



## UvA-DARE (Digital Academic Repository)

### Automorphisms of even unimodular lattices and equivariant Witt groups

Bayer-Fluckiger, E.; Taelman, L.

**DOI**

[10.4171/JEMS/991](https://doi.org/10.4171/JEMS/991)

**Publication date**

2020

**Document Version**

Final published version

**Published in**

Journal of the European Mathematical Society

[Link to publication](#)

**Citation for published version (APA):**

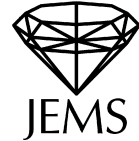
Bayer-Fluckiger, E., & Taelman, L. (2020). Automorphisms of even unimodular lattices and equivariant Witt groups. *Journal of the European Mathematical Society*, 22(11), 3467-3490. <https://doi.org/10.4171/JEMS/991>

**General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.



Eva Bayer-Fluckiger · Lenny Taelman

# Automorphisms of even unimodular lattices and equivariant Witt groups

Received September 13, 2017

**Abstract.** We characterize the irreducible polynomials that occur as the characteristic polynomial of an automorphism of an even unimodular lattice of a given signature, generalizing a theorem of Gross and McMullen. As part of the proof, we give a general criterion in terms of Witt groups for a bilinear form equipped with an action of a group  $G$  over a discretely valued field to contain a unimodular  $G$ -stable lattice.

**Keywords.** Even unimodular lattices, automorphisms, Witt group

## 1. Introduction

### 1.1. Statement of the main result

Let  $r$  and  $s$  be non-negative integers, and let  $\Lambda$  be an even unimodular lattice of signature  $(r, s)$ . Such a lattice exists if and only if  $r \equiv s \pmod{8}$ , and it is uniquely determined by  $(r, s)$  if  $r$  and  $s$  are non-zero. Let  $\alpha \in \mathrm{SO}(\Lambda)$  and denote by  $S$  its characteristic polynomial. Denote by  $m(S)$  be the number of complex roots  $z$  of  $S$  with  $|z| > 1$  (counted with multiplicity). Gross and McMullen [10] show that if  $S$  has no linear factor, then

- (C1)  $S$  is reciprocal (i.e.  $t^{r+s}S(1/t) = S(t)$ ),
- (C2)  $m(S) \leq r$ ,  $m(S) \leq s$  and  $m(S) \equiv r \equiv s \pmod{2}$ ,
- (C3)  $|S(1)|$ ,  $|S(-1)|$  and  $(-1)^{(r+s)/2}S(1)S(-1)$  are squares.

They speculate that for a monic irreducible  $S \in \mathbb{Z}[t]$  of degree  $r + s$ , the above conditions may be *sufficient* for the existence of an even unimodular lattice  $\Lambda$  of signature  $(r, s)$  and an  $\alpha \in \mathrm{SO}(\Lambda)$  with characteristic polynomial  $S$ . They show that this is indeed so if  $|S(1)| = |S(-1)| = 1$  (a different proof was given by the first author in [3]). The main result of this paper confirms their speculation:

**Theorem A.** *Let  $r, s$  be non-negative integers satisfying  $r \equiv s \pmod{8}$ . Let  $P$  be a monic irreducible polynomial, and let  $S$  be a power of  $P$ . Assume that  $S$  has degree  $r + s$ , and*

E. Bayer-Fluckiger: EPFL, Department of Mathematics, CH-1015 Lausanne, Switzerland;  
e-mail: eva.bayer@epfl.ch

L. Taelman: UvA, KdVI, PO Box 94248, 1090 GE Amsterdam, the Netherlands;  
e-mail: l.d.j.taelman@uva.nl

*Mathematics Subject Classification (2020):* 11H56, 11E81

that it satisfies (C1)–(C3). Then there exists an even unimodular lattice  $\Lambda$  of signature  $(r, s)$  and an  $\alpha \in \mathrm{SO}(\Lambda)$  with characteristic polynomial  $S$ .

Gross and McMullen have observed [10, Prop. 5.2] that the theorem does not hold for  $S$  that have distinct irreducible factors. There are results by the first author on reducible characteristic polynomials of *definite* even unimodular lattices [1, 2], but in general it is not even clear what to conjecture.

As in [10, §8] and [14, Thm. 3.4], Theorem A together with the Torelli theorem for K3 surfaces has the following immediate consequence.

**Corollary.** *Let  $S \in \mathbb{Z}[t]$  be a monic, irreducible, reciprocal polynomial of degree 22. Assume that  $S$  has precisely one root  $z \in \mathbb{C}$  with  $|z| > 1$ , and assume that  $|S(1)|$ ,  $|S(-1)|$  and  $-S(1)S(-1)$  are squares. Then there exists a complex analytic K3 surface  $X$  and an  $\alpha \in \mathrm{Aut} X$  such that the characteristic polynomial of  $\alpha^*$  on  $H^2(X, \mathbb{Z})$  is  $S$ .  $\square$*

## 1.2. Strategy of proof

We sketch the proof of Theorem A, and refer to the main body of the paper for the details. Assume for simplicity that  $S$  is irreducible.

Let  $E = \mathbb{Q}[t]/(S)$  and let  $\alpha \in E$  be the class of  $t$ . By condition (C1), the field  $E$  comes with an involution  $\sigma$  characterized by  $\sigma(\alpha) = \alpha^{-1}$ . Let  $E_0 \subset E$  be the fixed field under  $\sigma$ . For every  $\lambda \in E_0^\times$  we have a symmetric  $\mathbb{Q}$ -bilinear form

$$b_\lambda : E \times E \rightarrow \mathbb{Q}, \quad (x, y) \mapsto \mathrm{tr}_{E/\mathbb{Q}}(\lambda x \sigma(y)),$$

and  $\alpha$  acts on  $(E, b_\lambda)$  by isometries. Condition (C2) guarantees that for suitable  $\lambda$  the form  $b_\lambda$  will have signature  $(r, s)$ . If we can moreover choose  $\lambda$  in such a way that  $b_\lambda$  contains an  $\alpha$ -stable even unimodular lattice, then the theorem follows.

Gross and McMullen show that if  $|S(1)| = |S(-1)| = 1$ , then for suitable  $\lambda$  the lattice  $\Lambda$  can be taken to be a fractional  $\mathcal{O}_E$ -ideal. In general, however, an  $\alpha$ -stable lattice  $\Lambda$  will only be a module over the order  $\mathbb{Z}[\alpha^{\pm 1}] \subset \mathcal{O}_E$ , severely complicating the situation at places where  $\mathbb{Z}[\alpha^{\pm 1}]$  fails to be maximal.

We take a somewhat different approach. We first show that for every  $p$  there are  $\lambda$  in  $(\mathbb{Q}_p \otimes E_0)^\times$  for which there exists a unimodular  $\alpha$ -stable  $\mathbb{Z}_p$ -lattice  $\Lambda_p$  in  $(\mathbb{Q}_p \otimes E, b_\lambda)$ . This is done by showing that under condition (C3) we can make the obstruction class in an ‘equivariant Witt group’ over  $\mathbb{F}_p$  vanish (see §1.3 below). A careful analysis at the prime 2 shows that one can moreover arrange for the  $\mathbb{Z}_2$ -lattice  $\Lambda_2$  to be even.

Thus, we can solve the problem locally. To finish the proof, it suffices to show that there exists a global  $\lambda$  satisfying the local conditions (at finite and infinite places). This is the case if and only if a certain local-global obstruction class in  $\mathbb{Z}/2\mathbb{Z}$  vanishes. It appears to be hard to compute the individual contributions to this obstruction directly, but we observe that the obstruction class can be realized as the difference of two obstruction classes coming from global objects, and hence that it must vanish. See §10 for more details.

1.3. Local obstructions in equivariant Witt groups

Let  $K$  be a field and  $G$  a group. We define a  $G$ -bilinear form to be a finite-dimensional  $K$ -linear representation  $V$  of  $G$  equipped with a non-degenerate  $G$ -invariant symmetric bilinear form  $V \times V \rightarrow K$ . We say  $V$  is *neutral* if there exists a  $G$ -stable subspace  $X \subset V$  with  $X = X^\perp$ . The *equivariant Witt group*  $W_G(K)$  is the quotient of the Grothendieck group of  $G$ -bilinear forms by the subgroup generated by the classes of neutral forms. If the group  $G$  is trivial, then  $W_G(K)$  coincides with the usual Witt group  $W(K)$ . In §3 we develop the basic properties of these equivariant Witt groups, in the slightly more general (and more natural) context of  $\epsilon$ -symmetric bilinear forms over a ring with involution.

Now let  $K$  be the fraction field of a discrete valuation ring  $\mathcal{O}_K$  with uniformizer  $\pi$  and residue field  $k$ . We call an  $\mathcal{O}_K$ -lattice  $\Lambda$  in a  $K$ -bilinear form  $V$  *almost unimodular* if

$$\pi \Lambda^\vee \subset \Lambda \subset \Lambda^\vee.$$

If  $V$  is a  $G$ -bilinear form over  $K$  and if  $\Lambda \subset V$  is almost unimodular and  $G$ -stable, then the quotient  $\Lambda^\vee/\Lambda$  equipped with the form

$$\frac{\Lambda^\vee}{\Lambda} \times \frac{\Lambda^\vee}{\Lambda} \xrightarrow{b} \frac{\pi^{-1}\mathcal{O}_K}{\mathcal{O}_K} \xrightarrow{\pi} k$$

is a  $G$ -bilinear form over  $k$ .

We call a  $G$ -bilinear form  $V$  *bounded* if  $V$  contains a  $G$ -stable  $\mathcal{O}_K$ -lattice, or equivalently if the closure of the image of  $G$  in  $O(V)$  is compact. We denote by  $W_G^b(K)$  the subgroup of  $W_G(K)$  generated by the bounded forms.

**Theorem B.** *Let  $K$  be the fraction field of a discrete valuation ring  $\mathcal{O}_K$  with residue field  $k$ , and fix a uniformizer  $\pi$  of  $\mathcal{O}_K$ . Let  $G$  be a group. Then*

- (i) every bounded  $G$ -bilinear form  $V$  contains an almost unimodular  $G$ -stable lattice  $\Lambda$ ,
- (ii) the class of  $[\Lambda^\vee/\Lambda]$  in  $W_G(k)$  only depends on the class of  $V$  in  $W_G(K)$ ,
- (iii) the map  $\partial: W_G^b(K) \rightarrow W_G(k)$  given by  $[V] \mapsto [\Lambda^\vee/\Lambda]$  is a homomorphism,
- (iv) a  $G$ -bilinear form  $V$  contains a  $G$ -stable unimodular  $\mathcal{O}_K$ -lattice if and only if  $V$  is bounded and  $\partial[V] = 0$  in  $W_G(k)$ .

As in our treatment of equivariant Witt groups, we show this in a slightly more general context (see Theorem 4.3). This theorem can be seen as an equivariant version of a theorem of Springer [20] (but see Remark 4.12), or of the theory of discriminant forms of Nikulin [15]. The result is without doubt well-known to experts, but for lack of proper reference we include a complete proof in Sections 3 and 4. See also [19], [23], and [22] where similar ideas are used.

If the residue field  $k$  is finite and  $G$  is the infinite cyclic group, then the group  $W_G(k)$  and the map  $\partial$  can be made reasonably explicit. We use this in the proof of Theorem A to show (using the notation of §1.2) that there is no local obstruction to finding a  $\lambda \in E_0^\times$  and a unimodular  $\Lambda \subset (E, b_\lambda)$ , stable under  $\alpha$  (see Propositions 7.1 and 7.2).

If  $K = \mathbb{Q}_2$ , then we use the spinor norm to refine the theorem into a necessary and sufficient condition for a  $G$ -bilinear form to contain a  $G$ -invariant *even* unimodular  $\mathbb{Z}_2$ -lattice (see Theorem 8.1, and its application in Proposition 9.1).

The full strength of Theorem B is not needed for the application in Theorem A, and one could make do with a few ad hoc computations in the spirit of the proof of Theorem B. However, we have included it since it helps keeping the argument organized, and since we believe Theorem B may be a useful tool in working with ‘ $G$ -lattices’, playing a role similar to Nikulin’s theory for lattices without group action.

## 2. Conventions

The *determinant*  $\det b$  of a non-degenerate symmetric bilinear form  $b$ , considered as an element of  $K^\times/(K^\times)^2$ , is the determinant of any Gram matrix of  $b$ . The *discriminant*  $\text{disc } b \in K^\times/(K^\times)^2$  is defined as

$$\text{disc } b := (-1)^{n(n-1)/2} \det b,$$

where  $n$  is the dimension of  $V$ . The discriminant of a hyperbolic form is trivial.

## 3. The equivariant Witt group

Let  $K$  be a field and  $A$  an (associative, unital)  $K$ -algebra. Let  $\sigma : A \rightarrow A$  be an involution. We will refer to the algebra with involution  $(A, \sigma)$  simply by  $A$ . Fix an  $\epsilon$  in  $\{\pm 1\}$ .

**Definition 3.1.** An  $(A, \epsilon)$ -bilinear form is a pair  $(V, b)$  consisting of an  $A$ -module  $V$  of finite  $K$ -dimension and a non-degenerate  $K$ -bilinear form  $b : V \times V \rightarrow K$  satisfying

- (i)  $b(ax, y) = b(x, \sigma(a)y)$  for all  $a \in A$  and  $x, y \in V$ ,
- (ii)  $b(x, y) = \epsilon b(y, x)$  for all  $x, y \in V$ .

We will sometimes suppress  $b$  and denote an  $(A, \epsilon)$ -bilinear form by  $V$ .

**Example 3.2.** In the proof of Theorem A only pairs  $(A, \epsilon)$  of the following kind will be considered. Let  $G$  be a group,  $A = K[G]$ , and  $\sigma$  the involution of  $A$  satisfying  $\sigma(g) = g^{-1}$  for all  $g \in G$ . In this case, an  $(A, +1)$ -bilinear form is the same as a non-degenerate symmetric bilinear form  $b : V \times V \rightarrow K$  together with an action  $\varrho : G \rightarrow \text{O}(V, b)$ . We will also refer to such a triple  $(V, b, \varrho)$  as a  $G$ -bilinear form.

**Definition 3.3.** Let  $V$  be an  $(A, \epsilon)$ -bilinear form. If  $X \subset V$  is an  $A$ -submodule, then its *orthogonal*  $X^\perp = \{x \in V \mid b(x, V) = 0\}$  is also an  $A$ -submodule. A *lagrangian* is an  $A$ -submodule  $X \subset V$  satisfying  $X = X^\perp$ . We say that  $V$  is *neutral* if it has a lagrangian. The group  $W_A^\epsilon(K)$  is defined as the quotient of the Grothendieck group of  $(A, \epsilon)$ -bilinear forms by the subgroup generated by the neutral forms.

If  $A = K[G]$  and  $\epsilon = 1$  then we will write  $W_G(K)$  for  $W_A^\epsilon(K)$ .

**Remark 3.4.** If  $A = K$  and  $\epsilon = 1$  then  $W_A^\epsilon(K)$  coincides with the usual Witt group of bilinear forms,  $W(K)$ . Indeed, if  $X \subset V$  satisfies  $X = X^\perp$  then  $V$  is isomorphic to  $X \oplus X^\vee$  equipped with the obvious bilinear form, and  $V$  is hyperbolic (or metabolic in characteristic 2).

**Remark 3.5.** The decomposition  $V \cong X \oplus X^\vee$  in the preceding remark is not canonical, and in general, if  $X$  is a lagrangian in an  $(A, \epsilon)$ -bilinear form  $V$  then the natural short exact sequence of  $A$ -modules

$$0 \rightarrow X \rightarrow V \rightarrow X^\vee \rightarrow 0$$

need not split.

If  $V = (V, b)$  is an  $(A, \epsilon)$ -bilinear form, then we denote by  $V(-1)$  the scaled  $(A, \epsilon)$ -bilinear form  $(V, -b)$ .

**Lemma 3.6.**  $V \oplus V(-1)$  is neutral.

*Proof.* The submodule  $\{(x, x) \mid x \in V\}$  is a lagrangian. □

**Corollary 3.7.** Every element of  $W_A^\epsilon(K)$  is of the form  $[V]$  for some  $V$ . □

**Lemma 3.8.** If  $X \subset V$  is an  $A$ -submodule and satisfies  $X \subset X^\perp$ , then  $[V] = [X^\perp/X]$  in  $W_G(K)$ .

*Proof.* The submodule  $\{(x, \bar{x}) \mid x \in X^\perp\}$  is a lagrangian in  $V(-1) \oplus X^\perp/X$ . □

**Proposition 3.9.**  $[V] = 0$  in  $W_A^\epsilon(K)$  if and only if  $V$  is neutral.

*Proof.* If  $V$  is neutral then  $[V] = 0$  by definition of  $W_A^\epsilon(K)$ .

Conversely, assume that  $[V] = 0$ . Then there exists a  $W$  and a neutral  $N$  such that  $V \oplus W \cong N \oplus W$ . Adding a summand  $W(-1)$  we find that there exists a neutral  $M$  such that  $V \oplus M$  is neutral.

Let  $2n$  be the dimension of  $V$ , and  $2m$  the dimension of  $M$ . Let  $X \subset V \oplus M$ , and  $Y \subset M$  be lagrangians. Consider the submodule

$$S := X \cap (V \times Y) \subset V \oplus M.$$

We have  $X + (V \times Y) \subset (X \cap Y)^\perp$ , so that

$$\dim X + \dim(V \times Y) \leq \dim S + \dim(X \cap Y)^\perp.$$

Expressing everything in terms of  $n, m, \dim S$  and  $\dim(X \cap Y)$  gives

$$(n + m) + (2n + m) \leq \dim S + (2n + 2m - \dim(X \cap Y)),$$

and hence  $\dim S - \dim(X \cap Y) \geq n$ . Now the subspace  $Z := \pi_V(S) \subset V$  is a totally isotropic  $A$ -submodule. The kernel of the projection  $S \rightarrow Z$  is  $X \cap Y$ , so we have

$$\dim Z = \dim S - \dim(X \cap Y) \geq n,$$

and therefore  $Z$  is a lagrangian. □

The following proposition is analogous to the diagonalizability of quadratic forms over fields.

**Proposition 3.10.** *The group  $W_A^\epsilon(K)$  is generated by the classes of  $(A, \epsilon)$ -bilinear forms  $(V, b)$  with  $V$  a simple  $A$ -module.*

*Proof.* Let  $W^{ss} \subset W_A^\epsilon(K)$  be the subgroup generated by the classes of forms on simple  $A$ -modules. Let  $[V]$  be an element of  $W_A^\epsilon(K) \setminus W^{ss}$  with  $\dim_K V$  minimal.

Since  $V$  is not simple, it contains a proper submodule  $W$ . Consider the submodule  $X = W \cap W^\perp$  of  $V$ . Either  $X = \{0\}$  and then  $[V] = [W] + [W^\perp]$ , or  $X \neq \{0\}$  and then  $[V] = [X^\perp/X]$ . In both cases we obtain a contradiction with the minimality of  $\dim V$ . □

**Corollary 3.11.** *Every class in  $W_A^\epsilon(K)$  is represented by an  $(A, \epsilon)$ -bilinear form whose underlying  $A$ -module is semisimple.* □

If  $M$  is a simple  $A$ -module, then we denote by  $W_A^\epsilon(K, M)$  the subgroup of  $W_A^\epsilon(K)$  generated by the classes of  $(A, \epsilon)$ -bilinear forms  $(M, b)$ .

**Theorem 3.12.**  $W_A^\epsilon(K) = \bigoplus_M W_A^\epsilon(K, M)$  where  $M$  ranges over the isomorphism classes of simple  $A$ -modules.

*Proof.* By Proposition 3.10 the map  $\bigoplus_M W_A^\epsilon(K, M) \rightarrow W_A^\epsilon(K)$  is surjective. Let  $([V_M])_M$  be an element of the kernel. Then by Proposition 3.9 there is a lagrangian  $X \subset \bigoplus_M V_M$ , and since  $\text{Hom}_A(M_1, M_2) = 0$  whenever  $M_1 \not\cong M_2$  we find that  $X$  decomposes as  $X = \bigoplus_M X_M$ . For every  $M$  the submodule  $X_M \subset V_M$  is a lagrangian, and we conclude that the map is injective. □

### 4. Equivariant forms over discrete valuation rings

#### 4.1. Statement of the result

Throughout this section,  $\mathcal{O}_K$  is a discrete valuation ring with field of fractions  $K$ , residue field  $k$ , and uniformizer  $\pi$ . Let  $(A, \sigma)$  be an  $\mathcal{O}_K$ -algebra with involution and write  $A_K$  and  $A_k$  for  $A \otimes_{\mathcal{O}_K} K$  and  $A \otimes_{\mathcal{O}_K} k$  respectively. To lighten notation, we will write  $W_A^\epsilon(K)$  for  $W_{A_K}^\epsilon(K)$  and similarly  $W_A^\epsilon(k)$  for  $W_{A_k}^\epsilon(k)$ .

We will be particularly interested in the case  $A = \mathcal{O}_K[G]$  with  $\epsilon = 1$ , in which case we have  $W_A^\epsilon(K) = W_G(K)$  and  $W_A^\epsilon(k) = W_G(k)$ .

**Definition 4.1.** An  $A$ -lattice in an  $(A_K, \epsilon)$ -bilinear form  $V$  is an  $A$ -submodule  $\Lambda$  which is finitely generated as an  $\mathcal{O}_K$ -module and satisfies  $K\Lambda = V$ . If  $\Lambda$  is an  $A$ -lattice, then so is its dual

$$\Lambda^\vee := \{x \in V \mid b(x, \Lambda) \subset \mathcal{O}_K\}.$$

We say that  $\Lambda$  is *almost unimodular* if  $\pi \Lambda^\vee \subset \Lambda \subset \Lambda^\vee$ , and *unimodular* if  $\Lambda = \Lambda^\vee$ .

If  $\Lambda$  is almost unimodular, then  $\Lambda^\vee/\Lambda$  equipped with the pairing

$$\Lambda^\vee/\Lambda \times \Lambda^\vee/\Lambda \xrightarrow{b} \frac{\pi^{-1}\mathcal{O}_K}{\mathcal{O}_K} \xrightarrow{\pi} k$$

is an  $(A_k, \epsilon)$ -bilinear form.

**Definition 4.2.** We say that an  $(A_K, \epsilon)$ -bilinear form is *bounded* if it contains an  $A$ -lattice. We denote by  $W_A^{\epsilon,b}(K)$  the subgroup of  $W_A^\epsilon(K)$  generated by the classes of bounded forms.

In this section we prove the following theorem, which for  $A = \mathcal{O}_K[G]$  and  $\epsilon = 1$  coincides with Theorem B.

- Theorem 4.3.** (i) *Every bounded  $(A_K, \epsilon)$ -bilinear form contains an almost unimodular  $A$ -lattice  $\Lambda$ .*  
 (ii) *The class of  $\Lambda^\vee/\Lambda$  in  $W_A^\epsilon(k)$  only depends on the class of  $V$  in  $W_A^\epsilon(K)$ .*  
 (iii) *The map  $\partial: W_A^{\epsilon,b}(K) \rightarrow W_A^\epsilon(k)$  given by  $[V] \mapsto \Lambda^\vee/\Lambda$  is a homomorphism.*  
 (iv)  *$V$  contains a unimodular  $A$ -lattice if and only if  $V$  is bounded and  $\partial[V] = 0$  in  $W_A^\epsilon(k)$ .*

We closely follow the proof of [17, §6.1], which treats the case  $A = \mathcal{O}_K, \epsilon = 1$ .

4.2. *Torsion forms and proof of Theorem 4.3*

**Definition 4.4.** An  $(A, \epsilon)$ -bilinear torsion form  $M$  is a pair  $(M, b)$  consisting of

- (i) an  $A$ -module  $M$  of finite length over  $\mathcal{O}_K$ ,
- (ii) a non-degenerate  $\mathcal{O}_K$ -bilinear map  $b: M \times M \rightarrow K/\mathcal{O}_K$  satisfying  $b(x, y) = \epsilon b(y, x)$  and  $b(ax, y) = b(x, \sigma(a)y)$  for all  $x, y \in M$  and  $a \in A$ .

A *lagrangian* in  $M$  is an  $A$ -submodule  $X \subset M$  with  $X = X^\perp$ . We say that  $M$  is *neutral* if  $M$  has a lagrangian.

If  $V$  is an  $(A_K, \epsilon)$ -bilinear form and  $\Lambda \subset V$  an  $A$ -lattice satisfying  $\Lambda \subset \Lambda^\vee$ , then  $M := \Lambda^\vee/\Lambda$  is naturally an  $(A, \epsilon)$ -bilinear torsion form (sometimes called the discriminant form of  $\Lambda$ ). The  $A$ -lattices  $\Lambda'$  satisfying

$$\Lambda \subset \Lambda' \subset \Lambda^{\vee\vee} \subset \Lambda^\vee$$

are in bijection with the totally isotropic  $A$ -submodules  $M' \subset M$ , and  $\Lambda'$  is almost unimodular (resp. unimodular) if and only if  $\pi M'^\perp \subset M'$  (resp.  $M'$  is a lagrangian).

**Proposition 4.5.** *Let  $M$  be an  $(A, \epsilon)$ -bilinear torsion form. Then every maximal totally isotropic  $A$ -submodule  $U \subset M$  satisfies  $\pi U^\perp \subset U$ .*

*Proof.* Let  $U \subset M$  be a maximal totally isotropic submodule. Let  $t$  be the largest integer such that  $\pi^{t-1}U^\perp/U \neq 0$ . Assume  $t \geq 2$  and set  $V := \pi^{t-1}U^\perp + U$ . Then  $V$  is an  $A$ -submodule, and we claim that it is totally isotropic. Indeed, if  $x \in U^\perp$  and  $y \in U$  then

$$b(\pi^{t-1}x + y, \pi^{t-1}x + y) = b(\pi^t x, \pi^{t-2}x) = 0,$$

since  $\pi^t x \in U$ . This contradicts the maximality of  $U$ . □

**Corollary 4.6.** *Let  $V$  be an  $(A_K, \epsilon)$ -bilinear form. Then any maximal  $A$ -lattice in  $V$  is almost unimodular.* □



**Corollary 4.7.** *Let  $V$  be a bounded  $(A, \epsilon)$ -bilinear form over  $K$ . Then  $V$  has an almost unimodular  $A$ -lattice.  $\square$*

The latter corollary also follows from [19, Thm. 3.1.1].

We denote by  $WT_A^\epsilon(\mathcal{O}_K)$  the Witt group of  $(A, \epsilon)$ -bilinear torsion forms, defined as the quotient of the Grothendieck group of  $(A, \epsilon)$ -bilinear torsion forms by the subgroup generated by the classes of the neutral forms.

If  $V$  is an  $A_k$ -bilinear form, then the composition

$$V \times V \rightarrow k \xrightarrow{\pi^{-1}} \frac{K}{\mathcal{O}_K}$$

makes  $V$  into an  $(A, \epsilon)$ -bilinear torsion form over  $\mathcal{O}_K$ . This defines a homomorphism  $W_A^\epsilon(k) \rightarrow WT_A^\epsilon(\mathcal{O}_K)$ .

**Proposition 4.8.** *The map  $W_A^\epsilon(k) \rightarrow WT_A^\epsilon(\mathcal{O}_K)$  is an isomorphism.*

*Proof.* For  $A = \mathcal{O}_K = \mathbb{Z}_p$ , this is [17, 5.1.5]. The argument carries over to our setting; we repeat it for the convenience of the reader.

For a non-zero finite length  $\mathcal{O}_K$ -module  $M$ , we call the smallest integer  $t$  such that  $\pi^t M = 0$  but  $\pi^{t-1} M \neq 0$  the *exponent* of  $M$ .

Let  $M$  be an  $(A, \epsilon)$ -bilinear torsion form of exponent  $t \geq 2$ . Then  $U := \pi^{t-1} M$  is totally isotropic, and the  $(A, \epsilon)$ -bilinear form  $M' := U^\perp/U$  has exponent  $< t$  and we have  $[M] = [M']$  in  $WT_A(\mathcal{O}_K)$ . Repeating this process, we find a canonical  $(A, \epsilon)$ -bilinear torsion form  $M^\dagger$  of exponent 1 (i.e. killed by  $\pi$ ).

Note that  $(M \oplus N)^\dagger = M^\dagger \oplus N^\dagger$ . Also, if  $M$  is neutral with lagrangian  $X \subset M$  then

$$X' := \frac{X \cap U^\perp}{X \cap U} \subset \frac{U^\perp}{U} = M'$$

is lagrangian, since

$$(X \cap U^\perp)^\perp \cap U^\perp = (X + U) \cap U^\perp = (X \cap U^\perp) + U$$

and hence  $X'$  is its own orthogonal in  $U^\perp/U$ . This shows that  $M \mapsto M^\dagger$  induces a two-sided inverse to  $W_A^\epsilon(k) \rightarrow WT_A(\mathcal{O}_K)$ .  $\square$

**Lemma 4.9.** *If  $\Lambda_0$  and  $\Lambda_1$  are  $A$ -lattices in  $V$  satisfying  $\Lambda_0 \subset \Lambda_0^\vee$  and  $\Lambda_1 \subset \Lambda_1^\vee$ , then  $[\Lambda_0^\vee/\Lambda_0] = [\Lambda_1^\vee/\Lambda_1]$  in  $WT_A^\epsilon(\mathcal{O}_K)$ .*

*Proof.* Passing to the intersection, we may without loss of generality assume  $\Lambda_0 \subset \Lambda_1$ . Let  $M = \Lambda_0^\vee/\Lambda_1$ . Then the image  $U$  of  $\Lambda_0$  in  $M$  is totally isotropic, and  $U^\perp/U \cong \Lambda_1^\vee/\Lambda_1$ . The same argument as in the proof of 3.8 shows that  $[M] = [U^\perp/U]$  and hence  $[\Lambda_0^\vee/\Lambda_0] = [\Lambda_1^\vee/\Lambda_1]$  in  $WT_A(\mathcal{O}_K)$ .  $\square$

Let  $b: V \times V \rightarrow K$  be a non-degenerate bilinear form. For an  $\mathcal{O}_K$ -submodule  $L$  of  $V$  (not necessarily a lattice) we define

$$L^\vee := \{x \in V \mid b(x, L) \subset \mathcal{O}_K\}.$$

The main properties of the dual of a lattice carry over to this generality:

**Lemma 4.10.** *For all  $\mathcal{O}_K$ -submodules  $L, M$  of a bilinear form  $V$  we have*

- (i) *if  $L$  is a  $K$ -vector subspace, then  $L^\vee = L^\perp$ ,*
- (ii)  *$(L^\vee)^\vee = L$ ,*
- (iii)  *$(L + M)^\vee = L^\vee \cap M^\vee$ ,*
- (iv)  *$(L \cap M)^\vee = L^\vee + M^\vee$ .*

*Proof.* For (i), note that  $b(x, \lambda y) \in \mathcal{O}_K$  for all  $\lambda \in K$  implies  $b(x, y) = 0$ .

The second assertion is clear if  $L$  is a  $K$ -vector subspace, or an  $\mathcal{O}_K$ -lattice. For a general  $L$ , note that there exist unique  $K$ -vector subspaces  $V_0$  and  $V_1$  such that  $V_0 \subset L \subset V_1$  and  $L/V_0$  is a lattice in  $V_1/V_0$ . The dual  $L^\vee$  satisfies  $V_1^\perp \subset L^\vee \subset V_0^\perp$ , with  $L^\vee/V_1^\perp$  the dual lattice of  $L/V_0$  under the perfect pairing

$$V_1/V_0 \times V_0^\perp/V_1^\perp \rightarrow K$$

induced by  $b$ . Consequently, the double dual of  $L$  coincides with  $L$ .

The third assertion is immediate, and the final one follows from the third using the double dual statement in (ii). □

**Lemma 4.11.** *If  $V$  is a neutral  $A_K$ -bilinear form, and if  $\Lambda \subset V$  is an  $A$ -lattice satisfying  $\Lambda \subset \Lambda^\vee$ , then  $\Lambda^\vee/\Lambda$  is a neutral torsion  $A$ -bilinear form.*

*Proof.* Let  $X \subset V$  be a lagrangian, and set

$$U := \frac{X \cap \Lambda^\vee}{X \cap \Lambda} \subset \frac{\Lambda^\vee}{\Lambda}.$$

Then using Lemma 4.10, we see that  $U^\perp \subset \Lambda^\vee/\Lambda$  satisfies

$$U^\perp = \frac{(X^\perp + \Lambda) \cap \Lambda^\vee}{(X^\perp + \Lambda) \cap \Lambda} = \frac{X \cap \Lambda^\vee}{X \cap \Lambda} = U,$$

and we conclude that  $U$  is a lagrangian in  $\Lambda^\vee/\Lambda$ . □

We are now ready to prove the main result of this section.

*Proof of Theorem 4.3.* Part (i) is Corollary 4.7. By Lemmas 4.9 and 4.11 the map  $[V] \mapsto [\Lambda^\vee/\Lambda]$  is a well-defined homomorphism. Composing with the inverse of the isomorphism of Proposition 4.8 we obtain (ii) and (iii). Assertion (iv) then follows from Proposition 3.9. □

**Remark 4.12.** If  $V = (V, b)$  is an  $(A, \epsilon)$ -bilinear form over  $K$ , then so is  $V(\pi) := (V, \pi b)$ . We obtain a map

$$W_A^\epsilon(K) \rightarrow W_A^\epsilon(k) \times W_A^\epsilon(k), \quad [V] \mapsto (\partial[V], \partial[V(\pi)]).$$

If  $K$  is complete,  $A = \mathcal{O}_K$  and  $\epsilon = 1$ , then this is precisely the isomorphism  $W(K) \rightarrow W(k) \times W(k)$  of Springer [20].

In general, however, the map fails to be an isomorphism. For example, if  $G$  is a  $p$ -group and  $K = \mathbb{Q}_p$ , then under the isotypical decomposition of Theorem 3.12 the group

$W_G(\mathbb{Q}_p)$  can have many non-trivial components (corresponding to the irreducible symmetrically self-dual representations of  $G$  over  $\mathbb{Q}_p$ ), whereas  $W_G(\mathbb{F}_p) = W(\mathbb{F}_p)$ .

For an explicit example, take  $p = 2$ , and  $G = \mathbb{Z}/2\mathbb{Z}$  acting on the hyperbolic plane  $H$  over  $\mathbb{Q}_2$  by interchanging the two isotropic lines. Then  $[H]$  is a non-zero element in the kernel of  $W_G(\mathbb{Q}_2) \rightarrow W_G(\mathbb{F}_2) \times W_G(\mathbb{F}_2)$ .

**Remark 4.13.** Let  $M$  be a bounded simple  $A_K$ -module and  $\Lambda \subset M$  an  $A$ -lattice. Let  $\overline{M}_1, \dots, \overline{M}_n$  be the (distinct) simple  $A_k$ -modules that occur as quotients in a Jordan–Hölder filtration of  $\Lambda/\pi\Lambda$ . Then under the decomposition of Theorem 3.12 the map  $\partial$  restricts to a map

$$W_A^\epsilon(K, M) \rightarrow \bigoplus_{i=1}^n W_A^\epsilon(k, \overline{M}_i).$$

Moreover, one can use the theory of Morita equivalence of [13, §I.9] to compute the groups  $W_A^\epsilon(k, \overline{M}_i)$  in terms of the usual Witt groups  $W(k)$ . Especially when  $k$  is finite, this gives quite a bit of control over the map  $\partial : W_A^\epsilon(K) \rightarrow W_A^\epsilon(k)$ , and makes it plausible that Theorem 4.3 will find applications beyond its use in the proof of Theorem A.

### 4.3. Sketch of a CAT(0)-proof

Since it may be of independent interest, we briefly sketch a different, more geometric proof of Theorem B, based on ideas of Goldman–Iwahori [9] and Bruhat–Tits [5, 6]. The argument does not seem to generalize to the more general setting of Theorem 4.3.

Let  $V$  be a finite-dimensional vector space over a discretely valued field  $K$ . A *valuation* on  $V$  is a map  $\alpha : V \rightarrow \mathbb{R} \cup \{\infty\}$  satisfying

- (i)  $\alpha(x) = \infty$  if and only if  $x = 0$ ,
- (ii)  $\alpha(ax) = v(a) + \alpha(x)$  for all  $a \in K, x \in V$ ,
- (iii)  $\alpha(x + y) \geq \inf\{\alpha(x), \alpha(y)\}$  for all  $x, y \in V$ .

If  $\alpha$  is a valuation on  $V$ , then

$$\alpha^\vee(\xi) := \inf_{x \in V} (v(\xi(x)) - \alpha(x))$$

defines a valuation on  $V^\vee$ . If  $b : V \times V \rightarrow K$  is a bilinear form, then we say that  $\alpha$  is *reflexive* if  $\alpha = \alpha^\vee$  under the identification  $V \cong V^\vee$  defined by  $b$ .

Let  $\mathcal{B}(V, b)$  be the set of all reflexive valuations on  $(V, b)$ . A *metric* on  $\mathcal{B}(V, b)$  is given by

$$d(\alpha, \beta) := \sup_{x \in V} |\beta(x) - \alpha(x)|.$$

Using the results of [9] and [5, §1] one can show that the metric space  $\mathcal{B}(V, b)$  is a CAT(0)-space. In particular, it is complete and uniquely geodesic. The group  $O(V, b)$  acts isometrically on  $\mathcal{B}(V, b)$ , and if the residue characteristic is different from 2, then one can identify  $\mathcal{B}(V, b)$  with the spherical Bruhat–Tits building of  $SO(V, b)$  (see [6, Thm. 2.12]).

Let  $\mathcal{L}(V, b)$  be the set of almost unimodular lattices in  $V$ . We have  $O(V, b)$ -equivariant maps

$$\begin{aligned} \mathcal{B}(V, b) &\rightarrow \mathcal{L}(V, b), & \alpha &\mapsto \Lambda_\alpha := \{x \in V \mid \alpha(x) \geq 0\}, \\ \mathcal{L}(V, b) &\rightarrow \mathcal{B}(V, b), & \Lambda &\mapsto \alpha_\Lambda := (x \mapsto \inf \{v(\pi^n x) \mid \pi^n x \in \Lambda\}). \end{aligned}$$

The first map is *semicontinuous* in the following sense: every  $\alpha \in \mathcal{B}(V, b)$  has an open neighbourhood  $U$  such that for all  $\beta \in U$  we have  $\Lambda_\beta \subset \Lambda_\alpha$ . The first map is a section of the second: for all almost unimodular lattices  $\Lambda$  we have  $\Lambda_{\alpha_\Lambda} = \Lambda$ .

*Sketch of alternative proof of Theorem B.* We only give the proof of the hardest part: that  $[\Lambda^\vee/\Lambda] \in W_G(k)$  is independent of  $\Lambda$ . Let  $(V, b, \varrho)$  be a  $G$ -bilinear form over  $K$ , and let  $\Lambda_0$  and  $\Lambda_1$  be almost unimodular  $G$ -lattices in  $V$ . If  $\Lambda_0$  and  $\Lambda_1$  are comparable ( $\Lambda_0 \subset \Lambda_1$  or  $\Lambda_1 \subset \Lambda_0$ ), then it is easy to see that  $[\Lambda_0^\vee/\Lambda_0] = [\Lambda_1^\vee/\Lambda_1]$  in  $W_G(k)$ .

Otherwise, since  $\mathcal{B}(V, b)$  is  $\text{CAT}(0)$ , there exists a unique geodesic

$$\alpha : [0, 1] \rightarrow \mathcal{B}(V, b), \quad t \mapsto \alpha_t,$$

such that  $\alpha_0 = \alpha_{\Lambda_0}$  and  $\alpha_1 = \alpha_{\Lambda_1}$ . By uniqueness,  $\alpha_t$  is fixed by  $G$  for all  $t$ , and hence  $\Lambda_{\alpha_t}$  is an almost unimodular  $G$ -lattice for all  $t$ . By semicontinuity (and compactness of  $[0, 1]$ ), we find a finite sequence  $(\Lambda_{t_i})_i$  of almost unimodular  $G$ -lattices with  $\Lambda_{t_0} = \Lambda_0$ ,  $\Lambda_{t_1} = \Lambda_1$ , and with  $\Lambda_{t_i}$  and  $\Lambda_{t_{i+1}}$  comparable for all  $i$ . □

In similar spirit, the existence of almost unimodular  $G$ -lattices (Corollary 4.7) can be deduced from the Bruhat–Tits fixed point theorem on  $\mathcal{B}(V, b)$ .

### 5. One-dimensional hermitian forms and the twisting group $\mu(E, \sigma)$

The remainder of this paper is about  $\mathbb{Z}$ -bilinear forms, that is, symmetric bilinear forms  $(V, b)$  equipped with an action  $\varrho : \mathbb{Z} \rightarrow O(V, b)$  of the infinite cyclic group  $\mathbb{Z}$ .

We begin by recalling the ‘hermitian’ construction of  $\mathbb{Z}$ -bilinear forms, and describe the local-global obstruction that will play a crucial role in the proof of Theorem A. All material in this section is well-known.

#### 5.1. Hermitian construction of $\mathbb{Z}$ -bilinear forms

Let  $K$  be a field of characteristic different from 2, let  $E_0$  be an étale  $K$ -algebra, and let  $E$  be an étale  $E_0$ -algebra that is free of rank 2 over  $E_0$ . Let  $\sigma$  denote the canonical involution of  $E$ , fixing  $E_0$ . Every  $\lambda \in E_0^\times$  defines a symmetric bilinear form

$$b_\lambda : E \times E \rightarrow K, \quad (x, y) \mapsto \text{tr}_{E/K}(\lambda x \sigma(y)).$$

If  $\alpha \in E^\times$  satisfies  $\alpha \sigma(\alpha) = 1$ , then multiplication by  $\alpha$  is an isometry of  $(E, b_\lambda)$ , and the homomorphism

$$\varrho_\alpha : \mathbb{Z} \rightarrow O(E, b_\lambda), \quad 1 \mapsto \alpha,$$

makes  $(E, b_\lambda, \varrho_\alpha)$  into a  $\mathbb{Z}$ -bilinear form.

5.2. *The twisting group*

Consider the group

$$\mu(E, \sigma) := \frac{E_0^\times}{\{z\sigma(z) \mid z \in E^\times\}}.$$

Up to  $E$ -linear isometry, the pair  $(E, b_\lambda)$  only depends on the class of  $\lambda$  in  $\mu(E, \sigma)$ . Note that  $\mu(E, \sigma)$  is trivial if  $E = E_0 \times E_0$ .

**Lemma 5.1.** *Let  $T$  be the group scheme over  $K$  defined by the short exact sequence*

$$1 \rightarrow T \rightarrow \text{Res}_{E/K} \mathbb{G}_{m,E} \xrightarrow{\text{Nm}} \text{Res}_{E_0/K} \mathbb{G}_{m,E_0} \rightarrow 1.$$

Then  $\mu(E, \sigma) = H^1(K, T)$ .

*Proof.* This follows from the long exact sequence of cohomology together with Hilbert 90. □

**Remark 5.2.** The group scheme  $T$  acts by isometries on the ‘standard’ form

$$b_1 : E \times E \rightarrow K, \quad (x, y) \mapsto \text{tr}_{E/K}(x\sigma(y)),$$

and  $b_\lambda$  is the twist of  $b_1$  by the class in  $H^1(K, T) = \mu(E, \sigma)$  determined by  $\lambda$ .

We can express  $\mu(E, \sigma)$  in terms of Brauer groups of  $E$  and  $E_0$ :

**Lemma 5.3.** *There is an exact sequence*

$$1 \rightarrow \mu(E, \sigma) \xrightarrow{\beta} \text{Br } E_0 \rightarrow \text{Br } E,$$

where the map  $\text{Br } E_0 \rightarrow \text{Br } E$  is the base change map.

*Proof.* This follows from Hilbert 90 and the long exact sequence of cohomology induced by the short exact sequence

$$1 \rightarrow \text{Res}_{E_0/K} \mathbb{G}_{m,E_0} \rightarrow \text{Res}_{E/K} \mathbb{G}_{m,E} \rightarrow T \rightarrow 1$$

of group schemes over  $K$ , where the last map sends  $z$  to  $\sigma(z)/z$ . □

5.3. *Hasse–Witt invariants of a hermitian form*

The Hasse–Witt invariant  $\epsilon(b_\lambda) \in \text{Br } K$  is determined by the Hasse–Witt invariant  $\epsilon(b)$  and by the twisting cocycle  $\lambda \in \mu(E, \sigma)$ , as follows.

**Proposition 5.4** ([7, Thm. 4.3]). *For every  $\lambda \in E_0^\times$  we have*

$$\epsilon(b_\lambda) = \epsilon(b_1) + \text{Nm}_{E_0/K} \beta(\lambda)$$

in  $\text{Br } K$ . □

5.4. Twisting group of local and global fields

If  $E$  is a local or global field, then the group  $\mu(E, \sigma)$  can easily be made explicit using the standard descriptions of Brauer groups of local and global fields.

**Lemma 5.5.** *Assume that  $E$  is a local field. Then we have a natural commutative diagram*

$$\begin{array}{ccccccccc}
 1 & \longrightarrow & \mu(E, \sigma) & \longrightarrow & \text{Br } E_0 & \longrightarrow & \text{Br } E & \longrightarrow & 1 \\
 & & \downarrow \theta & & \downarrow \text{inv} & & \downarrow \text{inv} & & \\
 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{1/2} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{2} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0
 \end{array}$$

in which the vertical map  $\theta: \mu(E, \sigma) \rightarrow \mathbb{Z}/2\mathbb{Z}$  is an isomorphism.

*Proof.* If  $E$  is non-archimedean then the two maps  $\text{inv}$  are isomorphisms, and the lemma follows from Lemma 5.3. If  $E$  is archimedean, then necessarily  $E = \mathbb{C}$  and  $E_0 = \mathbb{R}$ , and again the lemma follows from Lemma 5.3. □

**Remark 5.6.** We will use explicit descriptions of  $\theta$  in the following cases:

- (i) if  $(E, E_0) = (\mathbb{C}, \mathbb{R})$  then  $\theta(\lambda) = \text{sgn}(\lambda)$ ,
- (ii) if  $E/E_0$  is an unramified extension of non-archimedean local fields, then  $\theta(\lambda) = v_{E_0}(\lambda) \pmod 2$ ,
- (iii) if  $E/E_0$  is a ramified extension of non-archimedean local fields of odd residue characteristic, and if  $\pi_E$  is a uniformizer of  $E$  then  $\pi_{E_0} := \text{Nm } \pi_E$  is a uniformizer of  $E_0$ , and  $\theta$  is given by mapping  $\lambda \pi_{E_0}^n$  with  $\lambda \in \mathcal{O}_{E_0}^\times$  to the class of  $\lambda$  in  $\ell^\times / (\ell^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$ , where  $\ell$  is the residue field of  $\mathcal{O}_{E_0}$ .

**Theorem 5.7** (Local-global obstruction). *Assume that  $E$  is a global field. Let  $S$  be the set of places  $w$  of  $E_0$  for which*

$$E_w := E \otimes_{E_0} E_{0,w}$$

is a field. Then the sequence

$$1 \rightarrow \mu(E, \sigma) \rightarrow \bigoplus_{w \in S} \mu(E_w, \sigma) \xrightarrow{\sum \theta_w} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

is exact.

*Proof.* Class field theory gives a short exact sequence

$$1 \rightarrow \text{Br } E_0 \rightarrow \bigoplus_w \text{Br } E_{0,w} \xrightarrow{\sum \text{inv}} \mathbb{Q}/\mathbb{Z} \rightarrow 0,$$

and a similar sequence for  $E$ . These two sequences sit in a commutative diagram

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \text{Br } E_0 & \longrightarrow & (\bigoplus_{w \in S} \text{Br } E_{0,w}) \oplus (\bigoplus_{w \notin S} \text{Br } E_{0,w}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow 2 \\
 1 & \longrightarrow & \text{Br } E & \longrightarrow & (\bigoplus_{w \in S} \text{Br } E_w) \oplus (\bigoplus_{w \notin S} \text{Br } E_{0,w} \times \text{Br } E_{0,w}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \longrightarrow 1
 \end{array}$$

The kernels of the vertical maps give an exact sequence

$$1 \rightarrow \mu(E, \sigma) \rightarrow \bigoplus_{w \in \mathcal{S}} \mu(E_w, \sigma) \xrightarrow{\sum \theta_w} \mathbb{Z}/2\mathbb{Z}$$

and the rightmost map is surjective since  $\mathcal{S}$  is non-empty. □

### 6. Lattices in one-dimensional hermitian forms

Let  $K$  be a discrete valuation field with residue field  $k$ , maximal ideal  $\mathfrak{m}_K$  and uniformizing element  $\pi_K$ . Let  $E$  be a finite separable field extension of  $K$ , and let  $\sigma$  be a non-trivial involution of  $E$  over  $K$ . Denote by  $E_0$  the fixed field of  $\sigma$ , and by  $\ell$  the residue field of  $E$ . Let  $\lambda \in E_0^\times$ , and consider the associated  $K$ -bilinear form  $b_\lambda$  on  $E$  defined in §5.1. In this section we study lattices in  $(E, b_\lambda)$ , and the image of a  $\mathbb{Z}$ -bilinear form  $(E, b_\lambda, \varrho_\alpha)$  under  $W_{\mathbb{Z}}(K) \rightarrow W_{\mathbb{Z}}(k)$ .

#### 6.1. Almost unimodular $\mathcal{O}_E$ -lattices

We construct an  $\mathcal{O}_E$ -lattice  $\Lambda$  in  $(E, b_\lambda)$  satisfying  $\pi_E \Lambda^\vee \subset \Lambda \subset \Lambda^\vee$  and explicitly determine the  $k$ -bilinear form

$$\frac{\Lambda^\vee}{\Lambda} \times \frac{\Lambda^\vee}{\Lambda} \xrightarrow{b} \frac{\pi_K^{-1} \mathcal{O}_K}{\mathcal{O}_K} \xrightarrow{\pi_K} k \tag{1}$$

on the  $\ell$ -module  $\Lambda^\vee/\Lambda$ .

Denote the valuation of the different ideal  $\mathcal{D}_{E/K}$  by  $\delta$ , so that  $\mathcal{D}_{E/K} = \mathfrak{m}_E^\delta$ .

**Lemma 6.1.** *For every  $n$ , the dual of  $\mathfrak{m}_E^n$  with respect to  $b_\lambda$  is  $\mathfrak{m}_E^{-n-\delta-v_E(\lambda)}$ .*

*Proof.* The dual is an  $\mathcal{O}_E$ -module and hence it equals  $\mathfrak{m}_E^m$  where  $m$  is the smallest integer such that  $b_\lambda(\mathfrak{m}_E^n, \mathfrak{m}_E^m) \subset \mathcal{O}_E$ . By [18, §III.3, Prop. 7] we have  $b_\lambda(\mathfrak{m}_E^n, \mathfrak{m}_E^m) \subset \mathcal{O}_E$  if and only if  $\lambda \mathfrak{m}_E^{n+m} \subset \mathfrak{m}_E^{-\delta}$ , hence  $m = -\delta - n - v_E(\lambda)$ . □

**Corollary 6.2.** *If  $v_E(\lambda) + \delta = -2n$ , then the  $\mathcal{O}_K$ -lattice  $\Lambda := \mathfrak{m}_E^n$  in the  $K$ -bilinear form  $(E, b_\lambda)$  satisfies  $\Lambda^\vee = \Lambda$ .* □

Denote the maximal unramified extension of  $K$  in  $E$  by  $L$ . We have  $\mathcal{O}_L/\mathfrak{m}_L = \ell$ .

**Proposition 6.3.** *If  $v_E(\lambda) + \delta = 1 - 2n$ , then*

- (i) *the  $\mathcal{O}_K$ -lattice  $\Lambda := \mathfrak{m}_E^n$  satisfies  $\pi_E \Lambda^\vee = \Lambda$ ,*
- (ii) *the element*

$$u := \text{tr}_{E/L}(\lambda \pi_K \pi_E^{n-1} \sigma(\pi_E^{n-1}))$$

*is a  $\sigma$ -invariant unit in  $\mathcal{O}_L$ ,*

(iii) *the induced  $k$ -bilinear form on the one-dimensional  $\ell$ -vector space  $\Lambda^\vee/\Lambda$  is isomorphic to the form*

$$\ell \times \ell \rightarrow k, \quad (x, y) \mapsto \text{tr}_{\ell/k}(\bar{u} \cdot x\sigma(y)).$$

*Proof.* The first assertion follows from Lemma 6.1. For the second, note that  $u$  is  $\sigma$ -invariant by construction. Observe that

$$\lambda\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1}) \in \lambda\pi_K\mathfrak{m}_E^{2n-2} \subset \lambda\mathfrak{m}_E^{2n-1} = \mathfrak{m}_E^{-\delta}$$

so that  $u \in \mathcal{O}_L$  by [18, §III.3, Prop. 7]. That  $u$  is a unit will follow from the third assertion, which we now prove.

Let  $\xi, \eta \in \Lambda^\vee/\Lambda$ . We will compute their pairing in  $k$  under

$$\frac{\Lambda^\vee}{\Lambda} \times \frac{\Lambda^\vee}{\Lambda} \rightarrow \frac{\pi^{-1}\mathcal{O}_K}{\mathcal{O}_K} \xrightarrow{\pi_K} k.$$

We have  $\Lambda^\vee/\Lambda = \mathfrak{m}_E^{n-1}/\mathfrak{m}_E^n \cong \ell$  and we can find  $x, y \in \mathcal{O}_L$  with  $\xi = x\pi_E^{n-1}$  and  $\eta = y\pi_E^{n-1}$ . Using the linearity and transitivity properties of the trace, we find

$$\begin{aligned} \pi_K b_\lambda(x\pi_E^{n-1}, y\pi_E^{n-1}) &= \text{tr}_{E/K}(\pi_K \lambda x \pi_E^{n-1} \sigma(y\pi_E^{n-1})) \\ &= \text{tr}_{L/K} \text{tr}_{E/L}(\lambda \pi_K \pi_E^{n-1} \sigma(\pi_E^{n-1}) x \sigma(y)) \\ &= \text{tr}_{L/K}(u x \sigma(y)). \end{aligned}$$

It follows that  $\text{tr}_{L/K}(u x \sigma(y)) \in \mathcal{O}_K$ , and  $\xi$  and  $\eta$  pair to  $\text{tr}_{L/K}(u x \sigma(y)) \pmod{\mathfrak{m}_K}$  in  $k$ .

Since the pairing on  $\Lambda^\vee/\Lambda$  is perfect, and since  $L/K$  is unramified, we conclude that  $u$  must be a unit in  $\mathcal{O}_L$  and that the induced pairing on  $\Lambda^\vee/\Lambda$  is as described in the third assertion. □

### 6.2. Image of a hermitian form under the map $W_{\mathbb{Z}}^b(K) \rightarrow W_{\mathbb{Z}}(k)$

Fix  $\alpha \in E^\times$  with  $\alpha\sigma(\alpha) = 1$  and  $\alpha \neq \pm 1$ . For every  $\lambda$  in  $E_0^\times$  we have a  $\mathbb{Z}$ -bilinear form  $(E, b_\lambda, \varrho_\alpha)$  over  $K$ . Since  $\alpha$  is a unit in  $\mathcal{O}_E$ , this  $\mathbb{Z}$ -bilinear form is bounded. Every  $\mathcal{O}_E$ -submodule  $\Lambda \subset E$  is stable under the action of  $\varrho_\alpha(\mathbb{Z}) = \alpha^\mathbb{Z}$ , so we can use Corollary 6.2 and Proposition 6.3 to say something about the image of  $[E, b_\lambda, \varrho_\alpha]$  under the map  $\partial: W_{\mathbb{Z}}^b(K) \rightarrow W_{\mathbb{Z}}(k)$  of Theorem B.

**Proposition 6.4** (Unramified case). *If  $E/E_0$  is unramified, then there exists a  $\lambda$  in  $\mu(E, \sigma)$  such that  $\partial[E, b_\lambda, \varrho_\alpha] = 0$  in  $W_{\mathbb{Z}}(k)$ .*

*Proof.* Since  $E/E_0$  is unramified, there exists a  $\lambda \in E_0^\times$  such that  $v_E(\lambda) + \delta$  is even, and by Corollary 6.2 there is an  $\mathcal{O}_E$ -module  $\Lambda \subset E$  with  $\Lambda^\vee = \Lambda$ . This module is stable under  $\alpha$ , hence  $\partial[E, b_\lambda, \varrho_\alpha] = [\Lambda^\vee/\Lambda] = 0$ . □

**Lemma 6.5.** *If  $E/E_0$  is ramified, then  $\bar{\alpha} := \alpha \pmod{\mathfrak{m}_E}$  satisfies  $\bar{\alpha} \in \{\pm 1\}$ .*

*Proof.* We have  $\sigma_\ell = \text{id}$  and  $\bar{\alpha}\sigma_\ell(\bar{\alpha}) = 1$ . □



**Proposition 6.6** (Ramified case with odd residue characteristic). *Assume that  $E/E_0$  is ramified, and that the residue characteristic is odd. Let  $\chi : \mathbb{Z} \rightarrow k^\times$  be the character that maps 1 to  $\bar{\alpha}$ . Then for each of the two classes  $\gamma \in W(k)$  with  $\dim \gamma \equiv [\ell : k] \pmod 2$  there is a unique  $\lambda \in \mu(E, \sigma)$  such that*

$$\partial[E, b_\lambda, \varrho_\alpha] = \gamma$$

in  $W(k) = W_{\mathbb{Z}}(k, \chi) \subset W_{\mathbb{Z}}(k)$ .

Here  $W_{\mathbb{Z}}(k, \chi)$  denotes the subgroup of  $W_{\mathbb{Z}}(k)$  generated by the  $\mathbb{Z}$ -bilinear forms of the form  $(k, b, \chi)$ . It is one of the components in the decomposition of Theorem 3.12.

*Proof of Proposition 6.6.* Since the residue characteristic is odd, the quadratic extension  $E/E_0$  is tamely ramified and  $\mathcal{D}_{E/E_0} = \mathfrak{m}_E$ . The transitivity formula  $\mathcal{D}_{E/K} = \mathcal{D}_{E_0/K} \mathcal{D}_{E/E_0}$  implies

$$v_E(\lambda) + \delta = 2v_{E_0}(\lambda) + 2v_{E_0}(\mathcal{D}_{E_0/K}) + 1$$

and hence  $v_E(\lambda) + \delta$  is odd and Proposition 6.3 applies. Since  $\sigma_\ell = \text{id}$ , we see that  $\partial[E, b_\lambda, \varrho_\alpha]$  can be represented by the bilinear form

$$\bar{b} : \ell \times \ell \rightarrow k, \quad (x, y) \mapsto \text{tr}_{\ell/k}(\bar{u}xy),$$

on which  $\mathbb{Z}$  acts via  $\chi$ . The group  $W(k)$  has four elements, distinguished by their dimension in  $\mathbb{Z}/2\mathbb{Z}$  and determinant in  $k^\times/(k^\times)^2$ . For the form  $\bar{b}$  we have

$$\begin{aligned} \dim \bar{b} &= [\ell : k] \in \mathbb{Z}/2\mathbb{Z}, \\ \det \bar{b} &= -(-1)^{[\ell:k]} \text{Nm}(\bar{u}) \in k^\times/(k^\times)^2. \end{aligned}$$

Since the norm map  $\ell^\times \rightarrow k^\times$  is surjective, we see that by changing  $\lambda$  by a unit in  $\mathcal{O}_{E_0}^\times$ , we can reach both classes in  $W(k)$  of dimension  $[\ell : k]$ . □

**Proposition 6.7** (Ramified case with even residue characteristic). *Assume that  $E/E_0$  is ramified, and that the residue characteristic is even. Then for all  $\lambda \in \mu(E, \sigma)$  we have*

$$\partial[E, b_\lambda, \varrho_\alpha] = [\ell : k]\delta$$

in  $W_{\mathbb{Z}}(k, \mathbf{1}) = W(k) = \mathbb{Z}/2\mathbb{Z}$ .

*Proof.* Note that  $v_E(\lambda)$  is even. If  $\delta$  is even, then Corollary 6.2 implies  $\partial[E, b_\lambda, \varrho_\alpha] = 0$ . If  $\delta$  is odd, then Proposition 6.3 shows that  $\partial[E, b_\lambda, \varrho_\alpha]$  can be represented by a bilinear form of dimension  $[\ell : k]$ . □

### 6.3. Relation to the characteristic polynomial

**Lemma 6.8.** *Assume that  $E/E_0$  is ramified. Let  $S$  be the characteristic polynomial of  $\alpha$  over  $K$ . Then  $v_K(S(1)) + v_K(S(-1)) \equiv [\ell : k]\delta \pmod 2$ . If moreover  $k$  has odd characteristic, then either*

- (i)  $\bar{\alpha} = 1$  then  $v_K(S(1)) \equiv [\ell : k] \pmod 2$ , or
- (ii)  $\bar{\alpha} = -1$  then  $v_K(S(-1)) \equiv [\ell : k] \pmod 2$ .

*Proof.* The transitivity formula for the different shows  $\delta \equiv v_E(\mathcal{D}_{E/E_0}) \pmod 2$ , and hence  $\delta \equiv v_E(\sigma(\alpha) - \alpha) \pmod 2$ . Since  $\alpha$  and  $\sigma(\alpha)$  are mutually inverse units, we have

$$v_E(1 - \alpha) + v_E(1 + \alpha) = v_E(1 - \alpha^2) = v_E(\sigma(\alpha) - \alpha) \equiv \delta \pmod 2.$$

Since all the roots of  $S$  have the same valuation, we find

$$v_K(S(\pm 1)) = [E : K] \frac{v_E(1 \mp \alpha)}{e(E : K)} = [\ell : k]v_E(1 \mp \alpha),$$

where  $e(E : K)$  denotes the ramification index. Comparing the above expressions yields  $v_K(S(1)) + v_K(S(-1)) \equiv [\ell : k]\delta \pmod 2$ .

Now if the residue characteristic is odd then  $\delta \equiv 1 \pmod 2$ . If moreover  $\bar{\alpha} = 1$ , then  $1 + \alpha$  is a unit and  $v_K(S(-1)) = 0$ , and similarly if  $\bar{\alpha} = -1$ , then  $1 - \alpha$  is a unit and  $v_K(S(1)) = 0$ . □

### 7. Unimodular lattices in $\mathbb{Z}$ -bilinear forms over local fields

Let  $K$  be a non-archimedean local field,  $E_0$  an étale  $K$ -algebra, and  $E$  an étale  $E_0$ -algebra which is free of rank 2 over  $E_0$ . Denote by  $\sigma$  the involution of  $E$  fixing  $E_0$ . Let  $\alpha \in E^\times$  satisfy  $\alpha\sigma(\alpha) = 1$  and  $\alpha \neq \sigma(\alpha)$ , and denote by  $S$  the characteristic polynomial of  $\alpha$  over  $K$ .

**Proposition 7.1.** *Assume that the characteristic of  $k$  is odd,  $S(1)$  and  $S(-1)$  are non-zero, and  $v_K(S(1))$  and  $v_K(S(-1))$  are even. Then there exists a  $\lambda \in \mu(E, \sigma)$  and a unimodular  $\mathcal{O}_K$ -lattice  $\Lambda \subset (E, b_\lambda)$  stable under  $\alpha$ .*

*Proof.* The algebra  $E_0$  decomposes as a product of fields,  $E_0 = \prod_{w \in \mathcal{S}} E_{0,w}$ , indexed by a finite set  $\mathcal{S}$ . For every  $w \in \mathcal{S}$ , the algebra  $E_w := E \otimes_{E_0} E_{0,w}$  is a quadratic  $E_{0,w}$ -algebra of exactly one of the following types:

- (sp)  $E_w = E_{0,w} \times E_{0,w}$ .
- (un)  $E_w$  is an unramified quadratic extension of  $E_{0,w}$ .
- (+)  $E_w$  is a ramified quadratic extension of  $E_{0,w}$ , and the image  $\bar{\alpha}_v$  of  $\alpha$  in the residue field  $\ell_w$  of  $E_w$  is 1.
- (-)  $E_w$  is a ramified quadratic extension of  $E_{0,w}$ , and the image  $\bar{\alpha}_v$  of  $\alpha$  in the residue field  $\ell_w$  of  $E_w$  is  $-1$ .

This gives a partition  $\mathcal{S} = \mathcal{S}_{\text{sp}} \cup \mathcal{S}_{\text{un}} \cup \mathcal{S}_+ \cup \mathcal{S}_-$ .

Now choose  $\lambda = (\lambda_w)_w$  in  $E_0^\times = \prod_w E_{0,w}^\times$  such that

- (i) for every  $w \in \mathcal{S}_{\text{un}}$  we have  $\partial[E_w, b_{\lambda_w}, \alpha] = 0$ ,
- (ii)  $\sum_{w \in \mathcal{S}_+} \partial[E_w, b_{\lambda_w}, \alpha] = 0$  in  $W(k) = W(k, \chi_+) \subset W_{\mathbb{Z}}(k)$ ,
- (iii)  $\sum_{w \in \mathcal{S}_-} \partial[E_w, b_{\lambda_w}, \alpha] = 0$  in  $W(k) = W(k, \chi_-) \subset W_{\mathbb{Z}}(k)$ ,

where  $\chi_{\pm 1}$  denotes the character  $\mathbb{Z} \rightarrow k^\times, 1 \mapsto \pm 1$ . Such a  $\lambda = (\lambda_w)$  indeed exists. For (i) this follows from Proposition 6.4. For (ii) and (iii) note that by Lemma 6.8 and the condition on  $S(\pm 1)$  we have

$$\sum_{w \in \mathcal{S}_+} [\ell_w : k] \equiv \sum_{w \in \mathcal{S}_-} [\ell_w : k] \equiv 0 \pmod{2}.$$

Hence it follows from Proposition 6.6 that we can choose  $(\lambda_w)_{w \in \mathcal{S}_\pm}$  as required.

Since  $(E_w, b_{\lambda_w}, \alpha)$  is neutral for all  $w \in \mathcal{S}_{\text{sp}}$ , we conclude that

$$\partial[E, b_\lambda, \varrho_\alpha] = \sum_{w \in \mathcal{S}} \partial[E_w, b_{\lambda_w}, \varrho_{\alpha_w}] = 0$$

in  $W_{\mathbb{Z}}(k)$ , and Theorem B shows that  $(E, b_\lambda, \varrho_\alpha)$  contains a unimodular  $\mathbb{Z}$ -stable lattice. □

**Proposition 7.2.** *Assume that the characteristic of  $k$  is even,  $S(1)$  and  $S(-1)$  are non-zero, and  $v_K(S(1)) + v_K(S(-1))$  is even. Then there exists a  $\lambda \in \mu(E, \sigma)$  and a unimodular  $\mathcal{O}_K$ -lattice  $\Lambda \subset (E, b_\lambda)$  stable under  $\alpha$ .*

*Proof.* The algebra  $E_0$  decomposes as a product of fields,  $E_0 = \prod_{w \in \mathcal{S}} E_{0,w}$ . For every  $w \in \mathcal{S}$ , the algebra  $E_w := E \otimes_{E_0} E_{0,w}$  is a quadratic  $E_{0,w}$ -algebra of exactly one of the following types:

- (sp)  $E_w = E_{0,w} \times E_{0,w}$ ,
- (un)  $E_w$  is an unramified quadratic extension of  $E_{0,w}$ ,
- ( $\pm$ )  $E_w$  is a ramified quadratic extension of  $E_{0,w}$ .

This gives a partition  $\mathcal{S} = \mathcal{S}_{\text{sp}} \cup \mathcal{S}_{\text{un}} \cup \mathcal{S}_\pm$ .

Now choose  $\lambda = (\lambda_w)_w$  in  $E_0^\times = \prod_w E_{0,w}^\times$  such that for every  $w \in \mathcal{S}_{\text{un}}$  we have  $\partial[E_w, b_{\lambda_w}, \alpha] = 0$ . We have  $\partial[E_w, b_{\lambda_w}, \varrho_{\alpha_w}] = 0$  for  $w \in \mathcal{S}_{\text{sp}}$  and using Proposition 6.7 we find

$$\partial[E, b_\lambda, \varrho_\alpha] = \sum_{w \in \mathcal{S}_\pm} \partial[E_w, b_{\lambda_w}, \varrho_{\alpha_w}] = \sum_{w \in \mathcal{S}_\pm} [\ell_w : k] \delta_w$$

in  $\mathbb{Z}/2\mathbb{Z} = W(k) \subset W_{\mathbb{Z}}(k)$ . Lemma 6.8 then shows that  $\partial[E, b_\lambda, \varrho_\alpha] = 0$ , and hence by Theorem B we conclude that  $(E, b_\lambda, \varrho_\alpha)$  contains a unimodular  $\mathbb{Z}$ -stable lattice. □

**Remark 7.3.** Note that the components  $\lambda_w$  in the above proof can be chosen arbitrarily for  $w \in \mathcal{S}_{\text{sp}}$  and  $w \in \mathcal{S}_\pm$ . The only restriction concerns the places  $w \in \mathcal{S}_{\text{un}}$ .

### 8. An intermezzo on 2-adic lattices

By itself, Theorem B does not say anything about the existence of a  $G$ -stable even unimodular lattice in a  $G$ -bilinear form over  $\mathbb{Q}_2$ . The aim of this section is to establish the following criterion, which will be used in the proof of Theorem A.

**Theorem 8.1.** *Let  $G$  be a group and  $(V, b, \varrho)$  be a  $G$ -bilinear form over  $\mathbb{Q}_2$ . Assume that  $\varrho(G) \subset \text{SO}(V, b)$ . Then  $V$  contains a  $G$ -stable even unimodular lattice if and only if the following three conditions hold:*

- (i)  $(V, b, \varrho)$  contains a  $G$ -stable unimodular lattice,
- (ii)  $(V, b)$  contains an even unimodular lattice,
- (iii) for every  $g \in G$  we have  $v_2(\delta(\varrho(g))) = 0$  in  $\mathbb{Z}/2\mathbb{Z}$ .

Here  $\delta: \text{SO}(V, b) \rightarrow \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$  denotes the spinor norm. We will recall its definition in §8.2.

### 8.1. Classification

We start by recalling some results on the classification of unimodular lattices over  $\mathbb{Z}_2$ .

**Proposition 8.2.** *Let  $(V, b)$  be a bilinear form over  $\mathbb{Q}_2$  and let  $\Lambda_1$  and  $\Lambda_2$  be unimodular lattices in  $V$ . If  $\Lambda_1$  and  $\Lambda_2$  are either both even, or both odd, then there exists  $g \in \text{O}(V, b)$  such that  $g\Lambda_1 = \Lambda_2$ .*

*Proof.* Follows from [16, Thm. 93.29]. □

Denote by  $H$  and  $N$  the module  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$  equipped with the bilinear forms given in terms of Gram matrices by

$$b_H := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad b_N := \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}.$$

**Proposition 8.3.** *Every even unimodular  $\mathbb{Z}_2$ -lattice is of the form either  $H^n$  or  $N \oplus H^{n-1}$  for some  $n$ .*

*Proof.* See [4, Prop. 5.2] or [12, Satz 15.6]. □

We have  $\text{disc } H^n = 1$  and  $\text{disc}(N \oplus H^{n-1}) = -3$  in  $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2$ .

**Corollary 8.4.** *For every  $n > 0$  and  $d \in \{1, -3\} \subset \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$  there is a unique  $\epsilon \in \{\pm 1\} = (\text{Br } \mathbb{Q}_2)[2]$  such that the unique bilinear form  $V$  over  $\mathbb{Q}_2$  of dimension  $2n$ , discriminant  $d$  and Hasse–Witt invariant  $\epsilon$  contains an even unimodular lattice of rank  $2n$ .*

□

### 8.2. The spinor norm

If  $(V, b)$  is a bilinear form over a field  $K$  of characteristic different from 2, then the short exact sequence

$$1 \rightarrow \{\pm 1\} \rightarrow \text{Spin}(V, b) \rightarrow \text{SO}(V, b) \rightarrow 1$$

induces a morphism

$$\delta: \text{SO}(V, b) \rightarrow \text{H}^1(K, \{\pm 1\}) = K^\times/(K^\times)^2$$

called the *spinor norm*.

**Theorem 8.5** (Zassenhaus formula). *Let  $K$  be a field of characteristic different from 2. Let  $(V, b)$  be a bilinear form of dimension  $n$  over  $K$ , and let  $\alpha \in \text{SO}(V)$ . Let  $V_0 \subset V$  be the maximal subspace on which  $1 + \alpha$  is nilpotent, and  $V_1$  its orthogonal complement. Then*

$$\delta(\alpha) = \det(b|_{V_0}) \cdot \det\left(\frac{1+\alpha}{2}, V_1\right)$$

in  $K^\times / (K^\times)^2$ .

*Proof.* See [24] or [8, Thm. C.5.7]. □

**Proposition 8.6.** *Let  $(V, b)$  be a bilinear form over  $\mathbb{Q}_2$ . Assume that  $\alpha \in \text{SO}(V, b)$  stabilizes an even unimodular  $\mathbb{Z}_2$ -lattice  $\Lambda \subset V$ . Then  $v_2(\delta(\alpha)) \equiv 0 \pmod 2$ .*

*Proof.* Since  $\Lambda$  is even and unimodular, the quadratic form  $q(x) := b(x, x)/2$  on the  $\mathbb{Z}_2$ -module  $\Lambda$  is non-degenerate (or regular), and the short exact sequence of the spin cover (over  $\mathbb{Q}_2$ ) extends to a short exact sequence

$$1 \rightarrow \mu_2 \rightarrow \text{Spin}(\Lambda) \rightarrow \text{SO}(\Lambda) \rightarrow 1$$

of group schemes over  $\text{Spec } \mathbb{Z}_2$ , exact in the fppf topology (see [8, §C.4]). It follows that  $\delta(\alpha) \in \mathbb{Z}_2^\times / (\mathbb{Z}_2^\times)^2$  for all  $\alpha \in \text{SO}(\Lambda)$ , as we had to show. See [11, Lemma 4.3] for an alternative proof. □

### 8.3. Existence of invariant even unimodular lattices

We are now ready to prove our criterion.

*Proof of Theorem 8.1.* It is clear that (i) and (ii) are necessary, and Proposition 8.6 shows that also (iii) is necessary. So we are left with showing that (i)–(iii) imply the existence of a  $G$ -stable even unimodular lattice.

This follows from a more or less straightforward calculation, based on [4, §5]. We give the argument in case  $\text{disc } b = 1$ . The case  $\text{disc } b = -3$  is similar (and will not be used in the proof of Theorem A).

Let  $\Lambda_0$  be a  $G$ -stable unimodular lattice. If  $\Lambda_0$  is even, then we are done. If not, then by Propositions 8.2 and 8.3, we may assume without loss of generality that

$$\Lambda_0 = H^{n-1} \oplus U,$$

where  $U$  is the rank 2 module  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$  equipped with the odd unimodular form

$$b_U := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

If  $(e, f)$  denotes the standard basis of  $U$ , then  $\mathbb{Q}_2 \otimes \Lambda_0$  contains the even unimodular lattices

$$\Lambda_1 = H^{n-1} \oplus \left\langle e + f, \frac{e - f}{2} \right\rangle, \quad \Lambda_2 = H^{n-1} \oplus \left\langle e - f, \frac{e + f}{2} \right\rangle,$$

of discriminant 1.

Note that the lattice

$$\Lambda := \{x \in \Lambda_0 \mid b(x, x) \in 2\mathbb{Z}_2\} = H^{n-1} \oplus \langle e + f, e - f \rangle$$

is preserved by  $\text{SO}(\Lambda_0)$ . There are precisely three unimodular lattices containing  $\Lambda$ : the odd lattice  $\Lambda_0$ , and the even lattices  $\Lambda_1$  and  $\Lambda_2$ . It follows that the group  $\text{SO}(\Lambda_0)$  acts on the set  $\{\Lambda_1, \Lambda_2\}$ .

By [11, Lemma 4.4] the action on this two-element set is given by the homomorphism

$$\text{SO}(\Lambda_0) \rightarrow \mathbb{Z}/2\mathbb{Z}, \quad \alpha \mapsto v_2(\delta(\alpha)) \pmod 2,$$

which shows that under the hypothesis of the theorem,  $\Lambda_1$  and  $\Lambda_2$  are indeed  $G$ -stable. (The argument in loc. cit. works for  $n > 1$ . For  $n = 1$ , a direct computation shows that for every  $\alpha \in \text{SO}(\Lambda_0)$  we have  $\alpha\Lambda_1 = \Lambda_1$  and  $v_2(\delta(\alpha)) \equiv 0$ .) □

**Remark 8.7.** It is likely that a result similar to Theorem 8.1 holds over unramified extensions of  $\mathbb{Q}_2$ . However, if  $K$  is a ramified extension of  $\mathbb{Q}_2$ , then the classification of unimodular  $\mathcal{O}_K$ -lattices becomes more complicated (see [16, §93]), and it is not clear if one should expect such a simple criterion.

### 9. Even unimodular lattices in $\mathbb{Z}$ -bilinear forms over $\mathbb{Q}_2$

Using Theorem 8.1, we can now refine Proposition 7.2 to obtain the existence of an invariant even unimodular lattice.

As in §7, let  $E_0$  be an étale  $\mathbb{Q}_2$ -algebra of rank  $n$ , let  $E$  be an étale  $E_0$ -algebra, free of rank 2 over  $E_0$ . Denote by  $\sigma$  the involution of  $E$  fixing  $E_0$ . Let  $\alpha \in E^\times$  satisfy  $\alpha\sigma(\alpha) = 1$ , and denote by  $S$  the characteristic polynomial of  $\alpha$  over  $\mathbb{Q}_2$ .

**Proposition 9.1.** *Assume that  $S(1)$  and  $S(-1)$  are non-zero,  $v_2(S(1))$  and  $v_2(S(-1))$  are even, and the class of  $(-1)^n S(1)S(-1)$  in  $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$  lies in  $\{1, -3\}$ . Then there exists a  $\lambda \in \mu(E, \sigma)$  and an even unimodular  $\mathbb{Z}_2$ -lattice  $\Lambda \subset (E, b_\lambda)$  stable under  $\alpha$ .*

*Proof.* We will use Theorem 8.1. By Proposition 7.2, there is a  $\lambda \in \mu(E, \sigma)$  such that the  $\mathbb{Z}$ -bilinear form  $(E, b_\lambda, \varrho_\alpha)$  over  $\mathbb{Q}_2$  satisfies (i). Also, by the Zassenhaus formula, the condition on  $v_2(S(-1))$  guarantees that it satisfies (iii).

By [10, Prop. A.3] the bilinear form  $(E, b_\lambda)$  has discriminant 1 or  $-3$  in  $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ .

If  $E$  is everywhere unramified over  $E_0$ , then the trace map  $\text{tr}: E \rightarrow E_0$  is surjective, and there is an  $e \in E$  with  $e + \sigma(e) = 1$ . It follows that any lattice in  $E$  is even, since

$$b(x, x) = b((e + \sigma(e))x, x) = b(ex, x) + b(x, ex) = 2b(ex, x).$$

In particular, condition (ii) is satisfied.

If there is a component  $E_{0,w}$  such that  $E_w/E_{0,w}$  is ramified, then using Proposition 5.4 and Corollary 8.4 we can modify the component  $\lambda_w$  of  $\lambda$  to guarantee the existence of an even unimodular lattice in  $(E, b_\lambda, \varrho_\alpha)$ . By Remark 7.3, condition (i) in Theorem 8.1 is not affected. □

**10. Unimodular lattices in  $\mathbb{Z}$ -bilinear forms over  $\mathbb{Q}$**

*Proof of Theorem A.* Assume we are given integers  $r$  and  $s$  satisfying  $r \equiv s \pmod 8$ , a monic irreducible  $P \in \mathbb{Z}[t]$ , and a power  $S = P^N$  of degree  $r + s$  satisfying (C1)–(C3). If  $P$  is linear then  $S = (t \pm 1)^{r+s}$  and the conclusion holds for trivial reasons. So from now on we assume that the degree of  $P$  is at least 2.

*The number fields  $E_0$  and  $E$ .* Note that (C1) implies that  $P$  is also reciprocal. Consider the field  $F := \mathbb{Q}[t]/(P)$ , and let  $\alpha \in F$  be the image of  $t$ . Denote by  $\sigma$  the involution of  $F$  that maps  $\alpha$  to  $1/\alpha$ . Since  $\deg P \geq 2$ , this involution is non-trivial. Denote by  $F_0$  the fixed field of  $\sigma_F$ . Choose a field extension  $E_0$  of  $F_0$  of degree  $N$ , linearly disjoint from  $F$ . Then  $E := E_0 \otimes_{F_0} F$  is a field, and the characteristic polynomial of  $\alpha \in E$  is  $S$ . Denote by  $\sigma$  the canonical extension of  $\sigma_F$  to  $E$ .

In everything what follows,  $v$  will denote a place of  $\mathbb{Q}$  and  $w$  a place of  $E_0$ . We will write  $E_w$  for the quadratic  $E_{0,w}$ -algebra  $E \otimes_{E_0} E_{0,w}$ .

*Infinite places.* Let  $w$  be an infinite place of  $E_0$  and denote by  $\alpha_w$  the image of  $\alpha$  in  $E_w^\times$ . Then one of the following three holds:

- (i)  $E_{0,w} = \mathbb{R}$ ,  $E_w = \mathbb{R} \times \mathbb{R}$ , and  $\alpha_w = (\beta, 1/\beta)$  with  $\beta \in \mathbb{R}^\times$  and  $|\beta| \neq 1$ ,
- (ii)  $E_{0,w} = \mathbb{C}$ ,  $E_w = \mathbb{C} \times \mathbb{C}$ , and  $\alpha_w = (\beta, 1/\beta)$  with  $\beta \in \mathbb{C}^\times \setminus \mathbb{R}^\times$  and  $|\beta| \neq 1$ ,
- (iii)  $E_{0,w} = \mathbb{R}$ ,  $E_w = \mathbb{C}$ , and  $|\alpha_w| = 1$ .

In the first and second cases  $\mu(E_w, \sigma)$  is trivial, and the bilinear form  $(E_w, b_\lambda)$  over  $\mathbb{R}$  has signature  $(1, 1)$  resp.  $(2, 2)$  for all  $\lambda \in E_{0,w}^\times$ . In the third case  $\mu(E_w, \sigma) = \{\pm 1\}$  and  $(E_w, b_\lambda)$  has signature  $(2, 0)$  for  $\lambda = 1$  and  $(0, 2)$  for  $\lambda = -1$ .

As in the introduction to this paper, denote the number of roots  $z$  of  $S$  with  $|z| > 1$  by  $m = m(S)$ . Define

$$d_+ := \frac{r - m}{2}, \quad d_- := \frac{s - m}{2}.$$

Condition (C2) guarantees that these are non-negative integers. Note that there are exactly  $d_+ + d_- = (r + s - 2m)/2$  infinite places of the third type in  $E_0$ . Choose  $\lambda_\infty = (\lambda_w)_{w|\infty}$  in

$$\mu(\mathbb{R} \otimes E, \sigma) = \prod_{w|\infty} \mu(E_w, \sigma)$$

with  $d_+$  components 1 and  $d_-$  components  $-1$  at places  $w$  of the third type. Then  $(\mathbb{R} \otimes E, b_{\lambda_\infty})$  has signature  $(r, s)$ .

*Finite places.* For every prime number  $p$  choose  $\lambda_p = (\lambda_w)_{w|p}$  in

$$\mu(\mathbb{Q}_p \otimes E, \sigma) = \prod_{w|p} \mu(E_w, \sigma)$$

such that the bilinear form  $(\mathbb{Q}_p \otimes E, b_{\lambda_p})$  over  $\mathbb{Q}_p$  contains an even unimodular  $\alpha$ -stable  $\mathbb{Z}_p$ -lattice. Condition (C3) and Propositions 7.1 and 9.1 guarantee that this is possible. Note that for all but finitely many  $w$  we have  $\lambda_w = 1$  in  $\mu(E_w, \sigma)$ .

*Comparison with a standard lattice.* Let  $\Lambda_{r,s}$  be an even unimodular lattice of signature  $(r, s)$ . The congruence  $s \equiv r \pmod 8$  implies  $\text{disc } \Lambda_{r,s} = 1$ . We claim that for every place  $v$  of  $\mathbb{Q}$  we have

$$(\mathbb{Q}_v \otimes E, b_{\lambda_v}) \cong \mathbb{Q}_v \otimes \Lambda_{r,s}$$

as bilinear forms over  $\mathbb{Q}_v$ . For the infinite place this is clear. For  $v = v_p$ , note that both forms contain an even unimodular lattice, and by [10, Prop. A.3] they have discriminant 1 in  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ . This implies that they must be isomorphic: for  $p = 2$  this follows from Proposition 8.3, and for  $p \neq 2$  from [16, 92:1].

*Local-global obstruction.* For every place  $v$  of  $\mathbb{Q}$ , we now have in  $\text{Br } \mathbb{Q}_v$  the following three elements:

- (i)  $\epsilon_v(\mathbb{Q}_v \otimes E, b_{\lambda_v}) = \epsilon_v(\Lambda_{r,s})$ ,
- (ii)  $\epsilon_v(\mathbb{Q}_v \otimes E, b_1)$ ,
- (iii)  $\beta(\lambda_v) := \sum_{w|v} \text{Cor}_{E_{0,w}/\mathbb{Q}_v} \beta_w(\lambda_w)$ ,

where  $\beta_w$  is the map  $\mu(E_w, \sigma) \rightarrow \text{Br } E_{0,w}$  of Lemma 5.3. By Proposition 5.4 these Brauer classes are related by

$$\epsilon_v(\Lambda_{r,s}) = \epsilon_v(\mathbb{Q}_v \otimes E, b_1) + \beta(\lambda_v).$$

Since  $\Lambda_{r,s}$  and  $b_1$  are global objects, we have

$$\sum_v \text{inv}_v \epsilon_v(\Lambda_{r,s}) = 0, \quad \sum_v \text{inv}_v \epsilon_v(\mathbb{Q}_v \otimes E, b_1) = 0$$

in  $\mathbb{Q}/\mathbb{Z}$ , and therefore also  $\sum_v \text{inv}_v \beta(\lambda_v) = 0$ . Using the commutative square

$$\begin{array}{ccc} \text{Br } E_{0,w} & \xrightarrow{\text{inv}_w} & \mathbb{Q}/\mathbb{Z} \\ \text{Cor} \downarrow & & \downarrow \text{id} \\ \text{Br } \mathbb{Q}_v & \xrightarrow{\text{inv}_v} & \mathbb{Q}/\mathbb{Z} \end{array}$$

we conclude that  $\sum_w \theta_w(\lambda_w) = 0$ . By Theorem 5.7 there exists a  $\lambda$  in  $\mu(E, \sigma)$  specializing to the chosen  $\lambda_w$ 's. The bilinear form  $(E, b_\lambda)$  has signature  $(r, s)$ , and  $(\mathbb{Q}_p \otimes E, b_\lambda)$  contains an  $\alpha$ -stable even unimodular  $\mathbb{Z}_p$ -lattice  $\Lambda_p$  for all  $p$ . For all but finitely many  $p$  we may take  $\Lambda_p = \mathbb{Z}_p \otimes \mathcal{O}_E$ , and then

$$\Lambda := \{x \in E \mid x \in \Lambda_p \text{ for all } p\}$$

is an  $\alpha$ -stable even unimodular  $\mathbb{Z}$ -lattice in  $(E, b_\lambda)$ . □

*Acknowledgments.* We want to thank Asher Auel, Simon Brandhorst, Curt McMullen, Jean-Pierre Serre and Xun Yu for enlightening discussions and comments on an earlier draft. The second author is supported by a grant of the Netherlands Organisation for Scientific Research (NWO).

**References**

- [1] Bayer-Fluckiger, E.: Definite unimodular lattices having an automorphism of given characteristic polynomial. *Comment. Math. Helv.* **59**, 509–538 (1984) [Zbl 0558.10029](#) [MR 0780074](#)
- [2] Bayer-Fluckiger, E.: Réseaux unimodulaires. *Sém. Théor. Nombres Bordeaux (2)* **1**, 189–196 (1989) [Zbl 0729.11017](#) [MR 1050274](#)



- [3] Bayer-Fluckiger, E.: Determinants of integral ideal lattices and automorphisms of given characteristic polynomial. *J. Algebra* **257**, 215–221 (2002) [Zbl 1020.11021](#) [MR 1947320](#)
- [4] Belolipetsky, M., Gan, W. T.: The mass of unimodular lattices. *J. Number Theory* **114**, 221–237 (2005) [Zbl 1076.11025](#) [MR 2167969](#)
- [5] Bruhat, F., Tits, J.: Schémas en groupes et immeubles des groupes classiques sur un corps local. *Bull. Soc. Math. France* **112**, 259–301 (1984) [Zbl 0565.14028](#) [MR 0788969](#)
- [6] Bruhat, F., Tits, J.: Schémas en groupes et immeubles des groupes classiques sur un corps local. II. Groupes unitaires. *Bull. Soc. Math. France* **115**, 141–195 (1987) [Zbl 0636.20027](#) [MR 0919421](#)
- [7] Brusamarello, R., Chuard-Koulmann, P., Morales, J.: Orthogonal groups containing a given maximal torus. *J. Algebra* **266**, 87–101 (2003) [Zbl 1079.11023](#) [MR 1994530](#)
- [8] Conrad, B.: Reductive group schemes. In: *Autour des schémas en groupes. Vol. I, Panor. Synthèses 42/43*, Soc. Math. France, Paris, 93–444 (2014) [Zbl 1349.14151](#) [MR 3362641](#)
- [9] Goldman, O., Iwahori, N.: The space of  $p$ -adic norms. *Acta Math.* **109**, 137–177 (1963) [Zbl 0133.29402](#) [MR 0144889](#)
- [10] Gross, B. H., McMullen, C. T.: Automorphisms of even unimodular lattices and unramified Salem numbers. *J. Algebra* **257**, 265–290 (2002) [Zbl 1022.11016](#) [MR 1947324](#)
- [11] Günther, A., Nebe, G.: Automorphisms of doubly even self-dual binary codes. *Bull. London Math. Soc.* **41**, 769–778 (2009) [Zbl 1184.94267](#) [MR 2557457](#)
- [12] Kneser, M.: *Quadratische Formen*. Springer, Berlin (2002) [Zbl 1001.11014](#) [MR 2788987](#)
- [13] Knus, M.-A.: *Quadratic and Hermitian Forms over Rings*. Grundlehren Math. Wiss. 294, Springer, Berlin (1991) [Zbl 0756.11008](#) [MR 1096299](#)
- [14] McMullen, C. T.: Dynamics on  $K3$  surfaces: Salem numbers and Siegel disks. *J. Reine Angew. Math.* **545**, 201–233 (2002) [Zbl 1054.37026](#) [MR 1896103](#)
- [15] Nikulin, V. V.: Integer symmetric bilinear forms and some of their geometric applications. *Izv. Akad. Nauk SSSR Ser. Mat.* **43**, 111–177 (1979) (in Russian) [Zbl 0408.10011](#) [MR 0525944](#)
- [16] O’Meara, O. T.: *Introduction to Quadratic Forms*. 3rd corrected printing, Grundlehren Math. Wiss. 117, Springer, New York (1973) [Zbl 0259.10018](#) [MR 0525944](#)
- [17] Scharlau, W.: *Quadratic and Hermitian Forms*. Grundlehren Math. Wiss. 270, Springer, Berlin (1985) [Zbl 0584.10010](#) [MR 0770063](#)
- [18] Serre, J.-P.: *Corps locaux*. Act. Sci. Indust. 1296, Hermann, Paris (1962) [Zbl 0137.02601](#) [MR 0150130](#)
- [19] Serre, J.-P.: On the mod  $p$  reduction of orthogonal representations. In: *Lie Groups, Geometry, and Representation Theory*, Progr. Math. 326, Birkhäuser/Springer, Cham, 527–540 (2018) [Zbl 07065410](#) [MR 3890220](#)
- [20] Springer, T. A.: Quadratic forms over fields with a discrete valuation. I. Equivalence classes of definite forms. *Indag. Math.* **17**, 352–362 (1955) [Zbl 0067.27605](#) [MR 0070664](#)
- [21] Springer, T. A.: On the equivalence of quadratic forms. *Indag. Math.* **21**, 241–253 (1959) [Zbl 0087.03501](#) [MR 0108468](#)
- [22] Stoltzfus, N. W.: Unraveling the integral knot concordance group. *Mem. Amer. Math. Soc.* **12**, no. 192, iv + 91 pp. (1977) [Zbl 0366.57005](#) [MR 0467764](#)
- [23] Thompson, J. G.: Bilinear forms in characteristic  $p$  and the Frobenius–Schur indicator. In: *Group Theory (Beijing 1984)*, Lecture Notes in Math. 1185, Springer, Berlin, 221–230 (1986) [Zbl 0542.35054](#)
- [24] Zassenhaus, H.: On the spinor norm. *Arch. Math. (Basel)* **13**, 434–451 (1962) [Zbl 0118.01804](#) [MR 0148760](#)