 3.1. Conversely suppose that G satisfies the three conditions. Then there exists some G-stable unimodular lattice L in (V, Φ). Let $L_{ev} = \{x \in L \mid \Phi(x,x) \in 2\mathfrak{o}\}$ be the maximal sublattice of L such that $\mathfrak{n}(L) \subseteq 2\mathfrak{o}$. Further let S_L be the set of all even unimodular lattices between L_{ev} and $(L_{ev})^{\#}$. The group G acts on S_L. We claim that every lattice in S_L is actually G-stable. To this end, it suffices to show that S_L satisfies the following two conditions:

(1) $\#S_L \in \{1, 2\}$.
(2) If $S_L = \{M_1, M_2\}$ consists of two lattices, then the spinor norm of some (and thus any) proper isometry between M_1 and M_2 lies in $\pi\mathfrak{o}^* K^{*,2}$.

Since L is unimodular, $\mathfrak{n}(L) = \pi^i\mathfrak{o}$ for some $0 \le i \le e$. The above claim is clear if $i = e$. Suppose now $i < e$. After rescaling the form Φ with some element of $\mathfrak{o}^*$, we may assume that π^i is a norm generator of L. Further, let $\pi^b\mathfrak{o}$ be the weight of L. We distinguish the five cases of Lemma 3.9.

Suppose that L is as in the first two cases of Lemma 3.9. Then $L \cong L_1 \perp L_2$ where $L_2 \cong \mathbb{H}^{n-1}$ is hyperbolic and L_1 has a basis (x, y) with Gram matrix

$$\begin{pmatrix} \pi^i & 1 \\ 1 & \varepsilon/\pi^i \end{pmatrix}$$

with $\varepsilon \in \{0, -4\delta\}$ and $\varepsilon = 0$ whenever $e \not\equiv i \pmod 2$. Write $k := \lceil (e-i)/2 \rceil \ge 1$, then

$$L_{ev} = (\pi^k x\mathfrak{o} \oplus y\mathfrak{o}) \perp L_2 \quad \text{and} \quad (L_{ev})^{\#} = (x\mathfrak{o} \oplus \pi^{-k} y\mathfrak{o}) \perp L_2 \,.$$

Let $M \in S_L$. Then $\pi^k x \in L_{ev} \subseteq M$ is a primitive vector of M. Hence there exists some $v \in M \subseteq L_{ev}^{\#}$ such that $\Phi(\pi^k x, v) = 1$. Without loss of generality, $v = \lambda x + \pi^{-k} y$ with $\lambda \in \mathfrak{o}$. The condition $\Phi(v,v) \in 2\mathfrak{o}$ shows that

$$\lambda^2\pi^i + 2\lambda\pi^{-k} \equiv 0 \pmod{\pi^e}$$

or equivalently

$$\lambda^2 + \frac{2}{\pi^e}\lambda\pi^{e-i-k} \equiv 0 \pmod{\pi^{e-i}}\,. \tag{3.2}$$

Suppose first $e \equiv i \pmod 2$, then $2k = e - i$. Comparing valuations, we see that eq. (3.2) implies $\lambda \in \pi^k\mathfrak{o}$. Since $\pi^k x \in L_{ev}$, we have $\pi^{-k} y \in M$. Hence $M = M_1 := L_{ev} + \pi^{-k} y\mathfrak{o}$. So $S_L = \{M_1\}$.
Suppose now $e \not\equiv i \pmod 2$. Then $\varepsilon = 0$ and $2k = e - i + 1$. In this case, eq. (3.2) holds if either $\lambda \in \pi^k\mathfrak{o}$ or $\lambda \equiv -2\pi^{k-e-1} \pmod{\pi^k}$. So in this case, $S = \{M_1,\ M_2\}$ where $M_2 := L_{ev} + (2\pi^{k-e-1}x - \pi^{-k}y)\mathfrak{o}$. It remains to construct a proper isometry between M_1 and M_2. For this, we may assume that $n = 1$, i.e. the lattices have rank 2. Further, let $x' = \pi^{k-1}x$, $y' = \pi^{1-k}y$ and $z' = x' - \pi^{e-1}/2y'$. Then

$$\begin{aligned} M_1 &= \pi x'\mathfrak{o} \oplus y'/\pi\mathfrak{o} = \pi z'\mathfrak{o} \oplus y'/\pi\mathfrak{o}\,, \\ M_2 &= \pi x'\mathfrak{o} + \pi^{k-1}y'\mathfrak{o} + z'\mathfrak{o} = z'\mathfrak{o} \oplus y'\mathfrak{o}\,. \end{aligned}$$

From $\Phi(z', z') = 0 = \Phi(y', y')$ and $\Phi(z', y') = 1$ it follows that the K-linear map $\varphi \colon KM_1 \to KM_1$ with $\varphi(z') = z'/\pi$ and $\varphi(y') = \pi y'$ is a proper isometry from M_1 to M_2. Lemma 2.1 shows that $\theta(\varphi) \equiv \pi \pmod{K^{*,2}}$.

Suppose now that L is as in the last three cases of Lemma 3.9. Then $L = L_1 \perp L_2$ where L_2 is hyperbolic and L_1 has a basis (x, y, z, w) with Gram matrix

$$\begin{pmatrix} \pi^i & 1 & 0 & 0 \\ 1 & \varepsilon_1/\pi^i & 0 & 0 \\ 0 & 0 & \pi^b & 1 \\ 0 & 0 & 1 & \varepsilon_2/\pi \end{pmatrix}$$

with $i < b \le e$, $i + b$ is odd and $\varepsilon_i \in \{0, -4\delta\}$ such that $\varepsilon_1 = 0$ if $e \not\equiv i \pmod 2$ and $\varepsilon_2 = 0$ if $e \not\equiv b \pmod 2$. We will reduce this case to the one before. To this end, let $k := \lceil (e-i)/2 \rceil$ and $\ell := \lceil (e-b)/2 \rceil$. Then

$$L_{ev} = (\pi^k x\mathfrak{o} \oplus y\mathfrak{o}) \perp (\pi^\ell z\mathfrak{o} \oplus w\mathfrak{o}) \perp L_2 ,$$
$$(L_{ev})^\# = (x\mathfrak{o} \oplus \pi^{-k} y\mathfrak{o}) \perp (z\mathfrak{o} \oplus \pi^{-\ell} w\mathfrak{o}) \perp L_2 .$$

We will not make use of the fact that $i < b$. So after exchanging the parameters i and b, we may assume that $b + 2\ell = e$ and $i + 2k = e + 1$. Then $\varepsilon_1 = 0$. Let $M \in S_L$ and suppose

$$v = \lambda x + \mu\pi^{-k} y + \nu z + \tau\pi^{-\ell} w \in M \quad \text{where } \lambda, \mu, \nu, \tau \in \mathfrak{o} .$$

Let $\alpha = \lambda^2\pi^i + 2\lambda\mu\pi^{-k}$ and $\beta = \nu^2\pi^b + 2\nu\tau\pi^{-\ell} + \tau^2\varepsilon_2\pi^{-e}$. Then

$$\alpha + \beta = \Phi(v, v) \in 2\mathfrak{o} .$$

If $\mathrm{ord}(\nu) < \ell$, then $\mathrm{ord}(\beta) = 2\mathrm{ord}(\nu) + b \le e - 2$. Further, $\mathrm{ord}(\alpha) = 2\mathrm{ord}(\lambda) + i$ if $\mathrm{ord}(\lambda) \le k-2$ and $\mathrm{ord}(\alpha) \ge e-1$ otherwise. Since $i \not\equiv b \pmod 2$ we conclude from $\alpha + \beta \in 2\mathfrak{o}$ that $\mathrm{ord}(\nu) \ge \ell$. Hence $M \subseteq Y := (x\mathfrak{o} + \pi^{-k} y\mathfrak{o} + \pi^\ell z\mathfrak{o} + \pi^{-\ell} w\mathfrak{o}) \perp L_2$. Thus

$$M \supseteq Y^\# = (\pi^{-k} x\mathfrak{o} + y\mathfrak{o} + \pi^\ell z\mathfrak{o} + \pi^{-\ell} w\mathfrak{o}) \perp L_2 .$$

This shows that $S_L \subseteq S_X$ where $X = (x\mathfrak{o} \oplus y\mathfrak{o}) \perp (z\pi^\ell\mathfrak{o} \oplus \pi^{-\ell} w\mathfrak{o}) \perp L_2$ is a unimodular lattice as in part (1) or (2) of Lemma 3.9. We have already seen that S_X satisfies the above claim and so does S_L. □

As a consequence of Theorem 3.10 one obtains the following dyadic analog of Proposition 3.2.

Proposition 3.11. *Suppose that K is dyadic,* $\mathrm{ord}(S(-1)) \in 2\mathbb{Z}$ *and that*

$$(-1)^{\deg(S)/2} S(1)S(-1) \cdot K^{*,2} \in \{K^{*,2},\ \Delta \cdot K^{*,2}\} .$$

Then there exists some $\lambda \in \mu(E, \sigma)$ such that (E, b_λ) contains an α-stable even unimodular $\mathfrak{o}$-lattice.

Proof. The proof of [2, Proposition 9.1] applies mutatis mutandis. □

4. Proof of Theorem A

First we show that the conditions of Theorem A are necessary. To this end, let L be an even unimodular $\mathfrak{o}$-lattice as in the Theorem and let (V, Φ) be its ambient bilinear space. Further, let φ be a proper automorphism of L and let $v \in \Omega(K)$ be finite. Conditions (C1) and (C2) are necessary by [6, Section 1 and Proposition A.1]. Theorem 3.1 shows that the fractional ideal $\theta(\pm\varphi)\mathfrak{o}_v$ is a square. By Lemma 2.1, the ideal $S(\pm 1)\mathfrak{o}_v$ is also a square. Hence condition (C3) is necessary. If $v \in \Omega_r(K)$, then $\mathrm{disc}(V_v, \Phi) = (-1)^{n+s_v}$. Similarly, if $v \in \Omega_2(K)$, then $\mathrm{disc}(V_v, \Phi)$ is either 1 or Δ_v, cf. Corollary (3.8). But $\mathrm{disc}(V, \Phi) = (-1)^n S(1)S(-1)$, cf. Lemma 2.2. This shows that (C4) and (C5) are necessary. The local Hasse-Witt invariants of (V,Φ) are given as follows:

$$c(V_v,\Phi) = \begin{cases} (-1)^{s_v(s_v-1)/2} & \text{if } v \in \Omega_r(K), \\ (-1,-1)_v^{n(n-1)/2} & \text{if } v \in \Omega_2(K) \text{ and } \operatorname{disc}(V_v,\Phi)=1, \\ (-1)^{e_v}\cdot(-1,-1)_v^{n(n-1)/2} & \text{if } v \in \Omega_2(K) \text{ and } \operatorname{disc}(V_v,\Phi)\neq 1, \\ 1 & \text{otherwise.} \end{cases} \tag{4.1}$$

For infinite places this is clear. For finite places, it follows from Lemma 3.8 and [8, 92:1 and 63:11a]. Let

$$c_1 = \#\{v \in \Omega_r(K) \mid n(n-1) \not\equiv s_v(s_v-1) \pmod 4\}$$
$$c_2 = \#\{v \in \Omega_2(K) \mid e_v \text{ is odd and } (-1)^n S(1)S(-1) \notin K_v^{*,2}\}$$

be the cardinalities of the two sets from (C6). The product formula for Hilbert symbols shows that

$$1 = \prod_{v\in\Omega(K)} c(V_v,\Phi) = (-1)^{c_1+c_2}\cdot \prod_{v\in\Omega(K)} (-1,-1)^{n(n-1)/2} = (-1)^{c_1+c_2}\,. \tag{4.2}$$

Thus condition (C6) is necessary.

We now show that the conditions are sufficient. To this end, we follow Section 10 of [2] closely.

For $v \in \Omega(K)$ let c_v be the Hasse-Witt invariant given by eq. (4.1). Eq. (4.2) shows that (C6) is equivalent to $\prod_v c_v = 1$. By [8, Theorem 72:1] there exists a bilinear space (V,Φ) over K such that

(1) (V,Φ) has rank $2n$ and discriminant $(-1)^n S(1)S(-1)$.
(2) For $v \in \Omega_r(K)$, the space (V_v,Φ) has signature (r_v,s_v).
(3) For $v \in \Omega(K)$, the Hasse-Witt invariant of (V_v,Φ) is c_v.

The polynomial P is assumed to be non-linear and reciprocal. Let α be the image of t in the field $F := K[t]/(P)$. Then there exists a unique K-linear automorphism σ of F with $\sigma(\alpha) = \alpha^{-1}$. Let $F_0 \neq F$ be the fixed field of σ. Let E_0 be a field extension of F_0 in some algebraic closure of F of degree $2n/\deg(P)$ which is linearly disjoint from F. Then the compositum $E := FE_0$ is a field extension of K of degree $2n$ and S is the characteristic polynomial of $\alpha \in E$ over K. Further, σ extends to E by setting $\sigma|_{E_0} = \mathrm{id}_{E_0}$.

Let v be a place of K and let w be a place of E_0 over v. Let $E_w = E \otimes_{E_0} E_{0,w}$ and write α_w for the image of α in E_w.
If v is real, there are three possibilities:

(1) $E_{0,w} \cong \mathbb{R}$ and $E_w \cong \mathbb{R}\times\mathbb{R}$. Then $\alpha_w = (x, 1/x)$ with $x \in \mathbb{R}^*$ and $|x| \neq 1$.
(2) $E_{0,w} \cong \mathbb{C}$ and $E_w \cong \mathbb{C}\times\mathbb{C}$. Then $\alpha_w = (x,1/x)$ with $x \in \mathbb{C}^*\setminus\mathbb{R}^*$ and $|x| \neq 1$.
(3) $E_{0,w} \cong \mathbb{R}$ and $E_w \cong \mathbb{C}$. Then $|\alpha_w| = 1$.

In the first two cases, (E_w, b_λ) has signature (d,d) where $d = \dim_{\mathbb{R}}(E_{0,w})$ for any $\lambda \in \mu(E_w,\sigma)$. The last case occurs $n - m_v(S)$ times. By (C2), the quotients

$$d_{v,+} := \frac{r_v - m_v(S)}{2} \quad\text{and}\quad d_{v,-} := \frac{s_v - m_v(S)}{2}$$

are integral and non-negative. Hence there exists some

$$\lambda_v \in \prod_{w|v} \mu(E_w, \sigma)$$

such that $\lambda_w = +1$ at exactly $d_{v,+}$ places of the third type and $\lambda_w = -1$ at exactly $d_{v,-}$ places of the third type. Thus (E_v, b_{λ_v}) has signature (r_v, s_v).
Suppose now that v is finite. Conditions (C3) and (C4) as well as Propositions 3.2 and 3.11 imply that there exists some

$$\lambda_v \in \prod_{w|v} \mu(E_w, \sigma)$$

such that (E_v, b_{λ_v}) contains an α-stable even unimodular $\mathfrak{o}$-lattice.

For any place v of K, the spaces (V_v, Φ) and (E_v, b_{λ_v}) are isometric since they have the same rank, discriminant and Hasse-Witt invariant. By [4, Theorem 4.3] this implies that

$$\varepsilon_v(V_v, \Phi) = \varepsilon_v(E_v, b_{\lambda_v}) = \varepsilon_v(E_v, b_1) + \beta_v(\lambda_v) \, .$$

Here $\beta_v(\lambda_v) := \sum_{w|v} \operatorname{Cor}_{E_{0,w}/K_v}(\beta_w(\lambda_w))$ where $\beta_w \colon \mu(E_w, \sigma) \to \operatorname{Br}(E_{0,w})$ is given by eq. (2.2) and $\operatorname{Cor}_{E_{0,w}/K_v} \colon \operatorname{Br}(E_{0,w}) \to \operatorname{Br}(K_v)$ denotes the corestriction map. Since (V, Φ) and (E, b_1) are bilinear K-spaces, we have $\operatorname{inv}_v(\varepsilon_v(V_v, \Phi)) = \operatorname{inv}_v(\varepsilon_v(E_v, b_{\lambda_v})) = 0$ almost everywhere and

$$\sum_v \operatorname{inv}_v(\varepsilon_v(V_v, \Phi)) = \sum_v \operatorname{inv}_v(\varepsilon_v(E_v, b_{\lambda_v})) = 0 \, .$$

Hence $\operatorname{inv}_v(\beta_v(\lambda_v)) = 0$ almost everywhere and $\sum_v \operatorname{inv}_v(\beta_v(\lambda_v)) = 0$. The commutative diagram

$$\begin{array}{ccc} \operatorname{Br}(E_{0,w}) & \xrightarrow{\operatorname{inv}_w} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \operatorname{Cor}_{E_{0,w}/K_v}} \downarrow & & \downarrow {\scriptstyle \operatorname{id}} \\ \operatorname{Br}(K_v) & \xrightarrow{\operatorname{inv}_v} & \mathbb{Q}/\mathbb{Z} \end{array}$$

shows that $\sum_w \operatorname{inv}_w(\beta_w(\lambda_w)) = 0$. Let $\varphi_w \colon \mu(E_w, \sigma) \cong \operatorname{Br}(E_w, E_{0,w}) \cong \mathbb{Z}/2\mathbb{Z}$ be an isomorphism. Then $\sum_w \operatorname{inv}_w(\beta_w(\lambda_w)) = 0$ implies $\sum_w \varphi_w(\lambda_w) = 0$. Theorem 5.7 of [2] shows that there exists some $\lambda \in \mu(E, \sigma)$ which specializes to the chosen elements λ_w locally everywhere. Thus (E, b_λ) is isometric to (V, Φ). Now multiplication by $\alpha \in E$ induces an isometry on (E, b_λ) with characteristic polynomial S. Further, at every place v of K there exists some α-stable even unimodular $\mathfrak{o}_v$-lattice M_v. Let $\mathcal{O}$ be the ring of integers of E, then we can choose $\mathcal{O}_v = M_v$ almost everywhere. Hence there exists some $\mathfrak{o}$-lattice L in E such that $L_v = M_v$ locally everywhere. This finishes the proof of Theorem A.

Remark 4.1. For $K = \mathbb{Q}$, Theorem A implies [2, Theorem A]. This means that for $K = \mathbb{Q}$, the six conditions of Theorem A are equivalent to the following conditions:

(C0) $r_\infty \equiv s_\infty \pmod 8$.
(C1) S is reciprocal.
(C2) $m_\infty(S) \le \min(r_\infty, s_\infty)$ and $m_\infty(S) \equiv r_\infty \equiv s_\infty \pmod 2$.
(C3') $|S(1)|$, $|S(-1)|$ and $(-1)^n S(1) S(-1)$ are squares.

Proof. For brevity, we write r and s for r_∞ and s_∞. Suppose first, that S, n, r, s satisfy the conditions (C1)–(C6) of Theorem A. Condition (C3) implies that $|S(\pm 1)|$ is a square. We claim that $(-1)^n S(1)S(-1)$ is also a square. If not, then $(-1)^{n+1} S(1)S(-1)$ must be square and hence $(-1)^{n+1}S(1)S(-1) \in \mathbb{Q}_2^{*,2}$. This contradicts (C4) since $\Delta_2 \equiv 5 \not\equiv -1 \pmod{\mathbb{Q}_2^{*,2}}$. Hence (C3') holds. From (C4) we know that $(-1)^s S(1)S(-1) \in \mathbb{Q}_2^{*,2}$. Thus $(r+s)/2 = n \equiv s \pmod 2$ and hence $r = s + 4k$ for some integer k. Since the second set in (C6) is empty, so must be the first. This implies $s(s-1) \equiv n(n-1) \equiv (s+2k)(s+2k-1) \pmod 4$. Hence k is even and thus (C0) holds.

Conversely, if S, n, r, s satisfy (C0)–(C2) and (C3'), then (C3)–(C6) hold trivially. □

References

[1] Eva Bayer-Fluckiger. Isometries of quadratic spaces. *J. Eur. Math. Soc. (JEMS)*, 17(7):1629–1656, 2015.

[2] Eva Bayer-Fluckiger and Lenny Taelman. Automorphisms of even unimodular lattices and equivariant Witt groups. arXiv:1708.05540 [math.NT].

[3] Constantin N. Beli. Integral spinor norm groups over dyadic local fields. *J. Number Theory*, 102(1):125–182, 2003.

[4] R. Brusamarello, P. Churad-Koulmann, and J. Morales. Orthogonal groups containing a given maximal torus. *J. Algebra*, 266(1):87–101, 2003.

[5] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press, 1978.

[6] B. H. Gross and C. T. McMullen. Automorphisms of even unimodular lattices and unramified Salem numbers. *J. Algebra*, 257(2):265–290, 2002.

[7] M. Kneser. Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen. *Arch. Math. (Basel)*, 7:323–332, 1956.

[8] O. T. O'Meara. *Introduction to Quadratic Forms*. Springer, 1973.

[9] H. Zassenhaus. On the spinor norm. *Arch. Math.*, 13:434–451, 1962.

Email address: `markus.kirschmer@math.rwth-aachen.de`

Lehrstuhl B für Mathematik, RWTH Aachen University, Pontdriesch 10–16, 52062 Aachen, Germany