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 [4] 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 [1] 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 [6, Section 63:A] 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.*

1. *S is reciprocal, i.e. $t^{2n}S(1/t) = S(t)$.*
2. *$m_v(S) \le \min(r_v, s_v)$ and $m_v(S) \equiv r_v \equiv s_v \pmod 2$ for all $v \in \Omega_r(K)$.*
3. *$S(1)\mathfrak{o}$ and $S(-1)\mathfrak{o}$ are squares.*
4. *$(-1)^n S(1)S(-1) \cdot (K_v^*)^2 \in \{(K_v^*)^2,\ \Delta_v \cdot (K_v^*)^2\}$ for all $v \in \Omega_2(K)$.*
5. *$(-1)^{s_v} S(1)S(-1) \in K_v$ is positive for all $v \in \Omega_r(K)$.*
6. *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.

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

If $K = \mathbb{Q}$, the conditions of Theorem A imply the well known facts that $r_\infty \equiv s_\infty \pmod 8$ and the determinant of L is $S(1)S(-1) = (-1)^n$. So in this special case, the above result simplifies to Theorem A in [1].

Note that these two facts do not hold for arbitrary fields K. For example, let $K = \mathbb{Q}(\sqrt{5})$ and let L be the even unimodular $\mathfrak{o}$-lattice with Gram matrix

$$\begin{pmatrix} 2 & 1-\sqrt{5} \\ 1-\sqrt{5} & 6 \end{pmatrix} .$$

The determinant of this matrix is the fundamental unit $u = 2\sqrt{5}+5$. Hence $\pm u$ is not a square. 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. Some notation

A bilinear space (V,Φ) is a finite-dimensional vector space V over a field 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 following elements of $K^*/(K^*)^2$

$$\det(V,\Phi) = \det(B) \cdot (K^*)^2 \quad \text{and} \quad \operatorname{disc}(V,\Phi) = (-1)^n \cdot \det(B) \cdot (K^*)^2$$

are called the determinant and the discriminant of (V,Φ) respectively. 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 $\theta(\tau_v) = \Phi(v,v) \cdot K^*/(K^*)^2$ for all anisotropic vectors $v \in V$.

The following result is well known. For example, [4, Proposition A.3] provides a proof in the case that S is square-free.

Lemma 2.1. *Let K be a field of characteristic different from 2 and 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 $S(1)S(-1) \in K^*$ represents $\det(V,\Phi)$.*

Proof. Zassenhaus' method to compute spinor norms [8] shows that

$$\begin{aligned} \theta(\alpha) &= \det((1+\alpha)/2) \cdot (K^*)^2 = S(-1) \cdot (K^*)^2 , \\ \theta(-\alpha) &= \det((1-\alpha)/2) \cdot (K^*)^2 = S(+1) \cdot (K^*)^2 , \\ \theta(-1) &= \det(V,\Phi) . \end{aligned}$$

The result follows since θ is a group homomorphism. $\square$

Let $\mathfrak{o}$ be a Dedekind ring with field of fractions K. 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 K be an algebraic number field or a completion thereof. Further, 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 E is a field. Then the elements of the Brauer groups of E and E_0 are represented by cyclic algebras, see for example [7] for details. Hence $\mu(E, \sigma)$ is isomorphic to the relative Brauer group $\mathrm{Br}(E/E_0)$. So there exists some short exact sequence

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

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 $\mathrm{ord} \colon K \to \mathbb{Z} \cup \{\infty\}$ be the usual discrete valuation of K.

Theorem 3.1. *Let (V, Φ) 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 [5, Satz 3] in the case that $\mathrm{ord}(2) = 0$. The case $\mathrm{ord}(2) > 0$ is solved by Beli in [2, 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.

If K is non-dyadic, i.e. $2 \in \mathfrak{o}^*$ then Bayer-Fluckiger and Taelman prove the following result.

Proposition 3.2. *Let K be non-dyadic. If $S(1)$ and $S(-1)$ are non-zero and have even valuations, then there exists some $\lambda \in \mu(E, \sigma)$ such that (E, b_λ) contains an α-stable unimodular $\mathfrak{o}$-lattice.*

Proof. See Proposition 7.1 of [1]. □

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. We extend this classification to any ramification index e. The result is heavily based on O'Meara's classification of unimodular lattices over $\mathfrak{o}$. Any unexplained notation is taken from O'Meara's book [6]. Let $\Delta \in \mathfrak{o}^*$ be a unit of quadratic defect $4\mathfrak{o}$. This means that $\Delta \notin (\mathfrak{o}^*)^2$ but Δ is a square modulo $4\mathfrak{o}$. Equivalently, $K(\sqrt{\Delta})$ is the unique unramified quadratic extension of K. In particular, the square class $\Delta(\mathfrak{o}^*)^2$ is uniquely determined. After multiplying with a unit square, we may assume that $\Delta = 1 + 4\delta$ for some unit $\delta \in \mathfrak{o}^*$.

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 $\mathbb{H}$.

Suppose now that L is an even unimodular $\mathfrak{o}$-lattice. O'Meara's classification [6, Section 93] shows that $\operatorname{rank}(L) = 2n$ is even and L isometric to either

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

The discriminant of the ambient bilinear space KL is $(K^*)^2$ or $\Delta \cdot (K^*)^2$ respectively.

Lemma 3.3. *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 $0 \leq \operatorname{ord}(a) \leq b \leq e$ and one of the following conditions holds.*

(1) $\operatorname{disc}(KL) = (K^*)^2$, *$b = e$ and* $L \cong \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \perp \mathbb{H}^{n-1}$.

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

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

(4) $\operatorname{disc}(KL) = \Delta \cdot (K^*)^2$, $\operatorname{ord}(a) + b$ *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) $\operatorname{disc}(KL) = \Delta \cdot (K^*)^2$, $\operatorname{ord}(a) + b$ *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. This follows from O'Meara's classification of unimodular lattices, see [6, Section 93]. □

The following result generalizes [1, Theorem 8.1].

Theorem 3.4. *Let (V, Φ) be a bilinear space of rank $2n$ over K. Let G be a subgroup of $\mathrm{SO}(V, \Phi)$. 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 $e = i$. 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 3.3.

Suppose that L is as in the first case of Lemma 3.3. 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

$$\begin{pmatrix} \pi^i & 1 \\ 1 & 0 \end{pmatrix} .$$

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 $2k = e - i + 1$. 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. Let $\tau_{z'-\pi y'}$ and $\tau_{z'-y'}$ be the reflections as in eq. (2.1). One checks that $\varphi = \tau_{z'-\pi y'} \circ \tau_{z'-y'}$. Hence

$$\theta(\varphi) = \Phi(z' - \pi y', z' - \pi y')\Phi(z' - y', z' - y')(K^*)^2 = \pi(K^*)^2 .$$

Suppose now that L is as in the second case of Lemma 3.3. 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

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

with $i < b \le e$ and $i + b$ is odd. 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

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

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 $i + 2k = e + 1$. 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 $\beta = \nu^2\pi^b + 2\nu\tau\pi^{-\ell}$. Then

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

If $\operatorname{ord}(\nu) < \ell$, then $\operatorname{ord}(\beta) = 2\operatorname{ord}(\nu) + b \le e - 2$. Further, $\operatorname{ord}(\alpha) = 2\operatorname{ord}(\lambda) + i$ if $\operatorname{ord}(\lambda) \le k - 2$ and $\operatorname{ord}(\alpha) \ge e - 1$ otherwise. Since $i \not\equiv b \pmod 2$ we conclude from $\alpha + \beta \in 2\mathfrak{o}$ that $\operatorname{ord}(\nu) \ge \ell$. 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) of Lemma 3.3. We have already seen that S_X satisfies the above claim and so does S_L.

The cases where $\operatorname{disc}(KL) = \Delta \cdot (K^*)^2$ are handled similarly. We leave the details to the reader. □

As a consequence of Theorem 3.4 one obtains the following dyadic analog of Proposition 3.2.

Proposition 3.5. *Assume that K is dyadic,* $\operatorname{ord}(S(-1)) \in 2\mathbb{Z}$ *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 [1, Proposition 9.1] applies mutatis mutandis. □

4. Proof of Theorem A

First we show that the conditions of Theorem A are necessary. Conditions (1) and (2) are necessary by [4, Section 1 and Proposition A.1]. The third condition is necessary by Theorem 3.1 while Lemma 2.1 and equation 3.1 show the necessity of (4) and (5). Let L be an even unimodular lattice as in the theorem and let (V, Φ) be the ambient bilinear space of L. Given any diagonal Gram matrix $\operatorname{diag}(a_1, \dots, a_{2n})$ of (V, Φ) and a place v of K set

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

where $(.,.)_v$ denotes the Hilbert symbol over K_v. The integer $c_v(V, \Phi)$ is (a version of) the Hasse-Witt invariant of (V_v, Φ). One checks that

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

The product formula for Hilbert symbols shows that $1 = \prod_v c_v(V, \Phi)$. Condition (6) is an immediate consequence of this product formula.

We now show that the conditions are sufficient. To this end, we follow Section 10 of [1] closely.

Conditions (3)–(6) imply that there exists some bilinear space (V, Φ) over K such that

(1) (V, Φ) has rank $2n$ and discriminant $(-1)^n S(1)S(-1) \cdot (K^*)^2$.

(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 invariant $c_v(m, \Phi)$ is given by eq. (4.1).

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 the algebraic closure of K 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 (2), 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 (3) and (4) as well as Propositions 3.2 and 3.5 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. In particular, the spaces have the same Clifford invariant $\varepsilon_v(V_v, \Phi) \in \mathrm{Br}(K_v)$. By [3, 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 $\beta_v(\lambda_v) := \sum_{w|v} \mathrm{Cor}_{E_{0,w}/K_v}(\beta_w(\lambda_w))$ where $\beta_w \colon \mu(E_w, \sigma) \to \mathrm{Br}(E_{0,w})$ is given by eq. (2.2) and $\mathrm{Cor}_{E_{0,w}/K_v} \colon \mathrm{Br}(E_{0,w}) \to \mathrm{Br}(K_v)$ denotes the corestriction map. Let $\mathrm{inv}_v \colon \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ be the usual Hasse invariant. Since (V, Φ) and (E, b_1) are bilinear K-spaces, we have $\mathrm{inv}_v(\varepsilon_v(V_v, \Phi)) = \mathrm{inv}_v(\varepsilon_v(E_v, b_{\lambda_v})) = 0$ almost everywhere and

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

Hence $\mathrm{inv}_v(\beta_v(\lambda_v)) = 0$ almost everywhere and $\sum_v \mathrm{inv}_v(\beta_v(\lambda_v)) = 0$. This shows that $\sum_w \mathrm{inv}_w(\beta_w(\lambda_w)) = 0$ since the corestriction map is characterized by the fact that it preserves Hasse invariants. Let $\varphi_w \colon \mu(E_w, \sigma) \cong \mathrm{Br}(E_w, E_{0,w}) \cong \mathbb{Z}/2\mathbb{Z}$ be an isomorphism. Then $\sum_w \mathrm{inv}_w(\beta_w(\lambda_w)) = 0$ implies that $\sum_w \varphi_w(\lambda_w) = 0$. Theorem 5.7 of [1] 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.

References

[1] E. Bayer-Fluckiger and L. Taelman. Automorphisms of even unimodular lattices and equivariant Witt groups. arXiv:1708.05540 [math.NT].
[2] C. N. Beli. Integral spinor norm groups over dyadic local fields. *J. Number Theory*, 102(1):125–182, 2003.
[3] R. Brusamarello, P. Churad-Koulmann, and J. Morales. Orthogonal groups containing a given maximal torus. *J. Algebra*, 266(1):87–101, 2003.
[4] B. H. Gross and C. T. McMullen. Automorphisms of even unimodular lattices and unramified Salem numbers. *J. Algebra*, 257(2):265–290, 2002.
[5] M. Kneser. Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen. *Arch. Math. (Basel)*, 7:323–332, 1956.
[6] O. T. O'Meara. *Introduction to Quadratic Forms*. Springer, 1973.
[7] I. Reiner. *Maximal Orders*, volume 28 of *LMS Monographs*. Oxford Science Publications, 2003.
[8] H. Zassenhaus. On the spinor norm. *Arch. Math.*, 13:434–451, 1962.

Lehrstuhl B für Mathematik, RWTH Aachen University, Pontdriesch 10-16, 52062 Aachen, Germany
E-mail address: markus.kirschmer@math.rwth-aachen.de