J. Eur. Math. Soc. 26, 3365–3428 (2024) DOI 10.4171/JEMS/1334

Eva Bayer-Fluckiger

Isometries of lattices and Hasse principles

Received January 6, 2021; revised May 7, 2021

Abstract. We give necessary and sufficient conditions for an integral polynomial without linear factors to be the characteristic polynomial of an isometry of some even, unimodular lattice of given signature. This gives rise to Hasse principle questions, which we answer in a more general setting. As an application, we prove a Hasse principle for signatures of knots.

Keywords. Quadratic forms, lattices, isometries, signatures of knots

Contents

Eva Bayer-Fluckiger: École Polytechnique Fédérale de Lausanne, SB MATHGEOM CSAG, 1015 Lausanne, Switzerland; eva.bayer@epfl.ch

Mathematics Subject Classification (2020): Primary 11D09; Secondary 57K10

0. Introduction

In [GM 02], Gross and McMullen give necessary conditions for a monic, irreducible polynomial to be the characteristic polynomial of an isometry of some even, unimodular lattice of prescribed signature. They speculate that these conditions may be sufficient; this is proved in [BT 20]. It turns out that the conditions of Gross and McMullen are local conditions, and that (in the case of an irreducible polynomial) a local-global principle holds.

More generally, if $F \in \mathbf{Z}[X]$ is a monic polynomial without linear factors, the conditions of Gross and McMullen are still necessary. Moreover, they are also sufficient everywhere locally (see Theorem 25.6). However, when F is reducible, the local-global principle no longer holds in general, as shown by the following example.

Example. Let F be the polynomial

$$(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)^2(X^6 - X^5 + X^4 - X^3 + X^2 - X + 1)^2,$$

and let L be an even, unimodular, positive definite lattice of rank 24. The lattice L has an isometry with characteristic polynomial F everywhere locally, but not globally (see Example 25.16). In particular, the Leech lattice has no isometry with characteristic polynomial F, in spite of having such an isometry everywhere locally.

More generally, let p be a prime number with $p \equiv 3 \pmod 4$ and set $F = \Phi_p^2\Phi_{2p}^2$, where Φ_m denotes the cyclotomic polynomial of the m-th roots of unity (the example above is the case $p = 7$); there exists an even, unimodular, positive definite lattice having an isometry with characteristic polynomial F if and only if $p \equiv 3 \pmod 8$. On the other hand, all even, unimodular and positive definite lattices of rank $\deg(F)$ have such an isometry locally everywhere.

Several other examples are given in §25, both in the definite and indefinite cases.

One of the aims of this paper is to give necessary and sufficient conditions for the local-global principle (also called Hasse principle) to hold, and hence for the existence of an even, unimodular lattice of given signature having an isometry with characteristic polynomial F; this is done in Theorem 25.11.

We consider a more general setting: isometries of lattices over rings of integers of global fields of characteristic $\neq 2$ with respect to a finite set of places. The local conditions on the polynomial then also depend on the field and on the finite set of places – in the case of unimodular, even lattices over the integers, they are given by the Gross–McMullen conditions, and the same question for rings of integers of arbitrary number fields is treated by Kirschmer [K 19]. We do not attempt to work out the local conditions in general: we assume that they are satisfied, and give the obstruction to the local-global principle.

Even more generally, in §13 we construct an "obstruction group" – a finite abelian group which gives rise to the obstruction group to the Hasse principle in several concrete situations.

To explain the results of the paper, let us come back to the original question: we have a monic polynomial $F \in \mathbf{Z}[X]$ without linear factors, we choose a pair of integers $r, s \geqslant 0$ and we would like to know whether there exists an even, unimodular lattice of signature (r, s) having an isometry with characteristic polynomial F. It is easy to see that all even, unimodular lattices with the same signature become isomorphic over $\mathbf{Q}$. This leads to an easier question: let $F \in \mathbf{Q}[X]$ be a monic polynomial and let q be a non-degenerate quadratic form over $\mathbf{Q}$; under what conditions does q have an isometry with characteristic polynomial F? This question was raised, for arbitrary ground fields of characteristic not 2, by Milnor [M 69], and an answer is given in [B 15] in the case of global fields; instead of just fixing the characteristic polynomial, the point of view of [B 15] is to fix a module over the group ring of the infinite cyclic group. As seen in [B 15], the crucial case is the one of a *semisimple* and *self-dual* module (the minimal polynomial is a product of distinct, symmetric irreducible polynomials – recall that a monic polynomial $f \in K[X]$ of even degree is said to be *symmetric* if $f(X) = X^{\deg(f)} f(X^{-1})$).

We start by studying this "rational" question, and then come back to the "integral" one. Assume that K is a global field, and that the irreducible factors of F are symmetric and of even degree. If q is a quadratic form over K, we say that the *rational Hasse principle* holds for q and F if q has a semisimple isometry with characteristic polynomial F if and only if such an isometry exists everywhere locally. Theorem 17.4 gives a necessary and sufficient condition for this to hold, in terms of an obstruction group (see §14).

Let I be the set of irreducible factors of F. We show that the rational Hasse principle always holds if for all $f \in I$, the extensions $K[X]/(f)$ are pairwise independent over K (see Corollary 18.3). We also obtain an "odd degree descent" result (see Theorem 20.1):

Theorem. *A quadratic form has an isometry with characteristic polynomial F if and only if such an isometry exists over a finite extension of K of odd degree.*

We next come to the "integral" questions, defining an integral obstruction group (see §21), which contains the rational one as a subgroup. The Hasse principle result is given in Theorem 23.4. Note that both the rational and integral Hasse principles are proved in a more general setting than the one outlined in this introduction.

The applications to the initial question are as follows. Let F be as above, with $F \in \mathbf{Z}[X]$. The integral obstruction group defined in §21 only depends on F; we denote it by $Ш_F$. Set $\deg(F) = 2n$, and let (r, s) be a pair of integers, $r, s \geqslant 0$, such that $r + s = 2n$. The following conditions (C1) and (C2) are necessary for the existence of an even, unimodular lattice with signature (r, s) having an isometry with characteristic polynomial F (see Lemma 25.3):

(C1) *The integers $|F(1)|$, $|F(-1)|$ and $(-1)^n F(1)F(-1)$ are all squares.*

Let $m(F)$ be the number of roots z of F with $|z| > 1$ (counted with multiplicity).

(C2) $r \equiv s \pmod 8$, *$r \geqslant m(F)$, $s \geqslant m(F)$, and* $m(F) \equiv r \equiv s \pmod 2$.

Assume that conditions (C1) and (C2) hold. We define a finite set of linear forms on $Ш_F$, and prove that there exists an even, unimodular lattice with signature (r,s) having a semisimple isometry with characteristic polynomial F if and only if one of these linear forms is zero (see Theorem 25.11).

Several examples are given in §25.

Example. Let $f_1(X) = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$, and $f_2 = \Phi_{14}$. Set $F = f_1 f_2^2$. Set $L_{3,19} = (-E_8) \oplus (-E_8) \oplus H \oplus H \oplus H$, where E_8 is the E_8-lattice and H the hyperbolic lattice. It is shown in Examples 25.8 and 25.20 that $L_{3,19}$ has an isometry with characteristic polynomial F.

Example. Let p and q be distinct prime numbers such that $p \equiv q \equiv 3 \pmod 4$. Let $n, m, t \in \mathbf{Z}$ with $n, m, t \geqslant 2$ and $m \neq t$, and set

$$f_1 = \Phi_{p^n q^m}, \quad f_2 = \Phi_{p^n q^t}, \quad \text{and} \quad F = f_1 f_2.$$

There exists a positive definite, even, unimodular lattice having an isometry with characteristic polynomial F if and only if $(\frac{p}{q}) = 1$ (see Examples 25.9 and 25.14).

With F and (r,s) as above, we ask a more precise question.

Question. *Let $t \in \mathrm{SO}_{r,s}(\mathbf{R})$ be a semisimple isometry with characteristic polynomial F. Does t preserve an even, unimodular lattice?*

Still assuming that the "local conditions" (C1) and (C2) hold, we define a linear form $Ш_F \to \mathbf{Z}/2$ and we show that the answer to the above question is affirmative if and only if this form is trivial (see Theorem 27.4). In particular, we have (see Theorem 27.5)

Theorem. *If $Ш_F = 0$, then all semisimple elements of $\mathrm{SO}_{r,s}(\mathbf{R})$ with characteristic polynomial F preserve an even, unimodular lattice.*

Finally, we give an application to *knot theory*. Let $\Delta \in \mathbf{Z}[X]$ be a symmetric polynomial with $\Delta(1) = 1$, and let $r, s \geqslant 0$ be integers with $r + s = \deg(\Delta)$. The results of this paper can be used to decide for which pair (r,s) there exists a knot with Alexander polynomial Δ and signature (r,s); for simplicity, we assume here that Δ is monic, $\Delta(-1) = \pm 1$ and Δ is a product of distinct irreducible and symmetric polynomials (see §30). We have (see Corollary 30.4)

Theorem. *Assume that conditions* (C1) *and* (C2) *hold for Δ and (r,s), and suppose that $Ш_\Delta = 0$. Then there exists a knot with Alexander polynomial Δ and signature (r,s).*

This is no longer the case in general if $Ш_\Delta \neq 0$. In §31, we discuss in detail the case where Δ is the polynomial

$$\Delta_{u,v} = \frac{(X^{uv} - 1)(X - 1)}{(X^u - 1)(X^v - 1)}$$

where $u, v > 1$ are relatively prime odd integers. Using properties of cyclotomic fields, one can explicitly determine the obstruction group $Ш_\Delta$ and the homomorphisms associated to the local data. For instance, we have (see Example 31.8)

Example. Let p and q be distinct prime numbers with $p \equiv q \equiv 3 \pmod 4$, let $e \geqslant 1$ be an integer, and set $\Delta = \Delta_{p^e,q}$. There exists a knot with Alexander polynomial Δ and signature (r, s) if and only if $r \equiv s \pmod 8$ and

- $(\frac{p}{q}) = -1$, or
- $(\frac{p}{q}) = 1$ and $|r - s| \leqslant 2n - 4(e - 1)$.

1. The equivariant Witt group

Let K be a field, and let A be a K-algebra with a K-linear involution $\sigma : A \to A$. All A-modules are supposed to be finite-dimensional over K.

Bilinear forms compatible with a module structure

Let M be an A-module, and let $b : M \times M \to K$ be a non-degenerate symmetric bilinear form. We say that (M, b) is an *A-bilinear form* if

$$b(ax, y) = b(x, \sigma(a)y)$$

for all $a \in A$ and all $x, y \in M$. If G is a group and $A = K[G]$, and $\sigma : K[G] \to K[G]$ is the K-linear involution sending $g \in G$ to g^{-1}, then this becomes $b(gx, gy) = b(x, y)$ for all $g \in G$ and $x, y \in M$.

Let V be a finite-dimensional K-vector space, and let $q : V \times V \to K$ be a non-degenerate symmetric bilinear form. We say that M and (V, q) are *compatible* if there exists a K-linear isomorphism $\varphi : M \to V$ such that the bilinear form $b_\varphi : M \times M \to K$ defined by $b_\varphi(x, y) = q(\varphi(x), \varphi(y))$ is an A-bilinear form.

Example 1.1. Take for A the group ring $K[\Gamma]$, where Γ is the infinite cyclic group, and for σ the canonical involution of $K[\Gamma]$; let γ be a generator of Γ. If b is a bilinear form compatible with a module M, then γ acts as an isometry of b. Conversely, an isometry of a bilinear form $b : V \times V \to K$ endows V with a structure of A-module compatible with b.

Theorem 1.2. *Let M and $q : V \times V \to K$ be as above, and assume that M and (V, q) are compatible. Let M^s be the semisimplification of M. There exists a non-degenerate symmetric bilinear form q on M^s with the following two properties:*

(a) *q' is compatible with the A-module structure of M^s.*

(b) *q' is isomorphic to q.*

Proof. See [S 18, Theorem 4.2.1]. ■

Example 1.3. Let A, γ and (V, b) be as in Example 1.1. We say that a polynomial in $k[X]$ is *square-free* if it is the product of distinct irreducible polynomials in $k[X]$. Let $f \in k[X]$. The following properties are equivalent:

(a) (V, b) has an isometry with characteristic polynomial f.

(b) (V, b) has an isometry with characteristic polynomial f and square-free minimal polynomial.

It is clear that (b) implies (a); the implication (a)⇒(b) follows from Theorem 1.2.

Let A_M be the image of A in $\mathrm{End}(M)$; if M is compatible with a non-degenerate bilinear form, then the kernel of the map $A \to A_M$ is stable by σ, and the algebra A_M carries the induced involution $\sigma : A_M \to A_M$.

Definition 1.4. We say that an A-module M is *self-dual* if the kernel of the map $A \to A_M$ is stable by σ.

If $\mathrm{char}(K) \neq 2$, the notions of symmetric bilinear form and quadratic form coincide; we then use the term *A-quadratic form* instead of A-bilinear form.

The equivariant Witt group

We denote by $W_A(K)$ the Witt group of A-bilinear forms (see [BT 20, Definition 3.3]).

If M is a simple A-module, let $W_A(K, M)$ be the subgroup of $W_A(K)$ generated by the classes of the (A, σ)-bilinear forms (M, q). We have

$$W_A(K) = \bigoplus_M W_A(K, M),$$

where M ranges over the isomorphism classes of simple A-modules (see [BT 20, Theorem 3.12]).

More generally, if M is a semisimple A-module, set $W_A(K, M) = \bigoplus_S W_A(K, S)$, where S ranges over the isomorphism classes of simple A-modules arising in a direct sum decomposition of M.

Example 1.5. Let $A = K[\Gamma]$ be as in Example 1.1. If (M, b) is an A-bilinear form, we associate to it an A-bilinear form (M^s, b') as in Theorem 1.2. Assuming that $\mathrm{char}(K) \neq 2$, this is also done in Milnor's paper [M 69, §3]. It follows from [M 69, Lemma 3.1 and Theorems 3.2 and 3.3] that the classes of (M, b) and (M^s, b') in $W_A(K)$ are equal.

2. Lattices

Let O be an integral domain, and let K be its field of fractions; let Λ be an O-algebra, and let $\sigma : \Lambda \to \Lambda$ be an O-linear involution. Set $\Lambda_K = \Lambda \otimes_O K$. Let M be a Λ_K-module. A *Λ-lattice* is a Λ-submodule L of M which is a projective O-module and satisfies $KL = M$.

Let (M, b) be a Λ_K-bilinear form; if L is a Λ-lattice, then so is its dual

$$L^\sharp = \{x \in M \mid b(x, L) \subset O\}.$$

We say that L is *unimodular* if $L^\sharp = L$.

3. Bounded modules, semisimplification and reduction mod π

We keep the notation of the previous section, and assume that O is a discrete valuation ring; let π be a uniformizer, and let $k = O/\pi O$ be the residue field. Set $\Lambda_k = \Lambda \otimes_O k$. We say that a Λ_K-module is *bounded* if it contains a Λ-lattice.

Let M be a bounded Λ_K-module, and let $L \subset M$ be a Λ-lattice; the quotient $L/\pi L$ is a Λ_k-module. The isomorphism classes of the simple Λ_k-modules occurring as quotients in a Jordan–Hölder filtration of $L/\pi L$ are independent of the choice of the Λ-lattice L in M; this is a generalization of the Brauer–Nesbitt theorem (see [S 18, Theorem 2.2.1]). The direct sum of these modules is called the *semisimplification* of $L/\pi L$; by the above quoted result it is independent of the choice of L. It will be called the *reduction mod π* of M, and will be denoted by $M(k)$; this Λ_k-module is defined up to a non-canonical isomorphism.

The involution $\sigma : \Lambda \to \Lambda$ induces an involution $\Lambda_k \to \Lambda_k$, which we still denote by σ. Recall that a Λ_k-module N is said to be *self-dual* if the kernel of the homomorphism $\Lambda_k \to \mathrm{End}(N)$ is stable by the involution σ; the image of $\Lambda_k \to \mathrm{End}(N)$ is denoted by $(\Lambda_k)_N$. Set $\kappa(N) = (\Lambda_k)_N$; if N is self-dual, then σ induces an involution $\sigma_N : \kappa(N) \to \kappa(N)$.

4. The residue map

We keep the notation of the previous section. We say that a Λ_K-bilinear form is *bounded* if it is defined on a bounded module, and we denote by $W^b_{\Lambda_K}(K)$ the subgroup of $W_{\Lambda_K}(K)$ generated by the classes of bounded forms.

Let (M, b) be a Λ_K-bilinear form, and let L be a lattice in M; we say that L is *almost unimodular* if $\pi L^\sharp \subset L \subset L^\sharp$, where π is a uniformizer. Every bounded Λ_K-bilinear form contains an almost unimodular lattice (see [BT 20, Theorem 4.3 (i)]). Recall also from [BT 20, Theorem 4.3] the following result.

Theorem 4.1. *The map*

$$\partial : W^b_{\Lambda_K}(K) \to W_{\Lambda_k}(k), \quad [M, b] \mapsto [L^\sharp/L],$$

where L is an almost unimodular lattice contained in M, is a homomorphism. Moreover, a Λ_K-bilinear form contains a unimodular lattice if and only if it is bounded and the image of its Witt class by ∂ is zero.

We call $\partial([M, b])$ the *discriminant form* of the almost unimodular lattice L.

Let (V, q) be a quadratic form over K, and let $\delta \in W_{\Lambda_k}(k)$. We say that (V, q) *contains an almost unimodular* Λ*-lattice with discriminant form* δ if there exists an isomorphism $\varphi : M \to V$ such that (M, b_φ) contains an almost unimodular Λ-lattice with discriminant form δ.

5. Lattices and discriminant forms

We keep the notation of §2; moreover we assume that K is a global field, and O is the ring of integers of K with respect to a finite non-empty set Σ of places of K (containing the infinite places when K is a number field). Let V_Σ be the set of places of K that are not in Σ.

We denote by V_K the set of all places of K; if $v \in V_K$, let K_v be the completion of K at v, let O_v be the ring of integers of K_v, let k_v be the residue field, and set $\Lambda^v = \Lambda \otimes_O O_v$.

Let (M, b) be a Λ_K-bilinear form; if L is a lattice of M and $v \in V_K$, set $M^v = M \otimes_K K_v$ and $L^v = L \otimes_O O_v$.

Definition 5.1. We say that a Λ-lattice L is *almost unimodular* if the lattice L^v is almost unimodular for all $v \in V_\Sigma$. The *discriminant form* of an almost unimodular Λ-lattice L is by definition the collection $\delta(L) = (\delta_v)$ of elements of $W_{\Lambda_{k_v}}(k_v)$ where δ_v is the discriminant form of L^v.

Note that $\delta_v = 0$ for almost all $v \in V_K$.

Proposition 5.2. *An almost unimodular lattice is unimodular if and only if its discriminant form is trivial.*

Proof. This follows from Theorem 4.1. ∎

6. Local-global problems

We keep the notation of the previous section. Let (V, q) be a quadratic form over K; for all places $v \in V_\Sigma$, let us fix $\delta = (\delta_v)$, with $\delta_v \in W_\Gamma(k_v)$ such that $\delta_v = 0$ for almost all v. We say that (V, q) *contains an almost unimodular* Λ*-lattice with discriminant form* δ if there exists an isomorphism $\varphi : M \to V$ such that (M, b_φ) contains an almost unimodular Λ-lattice with discriminant form δ.

We consider the following local and global conditions:

(L1) *For all $v \in V_K$, the quadratic form $(V, q) \otimes_K K_v$ is compatible with the module $M \otimes_K K_v$.*

(L2)$_\delta$ *For all $v \in V_\Sigma$, the quadratic form $(V, q) \otimes_K K_v$ contains an almost unimodular Λ^v-lattice with discriminant form δ_v.*

(G1) *The quadratic form* (V, q) *is compatible with the module* M.

$(\mathrm{G2})_\delta$ *The quadratic form* (V, q) *contains an almost unimodular* Λ*-lattice with discriminant form* δ.

For all $v \in V_K$, set

$$M^v = M \otimes_K K_v \quad \text{and} \quad V^v = V \otimes_K K_v.$$

Proposition 6.1. *The following are equivalent:*

(i) *For all* $v \in V_\Sigma$*, there exists an isomorphism* $\varphi_v : M^v \to V^v$ *such that*

$$\partial_v([M^v, b_{\varphi_v}]) = \delta_v.$$

(ii) *Conditions* (L1) *and* $(\mathrm{L2})_\delta$ *hold.*

Proof. This is clear. ∎

Proposition 6.2. *The following are equivalent:*

(i) *There exists an isomorphism* $\varphi : M \to V$ *such that for all* $v \in V_\Sigma$*, we have*

$$\partial_v([M, b_\varphi]) = \delta_v.$$

(ii) *Conditions* (G1) *and* $(\mathrm{G2})_\delta$ *hold.*

Proof. We have (ii)⇒(i) by definition. Condition (i) implies that for all $v \in V_\Sigma$, there exists a Λ^v-lattice L^v in M^v with discriminant form δ_v. Set

$$L = \{x \in M \mid x \in L^v \text{ for all } v \in V_K\};$$

then L is an almost unimodular lattice of (M, b_φ) with discriminant form δ, hence (ii) holds. ∎

7. Stable factors, orthogonal decomposition and transfer

We keep the notation of Section 1; in particular, K is a field, A is a K-algebra with a K-linear involution $\sigma : A \to A$, and M is an A-module. We also assume that M is *semisimple*. Note that by [BT 20, Theorem 3.12], a bilinear form compatible with M is in the same Witt class as a bilinear form on a semisimple module.

The module M decomposes into the direct sum of isotypic submodules, $M \simeq \bigoplus_N M_N$, where N ranges over the simple factors of M. If b is an A-bilinear form on M, and if N is a self-dual simple factor of M, then the restriction of b to M_N is an orthogonal direct factor of b, and it is compatible with the module M_N. If N a simple factor of M that is not self-dual, then M has a simple factor N' with $N' \neq N$ such that the restriction of b to $M_N \oplus M_{N'}$ is an orthogonal direct factor of b, and is compatible with the module $M_N \oplus M_{N'}$. Summarizing, we get the following well-known result:

Proposition 7.1. *Let b be an A-bilinear form on M. We have an orthogonal sum decomposition*

$$b \simeq \Big(\bigoplus_N b_N\Big) \oplus \Big(\bigoplus_{N,N'} b_{N,N'}\Big),$$

where in the first sum, N ranges over the self-dual simple factors of M, and b_N is compatible with the module M_N; in the second sum, N ranges over the simple factors of M that are not self-dual, and $b_{N,N'}$ is compatible with the module $M_N \oplus M_{N'}$. Moreover, the form $b_{N,N'}$ is metabolic.

Recall that A_M is the image of A in $\mathrm{End}(M)$, and that we are assuming that the kernel of the map $A \to A_M$ is stable by σ; the algebra A_M carries the induced involution $\sigma : A_M \to A_M$.

Assume in addition that A_M is a product of *commutative fields*, finite extensions of K. Some of these are stable under σ, others come in pairs, exchanged by σ.

We associate to the module M a set $\mathcal{A}_M$ of σ-stable commutative K-algebras, as follows. The set $\mathcal{A}_M$ consists of the σ-stable fields A_N, where N is a self-dual simple factor of M, and of the products of two fields interchanged by σ associated to the simple factors of M that are not self-dual.

The elements of $\mathcal{A}_M$ are called *simple σ-stable algebras* associated to M. These can be of three types:

Type (0): A field E stable by σ, and the restriction of σ to E is the identity.

Type (1): A field E stable by σ, and the restriction of σ to E is not the identity; E is then a quadratic extension of the fixed field of σ in E.

Type (2): A product of two fields exchanged by σ.

Proposition 7.1 implies that every bilinear form b compatible with M decomposes as an orthogonal sum $b \simeq b(0) \oplus b(1) \oplus b(2)$, corresponding to the factors of type 0, 1 and 2. Moreover, by Proposition 7.1 the class of $b(2)$ in $W_A(K)$ is zero.

Example 7.2. Let $A = K[\Gamma]$ as in Example 1.1, and let γ be a generator of Γ. In this case, the simple σ-stable factors are of the shape $K[X]/(f)$, where $f \in K[X]$ is as follows:

Type (0): $f(X) = X + 1$ or $X - 1$.

Type (1): $f \in K[X]$ is monic, irreducible, symmetric, of even degree [recall that an even degree polynomial f is symmetric if $f(X) = X^{\deg(f)} f(X^{-1})$].

Type (2): $f = gg^*$ for some irreducible, monic polynomial $g \in K[X]$ with non-zero constant term, and $g^*(X) = g(0)^{-1} X^{\deg(g)} g(X^{-1})$ such that $g \neq g^*$.

We say that f is a polynomial of type (0), (1) or (2).

Let E be a simple σ-stable factor as above, and let N be an isotypic factor of the direct sum decomposition of M with $A_N = E$. We denote by γ_N the image of the generator γ by the map $A \to A_N$. If b is a bilinear form compatible with N, the endomorphism γ_N is an isometry of b with minimal polynomial f and characteristic polynomial f^n, where $n = \dim_E(N)$.

Example 7.3. Let A and (V, q) be as in Example 1.1. Let $f = hh'$, where $h \in K[X]$ is a product of polynomials of type 0 and 1, and $h' \in K[X]$ is a product of polynomials of type 2. The quadratic form (V, q) has an isometry with characteristic polynomial f if and only if (V, q) is the orthogonal sum of a quadratic form having an isometry with characteristic polynomial h, and of a hyperbolic form of dimension $\deg(h')$.

Transfer

Assume now that $\mathcal{A}_M$ has only one element, an involution invariant field E; note that M is a finite-dimensional E-vector space. Let $\ell : E \to K$ be a non-trivial K-linear map such that $\ell(\sigma(x)) = \ell(x)$ for all $x \in E$. The following is well-known:

Proposition 7.4. *A bilinear form b is compatible with M if and only if there exists a non-degenerate hermitian form $h : M \times M \to E$ on the E-vector space M such that $b = \ell \circ h$.*

8. Signatures

We keep the notation of the previous section, with $K = \mathbf{R}$. If (M, b) is an A-quadratic form, we define a *signature* for each self-dual simple factor of M. Moreover, the signatures determine (M, b) up to an isomorphism of A-quadratic forms.

If (M, b) is as above, and if N is a simple self-dual factor of M, we set $A_N = E$; note that $E = \mathbf{C}$, and that $\sigma : E \to E$ is complex conjugation. By Proposition 7.4, there exists a non-degenerate hermitian form $h : N \times N \to E$ such that $b = \ell \circ h$. Let $(r_N, s_N) = (2r'_N, 2s'_N)$, where (r'_N, s'_N) is the signature of the hermitian form h. The following is immediate:

Proposition 8.1. *Let (M, b) be an A-quadratic form, and let (r, s) be the signature of b. Then*

$$r - s = \sum_N (r_N - s_N)$$

where N runs over the self-dual simple factors of M. Conversely, all pairs (r_N, s_N) with $r_N, s_N \leqslant 2\dim_E(M_N)$ and $r - s = \sum_N (r_N - s_N)$ are realized by an A-form (M, b) such that the signature of b is (r, s).

Notation 8.2. The difference $r - s$ is called the *index* of b, denoted by $\tau(b)$. Similarly, for each self-dual simple factor N of M, we denote by $\tau_N(b) = r_N - s_N$ the index of b at N.

Note that Proposition 8.1 implies that $\tau(b) = \sum_N \tau_N(b)$, where N runs over the self-dual simple factors of M.

It is easy to see that the signatures characterize the A-quadratic form up to isomorphism. We have

Proposition 8.3. *Two A-quadratic forms on M are isomorphic if and only if their signatures coincide for each self-dual simple factor of M.*

Proof. By Proposition 7.1 an A-quadratic form on M is determined by its restriction to the modules M_N, where N runs over the self-dual simple factors of M. On the other hand, it is easy to see that an A-quadratic form (M_N, b_N) is determined by the hermitian form $h : M_N \times M_N \to E$ with $b_N = \ell \circ h$. ∎

The following corollary is an immediate consequence of Proposition 8.3:

Corollary 8.4. *Let (M, b) and (M, b') be two A-quadratic forms. Then*

$$(M, b) \simeq (M, b') \iff \tau_N(b) = \tau_N(b') \text{ for each self-dual simple factor } N \text{ of } M.$$

Example 8.5. We keep the notation of Example 1.1, with $A = \mathbf{R}[\Gamma]$. Let (M, b) be an A-quadratic form; the action of a generator of Γ on M is an isometry of the quadratic form b. The simple, self-dual factors of M are of the shape $\mathbf{R}[X]/\mathcal{P}$, where $\mathcal{P} \in \mathbf{R}[X]$ is an irreducible, symmetric polynomial of degree 2; hence each such polynomial $\mathcal{P}$ gives rise to a signature of (M, b) at $\mathcal{P}$.

Example 8.6. The above results lead to a generalization of [GM 02, Theorem 2.4]. We keep the notation of Examples 1.1 and 8.5 with $A = \mathbf{R}[\Gamma]$. Let (r, s) be the signature of the quadratic form b. By the above construction, to all semisimple elements of $\mathrm{SO}_{r,s}(\mathbf{R})$ we associate a signature (and an index) at the irreducible, symmetric factors of its characteristic polynomial. Moreover, Proposition 8.3 shows that two such elements of $\mathrm{SO}_{r,s}(\mathbf{R})$ are conjugate if and only if these signatures coincide.

If $t \in \mathrm{SO}_{r,s}(\mathbf{R})$ is semisimple and if $\mathcal{P}$ is an irreducible, symmetric factor of the characteristic polynomial of t, we denote by $\tau_{\mathcal{P}}(t)$ the corresponding index. By Corollary 8.4, two semisimple isometries $t, t' \in \mathrm{SO}_{r,s}(\mathbf{R})$ with characteristic polynomial f are conjugate if and only if $\tau_{\mathcal{P}}(t) = \tau_{\mathcal{P}}(t')$ for each irreducible, symmetric factor $\mathcal{P}$ of f.

9. Simple modules and reduction

We keep the notation of §7. In particular, M is a semisimple A-module, and if N is a simple factor of M, then A_N is a commutative field. Assume moreover that K is a global field, and let O be a ring of integers with respect to a finite set Σ of places of K, containing the infinite places if K is a number field. Let Λ be an O-algebra; assume that $A = \Lambda \otimes_O K$, and that Λ is stable by the involution $\sigma : A \to A$.

Recall that we denote by V_K the set of places of K, by V_Σ the set of places of K that are not in Σ, and by K_v the completion of K at v; let O_v be the ring of integers of K_v, let $\pi_v \in O_v$ be a uniformizer, and let $k_v = O_v/\pi_v O_v$ be the residue field. Set $M^v = M \otimes_K K_v$ and $\Lambda^v = \Lambda \otimes_O O_v$. As in §3, we denote by $M^v(k_v)$ the reduction mod π_v of M^v.

Proposition 9.1. *Suppose that M is a simple A-module, and let $E = A_M$ be the image of A in* $\mathrm{End}(M)$. *If $w \in V_E$, denote by O_w the ring of integers of E_w, and by κ_w its residue field. Let $v \in V_\Sigma$. The simple components of $M^v(k_v)$ are isomorphic to κ_w for some $w \in V_E$ above v.*

Proof. Let O_{E^v} be the maximal order of E^v, and note that O_{E^v} is a Λ^v-lattice in $M^v = E^v$. The simple components of $O_{E^v}/\pi_v O_{E^v}$ are the residue fields of the rings of integers of E_w for all places $w \in V_E$ above v. This completes the proof of the proposition. ∎

Example 9.2. Assume that $\Lambda = O[\Gamma]$, hence $A = \Lambda \otimes_O K = K[\Gamma]$. With the notation of Example 7.2, let $f \in O[X]$ be of type 1, let $E = K[X]/(f)$ and let $M = [K[X]/(f)]^n$ for some integer $n \geqslant 1$. The homomorphism $O_v \to k_v$ induces $p_v : O_v[X] \to k_v[X]$. The simple components of $M^v(k_v)$ are isomorphic to $k_v[X]/(\mathcal{P})$, where $\mathcal{P} \in k_v[X]$ is an irreducible factor of the polynomial $p_v(f) \in k_v[X]$. Indeed, $[O_v[X]/(f)]^n$ is a lattice in $M^v = [K_v[X]/(f)]^n$, hence the simple components of the reduction mod π_v of M^v are of the shape $k_v[X]/(\mathcal{P})$ with $\mathcal{P} \in k_v[X]$ as above.

10. Twisting groups

We start by recalling some notions and facts from [BT 20, §5]. Assume that K is a field of characteristic $\neq 2$.

If F is a commutative semisimple K-algebra of finite rank, and E a K-algebra that is free of rank 2 over F, we denote by $\sigma : E \to E$ the involution fixing F, and we set

$$T(E,\sigma) = F^\times/\mathrm{N}_{E/F}(E^\times).$$

There is an exact sequence

$$1 \to T(E,\sigma) \xrightarrow{\beta} \mathrm{Br}(F) \xrightarrow{\mathrm{res}} \mathrm{Br}(E),$$

where $\mathrm{res} : \mathrm{Br}(F) \to \mathrm{Br}(E)$ is the base change map (see [BT 20, Lemma 5.3]). Let $d \in F^\times$ be such that $E = F(\sqrt{d})$; then $\beta(\lambda)$ is the class of the quaternion algebra (λ, d) in $\mathrm{Br}(F)$.

If E is a local field, then we have a natural commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & T(E,\sigma) & \longrightarrow & \mathrm{Br}(F) & \longrightarrow & \mathrm{Br}(E) \\ & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\mathrm{inv}} & & \downarrow{\scriptstyle\mathrm{inv}} \\ 0 & \longrightarrow & \mathbf{Z}/2\mathbf{Z} & \xrightarrow{1/2} & \mathbf{Q}/\mathbf{Z} & \xrightarrow{2} & \mathbf{Q}/\mathbf{Z} \end{array} \tag{10.1}$$

in which the vertical map $\theta : T(E,\sigma) \to \mathbf{Z}/2\mathbf{Z}$ is an isomorphism.

Assume now that E is a global field. Let S be the set of places w of F such that $E \otimes_F F_w$ is a field. Then we have (see [BT 20, Theorem 5.7])

Theorem 10.1. *The sequence*

$$1 \to T(E,\sigma) \to \bigoplus_{w \in S} T(E_w,\sigma) \xrightarrow{\sum \theta_w} \mathbf{Z}/2\mathbf{Z} \to 0$$

is exact.

Let v be a place of K, and let w be a place of F above v. Recall that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Br}(F_w) & \xrightarrow{\mathrm{inv}_w} & \mathbf{Q}/\mathbf{Z} \\ {\scriptstyle \mathrm{cor}}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ \mathrm{Br}(K_v) & \xrightarrow{\mathrm{inv}_v} & \mathbf{Q}/\mathbf{Z} \end{array} \tag{10.2}$$

11. Residue maps

We keep the notation of §10. Assume that K is a non-archimedean local field of characteristic $\neq 2$, that E is a finite field extension of K with a non-trivial involution $\sigma : E \to E$ and that F is the fixed field of σ. Let $\ell : E \to K$ be a non-trivial K-linear map such that $\ell(\sigma(x)) = \ell(x)$ for all $x \in E$. Let O be the ring of integers of K, and let k be its residue field. Let O_E be the ring of integers of E, and let m_E be its maximal ideal; set $\kappa_E = O_E/m_E$.

If $n \geqslant 1$ is an integer, we define a map

$$t_n : T(E,\sigma) \to W_E^b(K)$$

as follows. For $\lambda \in T(E,\sigma)$, denote by $h_{n,\lambda}$ the n-dimensional diagonal hermitian form $\langle \lambda, 1, \dots, 1 \rangle$ over E with respect to the involution σ, and set $q_{n,\lambda} = \ell(h_{n,\lambda})$; we obtain an element $[q_{n,\lambda}] \in W_E^b(K)$. Recall that we have a homomorphism $\partial : W_E^b(K) \to W_{\kappa_E}(k)$.

Proposition 11.1. *For all integers $n \geqslant 1$,*

(a) *if E/F is inert, then*

$$\partial \circ t_n : T(E,\sigma) \to W_{\kappa_E}(k)$$

is a bijection;

(b) *if E/F is ramified and* $\mathrm{char}(k) \neq 2$*, then $\partial \circ t_n$ is injective, and its image consists of the classes of forms of dimension $n[\kappa_E : k]$* mod 2*;*

(c) *if E/F is ramified and* $\mathrm{char}(k) = 2$*, then $\partial \circ t_n$ is constant.*

Proof. Let δ be the valuation of the different ideal $\mathfrak{D}_{E/K}$; in other words, we have $\mathfrak{D}_{E/K} = m_E^{\delta}$.

(a) Let $\overline{\sigma} : \kappa_E \to \kappa_E$ be the involution induced by σ. Since E/F is inert, this involution is non-trivial. The group $W_{\kappa_E}(k)$ is isomorphic to the Witt group $W(\kappa_E, \overline{\sigma})$ of hermitian forms over $(\kappa_E, \overline{\sigma})$. Note that since k is a finite field, the group $W(\kappa_E, \overline{\sigma})$ is of order 2.

Let π_E be a generator of m_E, and note that the class of π_E is the unique non-trivial element of $T(E, \sigma)$. By [BT 20, Corollary 6.2 and Proposition 6.3], we see that if δ is even, then $\partial \circ t_n(1) = 0$ and $\partial \circ t_n(\pi_E) \neq 0$; if δ and n are both odd, then $\partial \circ t_n(\pi_E) = 0$ and $\partial \circ t_n(1) \neq 0$; if δ is odd and n is even, then $\partial \circ t_n(1) = 0$ and $\partial \circ t_n(\pi_E) \neq 0$. Hence $\partial \circ t_n$ is bijective.

(b) follows from [BT 20, Proposition 6.6].

(c) follows from [BT 20, Proposition 6.7]. ■

The following special case will be useful.

Lemma 11.2. *Assume that E/K is unramified. Then $\partial \circ t_n(1) = 0$ in $W_{\kappa_E}(k)$ for all integers $n \geqslant 1$.*

Proof. The hypothesis implies that the valuation of the different ideal $\mathcal{D}_{E/K}$ is zero, and that E/F is inert; hence Proposition 11.1 yields the desired result. ■

12. Hermitian forms and Hasse–Witt invariants

Assume that K is a field of characteristic $\neq 2$. The aim of this section is to give some results relating the invariants of hermitian forms and those of the quadratic forms obtained from them via transfer. Recall that every quadratic form q over K can be diagonalized, in other words there exist $a_1, \dots, a_n \in K^\times$ such that $q \simeq \langle a_1, \dots, a_n \rangle$. The *determinant* of q is by definition the product $a_1 \dots a_n$, denoted by $\det(q)$; it is an element of $K^\times / K^{\times 2}$. Let us denote by $\mathrm{Br}(K)$ the Brauer group of K, considered as an additive abelian group, and let $\mathrm{Br}_2(K)$ be the subgroup of elements of order ≤ 2 of $\mathrm{Br}(K)$. The *Hasse–Witt invariant* of q is by definition $w_2(q) = \sum_{i<j} (a_i, a_j) \in \mathrm{Br}_2(k)$, where (a_i, a_j) is the class of the quaternion algebra over K determined by a_i, a_j.

Let E be a finite extension of K, and let $\sigma : E \to E$ be a non-trivial K-linear involution of E; let F be the fixed field of σ, and let $d \in F^\times$ be such that $E = F(\sqrt{d})$. Let $\ell : E \to K$ be a non-trivial K-linear map such that $\ell(x) = \ell(\sigma(x))$ for all $x \in E$.

For all $a \in F^\times$, let D_a be the determinant of the quadratic form $F \times F \to K$ defined by $(x, y) \mapsto \ell_F(axy)$, where ℓ_F is the restriction of ℓ to F.

Lemma 12.1. *For all $a \in F^\times$, we have*

$$D_a = \mathrm{N}_{F/K}(a) D_1.$$

Proof. Let $L_a : F \to \mathrm{Hom}_K(F, K)$ be defined by $L_a(x)(y) = \ell_F(axy)$ for all $x, y \in F$, and let $m_a : F \to F$ be multiplication by a; we have $L_a = L_1 \circ m_a$. Since $\det(L_a) = D_a$ and $\det(m_a) = \mathrm{N}_{F/K}(a)$, the lemma follows. ■

If $h : M \times M \to E$ is a non-degenerate hermitian form, composing with ℓ gives rise to a quadratic form $\ell(h) : M \times M \to K$ defined by $\ell(h)(x, y) = \ell(h(x, y))$.

Proposition 12.2. *Let $h : M \times M \to E$ be a non-degenerate hermitian form, and let $n = \dim(M)$. The determinant of the quadratic form $\ell(h)$ is $\mathrm{N}_{F/K}(-d)^n$.*

Proof. It suffices to prove the proposition when $n = 1$. Let $\lambda \in F^\times$ be such that $h(x, y) = \lambda x \sigma(y)$. Since $\ell(\sigma(x) = \ell(x)$ for all $x \in E$, we have $\ell(\sqrt{d}) = 0$, hence $\ell(h)$ is the orthogonal sum of two quadratic forms defined on the K-vector space F, namely $(x, y) \mapsto \ell_F(\lambda xy)$ and $(x, y) \mapsto \ell_F(-d\lambda xy)$, where ℓ_F is the restriction of ℓ to F. The determinant of $\ell(h)$ is the product of the determinants of these two forms. Lemma 12.1 implies that these determinants are $\mathrm{N}_{F/K}(\lambda)D_1$ and $\mathrm{N}_{F/K}(-d)\mathrm{N}_{F/K}(\lambda)D_1$; this completes the proof of the proposition. ∎

Notation 12.3. For all $\lambda \in F^\times$ and all integers $n \geqslant 1$, let $h_{n,\lambda}$ be the n-dimensional diagonal hermitian form $h_{n,\lambda} = \langle \lambda, 1, \dots, 1\rangle$ over E, and set $q_{n,\lambda} = \ell(h_{n,\lambda})$.

Proposition 12.4. *Let $\lambda \in F^\times$ and let $n \geqslant 1$ be an integer. We have*

$$w_2(q_{n,\lambda}) = w_2(q_{n,1}) + \mathrm{cor}_{F/K}(\lambda, d) \quad \textit{in } \mathrm{Br}_2(K).$$

To prove this proposition, we recall a theorem of Arason. If k is a field of characteristic $\neq 2$, we denote by $I(k)$ the ideal of even-dimensional forms of the Witt ring $W(k)$, and by $e_2 : I^2(k) \to \mathrm{Br}_2(k)$ the homomorphism sending a 2-fold Pfister form $\langle\langle a, b\rangle\rangle$ to the class of the quaternion algebra $(-a, -b)$ (see for instance [AEJ 84]).

Theorem 12.5 (Arason). *Let $s : F \to K$ be a non-trivial linear form. If $Q \in I^2(F)$, then $s(Q) \in I^2(K)$, and*

$$e_2(s(Q)) = \mathrm{cor}_{F/K}(e_2(Q)) \quad \textit{in } \mathrm{Br}_2(K).$$

Proof. See [AEJ 84, Theorem 1.21] or [Ar 75, Satz 4.1 and Satz 4.18]. ∎

Corollary 12.6. *If $Q \in I^2(F)$, then*

$$w_2(s(Q)) = \mathrm{cor}_{F/K}(w_2(Q)) \quad \textit{in } \mathrm{Br}_2(K).$$

Proof. [L 05, Proposition 3.20] implies that for $Q \in I^2(F)$, either $w_2(Q) = e_2(Q)$ or $w_2(Q) = e_2(Q) + (-1, -1)$. In the first case, there is nothing to prove; assume that $w_2(Q) = e_2(Q) + (-1, -1)$. We have $e_2(Q) = \mathrm{cor}_{F/K}(e_2(Q))$ by Theorem 12.5. Since $w_2(Q) = e_2(Q) + (-1, -1)$, we have

$$\begin{aligned}\mathrm{cor}_{F/K}(w_2(Q)) &= \mathrm{cor}_{F/K}(e_2(Q)) + (-1, (-1)^{[F:K]}) \\ &= \mathrm{cor}_{F/K}(e_2(Q))[F : K](-1, -1).\end{aligned}$$

On the other hand, $w_2(s(Q)) = e_2(s(Q)) + [F : k](-1. -1)$ (see [L 05, Proposition 3.20]), and this implies that $w_2(s(Q)) = \mathrm{cor}_{F/K}(w_2(Q))$, as claimed. ∎

For all $n \in \mathbf{N}$, set $D_n = \mathrm{N}_{F/K}(-d)^n$; Proposition 12.2 implies that

$$\det(q_{n,\lambda}) = D_n \quad \text{for all } \lambda \in F^\times.$$

Proof of Proposition 12.4. Assume first that $n = 1$, and let $s : F \to K$ be the restriction of $\ell : E \to K$ to F. Note that $\ell(h_{1,1}) = s(\langle 2, -2d\rangle)$, and $\ell(h_{1,\lambda}) = s(\langle 2, -2\lambda d\rangle)$.

Set $q_1 = \langle 2, -2d \rangle$, $q_2 = \langle 2, -2\lambda d \rangle$, and $Q = q_1 + q_2$. We have $w_2(Q) = w_2(q_1) + w_2(q_2) + (\det(q_1), \det(q_2)) = (\lambda, d) + (-1, d)$, hence

$$\mathrm{cor}_{F/K}(w_2(Q)) = \mathrm{cor}_{F/K}(\lambda, d) + (-1, N_{F/K}(-d)).$$

On the other hand, $w_2(s(Q)) = w_2(s(q_1)) + w_2(s(q_2)) + (\det(s(q_1)), \det(s(q_2)))$. By Proposition 12.2, we have $\det(s(q_1)) = \det(s(q_2)) = \mathrm{N}_{F/K}(-d)$, hence

$$w_2(s(Q)) = w_2(s(q_1)) + w_2(s(q_2)) + (-1, \mathrm{N}_{F/K}(-d)).$$

By Corollary 12.6, we have $w_2(s(Q)) = \mathrm{cor}_{F/K}(w_2(Q))$, therefore $w_2(s(q_1)) + w_2(s(q_2)) = \mathrm{cor}_{F/K}(\lambda, d)$. Since $q_{1,1} = \ell(h_{1,1}) = s(q_1)$ and $q_{1,\lambda} = \ell(h_{1,\lambda}) = s(q_2)$, this proves the proposition when $n = 1$.

Assume now that $n \geqslant 2$. We have

$$w_2(q_{n,\lambda}) = w_2(q_{1,\lambda}) + (D_1, D_{n-1}) + w_2(q_{n-1,1}),$$
$$w_2(q_{n,1}) = w_2(q_{1,1}) + (D_1, D_{n-1}) + w_2(q_{n-1,1}).$$

By the one-dimensional case, $w_2(q_{1,\lambda}) = w_2(q_{1,1}) + \mathrm{cor}_{F/K}(\lambda, d)$, hence

$$w_2(q_{n,\lambda}) = w_2(q_{n,1}) + \mathrm{cor}_{F/K}(\lambda, d),$$

as claimed. ∎

Local fields

Assume that K is a local field.

Lemma 12.7. *Two hermitian forms over E having the same dimension and determinant are isomorphic.*

Proof. See for instance [Sch 85, §10.1.6, (ii)]. ∎

Proposition 12.8. *Let $\lambda \in F^\times$, let h be an n-dimensional hermitian form of determinant λ over E, and set $q = \ell(h)$. We have*

$$w_2(q) = w_2(q_{n,1}) + \mathrm{cor}_{F/K}(\lambda, d) \quad \text{in } \mathrm{Br}_2(K).$$

Proof. If K is a non-archimedean local field, then by Lemma 12.7 the hermitian form h is isomorphic to the diagonal form $h_{n,\lambda} = \langle \lambda, 1, \dots, 1 \rangle$, hence the statement follows from Proposition 12.4.

Assume now that $K = \mathbf{R}$; then $F = K = \mathbf{R}$, and $E = \mathbf{C}$, hence $d = -1$. We have $h = \langle \lambda_1, \dots, \lambda_n \rangle = \langle \lambda_1 \rangle \oplus \cdots \oplus \langle \lambda_n \rangle$ with $\lambda_i \in \mathbf{R}$. Note that $\det(\ell(\langle \lambda_i \rangle) = 1$ for all i; hence

$$w_2(q) = \sum_{i \in I} w_2(\ell(\langle \lambda_i \rangle)) \quad \text{and} \quad w_2(q_{n,1}) = \sum_{i \in I} w_2(\ell(\langle 1 \rangle)).$$

We have $\ell(\lambda_i) = \langle 1, 1 \rangle$ if $\lambda_i > 0$, and $\ell(\lambda_i) = \langle -1, -1 \rangle$ if $\lambda_i < 0$; note that $w_2(\langle 1, 1 \rangle) = 0$ and $w_2(\langle -1, -1 \rangle) = 1$. This implies that $w_2(q) = w_2(q_{n,1})$ if and only if λ_i is negative for an even number of $i \in I$. On the other hand, $\mathrm{cor}_{F^v/K_v}(\lambda, d) = 0$ if and only if λ_i is negative for an even number of $i \in I$; this concludes the proof of the proposition. ∎

13. Obstruction

The aim of this section is to describe an obstruction group in a general situation. The group depends on a finite set I, a set V, and, for all $i, j \in I$, a subset $V_{i,j}$ of V; in the applications, the vanishing of the group detects the validity of the local-global principle (also called Hasse principle).

To obtain a necessary and sufficient condition for the Hasse principle to hold, we need additional data; in the applications, it is provided by local solutions. For all $v \in V$, we choose a set $\mathcal{C}^v$ having certain properties (see below for details); this set corresponds to the local data.

The basic setting

Let I be a finite set, let $\sim$ be an equivalence relation on I, and let $\overline{I}$ be the set of equivalence classes. Let $C(I)$ be the set of maps $I \to \mathbf{Z}/2\mathbf{Z}$. Let $C_\sim(I)$ be the subgroup of $C(I)$ consisting of the maps that are constant on equivalence classes, and note that $C_\sim(I) = C(\overline{I})$; it is a finite elementary abelian 2-group.

Let $Ш_\sim(I)$ be the quotient of $C_\sim(I)$ by the constant maps; equivalently, we can regard $Ш_\sim(I)$ as the quotient of $C(\overline{I})$ by the constant maps.

We start by giving a useful example.

Example 13.1. This example will be used in §14 and §18. We say that two finite extensions L_1 and L_2 of a field K are *independent over* K if the tensor product $L_1 \otimes_K L_2$ is a field. Let $E = \prod_{i \in I} E_i$ be a product of finite field extensions E_i of K, and let us consider the equivalence relation $\sim$ generated by the elementary equivalence

$$i \sim_e j \iff E_i \text{ and } E_j \text{ are independent over } K.$$

We denote by $Ш_{\mathrm{indep}}(E) = Ш_\sim(I)$ the quotient of $C_\sim(I)$ by the constant maps.

Equivalence relation on $C(I)$

As above, I is a finite set and $\sim$ an equivalence relation on I. If $i, j \in I$, let $c_{i,j} \in C(I)$ be such that $c_{i,j}(i) = c_{i,j}(j) = 1$ and $c_{i,j}(k) = 0$ if $k \neq i, j$. Let $(i, j) : C(I) \to C(I)$ be the map sending c to $c + c_{i,j}$. We also denote by $\sim$ the equivalence relation on $C(I)$ generated by the elementary equivalence

$$c \sim_e c' \iff c = (i, j)(c') \text{ for some } i, j \in I \text{ such that } i \sim j.$$

The following remark will be useful.

Lemma 13.2. *Let $a, b \in C(I)$ be such that $a \sim b$. Then*

$$\sum_{i \in I} c(i)a(i) = \sum_{i \in I} c(i)b(i) \quad \textit{for all } c \in C_\sim(I).$$

Proof. We can assume that $b = (i, j)(a)$ for some $i, j \in I$ with $i \sim j$. Since $c \in C_\sim(I)$, we have $c(i) = c(j)$, hence $\sum_{k \in I} c(k)a(k) = \sum_{k \in I} c(k)b(k)$, as claimed. ∎

The sets V, $V_{i,j}$ and the associated equivalence relations

Let V be a set, and for all $i, j \in I$, let $V_{i,j}$ be a subset of V. We take for $\sim$ the equivalence relation generated by

$$i \sim j \iff V_{i,j} \neq \varnothing,$$

and consider the equivalence relation $\sim$ on $C(I)$ generated by

$$c \sim c' \iff c = (i,j)(c') \text{ for some } i, j \in I \text{ with } V_{i,j} \neq \varnothing.$$

Let Ш $=$ Ш$_\sim(I)$ be the group corresponding to the equivalence relation $\sim$ defined as above.

For all $v \in V$, we define equivalence relations $\sim_v$ on I and $C(I)$, generated by

$$i \sim_v j \iff v \in V_{i,j},$$

and

$$c \sim_v c' \iff c = (i,j)(c') \text{ for some } i, j \in I \text{ with } v \in V_{i,j}.$$

Let $V = V' \cup V''$, and assume that for all $i, j \in I$, if $V_{i,j} \neq \varnothing$, then $V_{i,j} \cap V' \neq \varnothing$.

For all $v \in V$, let $A^v \in \mathbf{Z}/2\mathbf{Z}$ be such that

(i) $A^v = 0$ for almost all $v \in V$, and

$$\sum_{v \in V} A^v = 0.$$

For all $v \in V$, we consider subsets $\mathcal{C}^v$ of $C(I)$ satisfying conditions (ii) and (iii) below:

(ii) For all $a^v \in \mathcal{C}^v$, we have

$$\sum_{i \in I} a^v(i) = A^v.$$

(iii) If $v \in V'$, then $\mathcal{C}^v$ is stable by the maps (i,j) for $i \sim_v j$.

Let $\mathcal{C}$ be the set of $(a^v)_{v \in V}$ with $a^v \in \mathcal{C}^v$ such that $a^v = 0$ for almost all $v \in V$.

We now prove some results that will be useful in the following sections.

For all $a \in \mathcal{C}$ and $i \in I$, set

$$\Sigma_i(a) = \sum_{v \in V} a^v(i).$$

Proposition 13.3. *Let $a \in \mathcal{C}$, and let $i, j \in I$ with $i \sim j$. Then there exists $b \in \mathcal{C}$ such that $\Sigma_i(b) \neq \Sigma_i(a)$, $\Sigma_j(b) \neq \Sigma_j(a)$, and $\Sigma_k(b) = \Sigma_k(a)$ for all $k \neq i, j$.*

Proof. Let $i_1, \dots, i_k \in I$ be such that $i = i_1$, $j = i_k$, and $V_{i_s,i_{s+1}} \neq \varnothing$ for all $s = 1, \dots, k-1$; then $V_{i_s,i_{s+1}} \cap V' \neq \varnothing$ for all $s = 1, \dots, k-1$.

If $v \in V_{i_s,i_{s+1}} \cap V'$, then by condition (iii) the map (i_s, i_{s+1}) sends $\mathcal{C}^v$ to $\mathcal{C}^v$. Consider the map $\mathcal{C} \to \mathcal{C}$ that is equal to (i_s, i_{s+1}) on $\mathcal{C}^v$, and is the identity on $\mathcal{C}^w$ if $w \neq v$. Applying to $a \in \mathcal{C}$ the maps induced by $(i_1, i_2), \dots, (i_{k-1}, i_k)$ successively yields $b \in \mathcal{C}$ with the required properties. ∎

If $c \in Ш$ and $a = (a^v) \in \mathcal{C}$, then by conditions (i) and (ii) the sum

$$\sum_{v \in V} \sum_{i \in I} c(i) a^v(i)$$

is well-defined. The following result is used in §17 and §23 to give necessary and sufficient conditions for some Hasse principles to hold.

Theorem 13.4. *Let $a = (a^v) \in \mathcal{C}$ be such that*

$$\sum_{v \in V} \sum_{i \in I} c(i) a^v(i) = 0 \quad \textit{for all } c \in Ш.$$

Then there exists $b = (b^v) \in \mathcal{C}$ such that

$$\sum_{v \in V} b^v(i) = 0 \quad \textit{for all } i \in I.$$

Proof. If $\Sigma_i(a) = 0$ for all $i \in I$, then we are done. Assume that $\Sigma_{i_0}(a) = 1$. We claim that there exists $i \in I$ with $i \neq i_0$ and $i \sim i_0$ such that $\Sigma_i(a) = 1$. In order to prove this claim, let $c \in C(I)$ be such that $c(i_0) = 1$ and $c(i) = 0$ if $i \neq i_0$. Then

$$\sum_{v \in V} \sum_{i \in I} c(i) a^v(i) = \Sigma_{i_0}(a) = 1,$$

hence $c \notin Ш$. Therefore c is not constant on equivalence classes. This implies that there exists $i_1 \in I$ with $i_1 \neq i_0$ such that $i_1 \sim i_0$. If $\Sigma_{i_1}(a) = 1$, we stop. Otherwise, let $c \in C(I)$ be such that $c(i_0) = c(i_1) = 1$ and $c(i) = 0$ if $i \neq i_0, i_1$. We again have

$$\sum_{v \in V} \sum_{i \in I} c(i) a^v(i) = \Sigma_{i_0}(a) = 1,$$

hence $c \notin Ш$. Therefore c is not constant on equivalence classes. This implies that there exists $i_2 \in I$, $i_2 \neq i_0, i_1$, such that either $i_2 \sim i_0$ or $i_2 \sim i_1$. Note that since $i_1 \sim i_0$, we have $i_2 \sim i_0$ in both cases. Since I is finite and $\sum_{v \in V} \sum_{i \in I} c(i) a^v(i) = 0$, we eventually get $i_r \in I$ with $i_r \neq i_0$, $i_r \sim i_0$, and $\Sigma_{i_r}(a) = 1$. By Proposition 13.3, there exists $b \in \mathcal{C}$ such that

$$\Sigma_{i_0}(b) = \Sigma_{i_r}(b) = 0.$$

Continue inductively until the theorem is proved. ∎

Under some additional hypothesis on $\mathcal{C}^v$ for $v \in V''$, a necessary and sufficient condition for the Hasse principle can be given by the vanishing of a homomorphism:

The homomorphism

Let us make the additional assumption that

(iv) For all $v \in V$, the set $\mathcal{C}^v$ is a subset of a $\sim_v$-equivalence class of $C(I)$.

Let $a \in \mathcal{C}$. We define a homomorphism $\alpha = \alpha_a : Ш \to \mathbf{Z}/2\mathbf{Z}$ as follows. For all $c \in Ш$, we set

$$\alpha(c) = \sum_{v \in V} \sum_{i \in I} c(i) a^v(i).$$

Note that this is well-defined, since by conditions (i) and (ii),

$$\sum_{v \in V} \sum_{i \in I} a^v(i) = \sum_{v \in V} A^v = 0.$$

Proposition 13.5. *The homomorphism α is independent of the choice of $a \in \mathcal{C}$.*

Proof. Let $a = (a^v), b = (b^v) \in \mathcal{C}$, and let us show that $\alpha_a = \alpha_b$. Let $v \in V$. Since $a^v, b^v \in \mathcal{C}^v$, we have $a^v \sim_v b^v$, hence $a^v \sim b^v$. Therefore by Lemma 13.2, we have

$$\sum_{i \in I} c(i) a^v(i) = \sum_{i \in I} c(i) b^v(i).$$

This holds for all $v \in V$, hence $\alpha_a = \alpha_b$. ∎

Corollary 13.6. *Let $a \in \mathcal{C}$, and assume that $\alpha_a = 0$. Then there exists $b = (b^v) \in \mathcal{C}$ such that*

$$\sum_{v \in V} b^v(i) = 0 \quad \textit{for all } i \in I.$$

Proof. This follows from Theorem 13.4. ∎

14. Obstruction group – the rational case

The aim of this section is to associate an "obstruction group" to certain algebras with involution; this group will play an important role in the Hasse principle results of the following sections.

Assume that K is a global field of characteristic $\neq 2$, and let I be a finite set. For all $i \in I$, let E_i be a finite degree extension of K, and let $\sigma_i : E_i \to E_i$ be a non-trivial involution; let F_i be the fixed field of σ_i, and let $d_i \in F_i^\times$ be such that $E_i = F_i(\sqrt{d_i})$. Set $F = \prod_{i \in I} F_i$ and $E = \prod_{i \in I} E_i$; let $\sigma : E \to E$ be the involution such that the restriction of σ to E_i is equal to σ_i.

We denote by V_K the set of places of K.

Notation 14.1. For all $i \in I$, let V_i be the set of places $v \in V_K$ such that there exists a place of F_i above v which is inert or ramified in E_i.

Let $Ш = Ш_E$ be the group constructed in §13 using the data I and $V_{i,j} = V_i \cap V_j$; recall that the equivalence relation $\sim$ on I is generated by the elementary equivalence

$$i \sim_e j \iff V_i \cap V_j \neq \varnothing;$$

$C_\sim(I)$ is the subgroup of $C(I)$ consisting of the maps $I \to \mathbf{Z}/2\mathbf{Z}$ that are constant on equivalence classes; and $Ш_E$ is the quotient of $C_\sim(I)$ by the constant maps.

In the remainder of the section, we give some examples and some results that will be used in the next sections. We start by giving some examples in which the obstruction group is trivial.

Example 14.2. Assume that there exists a real place v of K such that for all $i \in I$, there exists a real place of F_i above v which extends to a complex place of E_i. Then $Ш_E = 0$. Indeed, $v \in V_i$ for all $i \in I$, hence $V_i \cap V_j \neq \varnothing$ for all $i, j \in I$. Therefore all the elements of I are equivalent, and this implies that $Ш_E = 0$.

In particular, if $K = \mathbf{Q}$, and if for all $i \in I$, the field E_i is a CM field (that is, E_i is totally complex and F_i is totally real), then $Ш_E = 0$.

Recall that two finite extensions K_1 and K_2 of K are *independent* if the tensor product $K_1 \otimes_K K_2$ is a field. If K_1 and K_2 are subfields of a field extension Ω of K, then this means that K_1 and K_2 are linearly disjoint.

Proposition 14.3. *Assume that E_i and E_j are independent field extensions of K. Then $V_{i,j} \neq \varnothing$.*

Proof. Let Ω/K be a Galois extension containing E_i and E_j, and set $G = \mathrm{Gal}(\Omega/L)$. Let $H_i \subset G_i$ and $H_j \subset G_j$ be subgroups of G such that $E_i = \Omega^{H_i}$, $E_j = \Omega^{H_j}$ and $F_i = \Omega^{G_i}$, $F_j = \Omega^{G_j}$. Since E_i/F_i and E_J/F_J are quadratic extensions, the subgroup H_i is of index 2 in G_i, and H_j is of index 2 in G_j. By hypothesis, E_i and E_j are linearly disjoint over K, therefore $[G : H_i \cap H_j] = [G : H_i][G : H_j]$. Note that F_i and F_j are also linearly disjoint over K, hence $[G : G_i \cap G_j] = [G : G_i][G : G_j]$. This implies that $[G_i \cap G_j : H_i \cap H_j] = 4$, hence the quotient $G_i \cap G_j/H_i \cap H_j$ is an elementary abelian group of order 4.

The field Ω contains the composite fields F_iF_j and E_iE_j. By the above argument, the extension E_iE_j/F_iF_j is biquadratic. Hence there exists a place of F_iF_j that is inert in both E_iF_j and E_jF_i. Therefore there exists a place v of K and places w_i of F_i and w_j of F_j above v such that w_i is inert in E_i, and w_j is inert in E_j, hence $v \in V_i \cap V_j$; by definition, this implies that $v \in V_{i,j}$. ■

Recall from §13, Example 13.1, the equivalence relation $\approx$ on I generated by the elementary equivalence

$$i \approx_e j \iff E_i \text{ and } E_j \text{ are independent over } K,$$

and recall the associated obstruction group $Ш_{\mathrm{indep}}(E) = Ш_\approx(I)$ (see §13). Proposition 14.3 implies that the identity $C(I) \to C(I)$ induces a surjection $Ш_{\mathrm{indep}}(E) \to Ш_E$. Hence we have

Corollary 14.4. *Assume that $Ш_{\mathrm{indep}}(E) = 0$. Then $Ш_E = 0$.*

On the other hand, one can show that all elementary abelian 2-groups occur as $Ш_E$ for some (E, σ).

Finally, we show a result that will be used in §20 to prove an odd degree descent property. Let K'/K be a finite extension of odd degree. We define a homomorphism

$$Ш_E \to Ш_{E \otimes_K K'}$$

as follows. For all $i \in I$, let $F_i \otimes_K K' = \prod_{j \in I(i)} F'_{i,j}$, where $F'_{i,j}$ is a field extension of K'. Set

$$I' = \{(i,j) \mid i \in I,\ j \in I(i) \text{ and the image of } d_i \text{ in } F'_{i,j} \text{ is not a square}\}.$$

Let $\pi : I' \to I$ be the map sending (i,j) to i; this map induces a homomorphism $\pi' : C(I) \to C(I')$.

Proposition 14.5. *The map $\pi' : C(I) \to C(I')$ induces an injective homomorphism*

$$\pi' : Ш_E \to Ш_{E \otimes_K K'}.$$

Proof. Let us show that π' sends $C_\sim(I)$ to $C_\sim(I')$. Let $(i_1, j_1), (i_2, j_2) \in I'$ be such that $(i_1, j_1) \sim_e (i_2, j_2)$; by definition, this means that $V_{(i_1,j_1),(i_2,j_2)} \neq \varnothing$. Let $v' \in V_{(i_1,j_1),(i_2,j_2)}$, and let $v \in V_K$ be the restriction of v' to K. Then $v \in V_{i_1,i_2}$, hence $i_1 \sim_e i_2$. This shows that if $c \in C_\sim(I)$, then $\pi'(c) \in C_\sim(I')$, hence we have a well-defined homomorphism $C_\sim(I) \to C_\sim(I')$. This in turn induces a homomorphism $\pi' : Ш_E \to Ш_{E \otimes_K K'}$, and it is clearly injective. ■

Finally, note that one can give a simpler description of the obstruction group of [BLP 18] in the framework of this section (see [B 20, §2]).

15. Twisting groups and equivalence relations

In this section, we introduce some notation that will be used throughout the paper; we also prove some results concerning equivalence relations defined on the twisting groups.

We keep the notation of §14. If $v \in V_K$, we denote by K_v the completion of K at v, and set $E_i^v = E_i \otimes_K K_v$ and $F_i^v = F_i \otimes_K K_v$.

Notation 15.1. For all $i \in I$, let S_i be the set of places w of F_i such that $E_i \otimes_{F_i} (F_i)_w$ is a field. If $w \in S_i$, set $E_i^w = E_i \otimes_{F_i} (F_i)_w$, and let

$$\theta_i^w : T(E_i^w, \sigma_i) \to \mathbf{Z}/2\mathbf{Z}$$

be the isomorphism defined in (10.1). If $v \in V_K$, we denote by S_i^v the set of places of S_i above v. For all $v \in V_K$, set

$$T(E_i^v, \sigma_i) = \prod_{w \in S_i^v} T(E_i^w, \sigma_i), \quad T(E^v, \sigma) = \prod_{i \in I} T(E_i^v, \sigma_i).$$

Recall that $C(I)$ is the set of maps $I \to \mathbf{Z}/2\mathbf{Z}$. For all $\lambda^v = (\lambda_i^w) \in T(E^v, \sigma)$, we define $a(\lambda^v) \in C(I)$ by setting

$$a(\lambda^v)(i) = \sum_{w \in S_i^v} \theta_i^w(\lambda_i^w).$$

Let $\tilde{C}(I)$ be the set of maps $I \to \mathbf{Q}/\mathbf{Z}$. If $\lambda^v = (\lambda_i^w) \in T(E^v, \sigma)$, let $\tilde{a}(\lambda^v) \in \tilde{C}(I)$ be defined by

$$\tilde{a}(\lambda^v)(i) = \mathrm{inv}_v(\mathrm{cor}_{F^v/K_v}(\lambda_i^v, d_i)).$$

For all $v \in V_K$, let $C_{T^v}(I)$ be the subset of $C(I)$ consisting of the maps $a(\lambda^v)$ for $\lambda^v \in T(E^v, \sigma)$. Similarly, denote by $\tilde{C}_{T^v}(I)$ the subset of $C(I)$ consisting of the maps $\tilde{a}(\lambda^v)$ for $\lambda^v \in T(E^v, \sigma)$.

Lemma 15.2. *Let $v \in V_K$. Sending $a(\lambda^v)$ to $\tilde{a}(\lambda^v)$ yields a bijection $C_{T^v}(I) \to \tilde{C}_{T^v}(I)$.*

Proof. Let $\iota : \mathbf{Z}/2\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ be the canonical injection, and let ι also denote the induced injection $C(I) \to \tilde{C}(I)$. Let us show that $\tilde{a}(\lambda^v) = \iota \circ a(\lambda^v)$ for all $\lambda^v \in T(E^v, \sigma)$.

Recall from (10.1) that for all $\lambda^v = (\lambda_i^w) \in T(E^v, \sigma)$, the injection $\iota : \mathbf{Z}/2\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ sends $\theta_i^w(\lambda_i^w)$ to $\mathrm{inv}_w(\lambda_i^w, d_i)$. Since $a(\lambda^v)(i) = \sum_{w \in S_i^v} \theta_i^w(\lambda_i^v)$, the injection $\iota : C(I) \to \tilde{C}(I)$ sends $a(\lambda^v)(i)$ to $\sum_{w \in S_i^v} \mathrm{inv}_w(\lambda_i^w, d_i)$. By (10.2), this is equal to $\sum_{w \in S_i^v} \mathrm{inv}_v(\mathrm{cor}_{(F_{i,w}/K_v}(\lambda_i^w, d_i))$, which in turn is equal to $\mathrm{inv}_v(\mathrm{cor}_{F^v/K_v}(\lambda_i^v, d_i))$; hence $\tilde{a}(\lambda^v) = \iota \circ a(\lambda^v)$, as claimed. ∎

Note that $C(I)$ is a group, and $C_{T^v}(I)$ is a subgroup of $C(I)$.

Recall that for all $i \in I$, we denote by V_i the set of places $v \in V_K$ such that there exists a place of F_i above v which is inert or ramified in E_i. Note that

$$v \in V_i \iff S_i^v \neq \varnothing.$$

Lemma 15.3. *The subgroup $C_{T^v}(I)$ of $C(I)$ is stable by the maps (i, j) for $v \in V_i \cap V_j$.*

Proof. Let $v \in V_i \cap V_j$, and let $\lambda^v = (\lambda_i^w) \in T(E^v, \sigma)$. Let $(+1) : \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ be the map sending n to $n + 1$. Let $w_i \in S_i^v$ and $w_j \in S_j^v$. Set

$$\mu_i^{w_i} = [(\theta_i^{w_i})^{-1} \circ (+1) \circ \theta_j^{w_j}](\lambda_j^{w_j}), \quad \mu_j^{w_j} = [(\theta_j^{w_j})^{-1} \circ (+1) \circ \theta_i^{w_i}](\lambda_i^{w_i}),$$

and $\mu_r^w = \lambda_r^w$ for all $(r, w) \neq (i, w_i), (j, w_j)$. Then $\mu^v = (\mu_i^w) \in T(E^v, \sigma)$, and

$$a(\mu^v) = (i, j)a(\lambda^v).$$ ∎

Let $v \in V_K$ and $A^v \in \mathbf{Z}/2\mathbf{Z}$.

Notation 15.4. Let $\mathcal{L}_{A^v}$ be the set of $\lambda^v = (\lambda_i^w) \in T(E^v, \sigma)$ such that

$$A^v = \sum_{i \in I} a(\lambda^v)(i),$$

and let $\mathcal{C}_{A^v}$ be the set of $a(\lambda^v)$ for $\lambda^v \in \mathcal{L}_{A^v}$.

Let $\equiv_v$ be the equivalence relation on $C(I)$ generated by

$$c \equiv_v c' \iff c = (i, j)(c') \text{ for some } i, j \in I \text{ with } v \in V_i \cap V_j.$$

Proposition 15.5. *The set $\mathcal{C}_{A^v}$ is an $\equiv_v$-equivalence class of $C(I)$.*

Proof. Let us first show that $\mathcal{C}_{A^v}$ is stable by the maps (i, j) for $v \in V_i \cap V_j$. Let $\lambda^v \in \mathcal{L}_{A^v}$. By Lemma 15.3, there exists $\mu^v \in T(E^v, \sigma)$ such that $a(\mu^v) = (i, j)a(\lambda^v)$. Note that this implies that

$$\sum_{r \in I} a(\mu^v)(r) = \sum_{r \in I} a(\lambda^v)(r) = A^v,$$

hence $\mu^v \in \mathcal{L}_{A^v}$.

Let us show that if $\lambda^v, \mu^v \in \mathcal{L}_{A^v}$, then $a(\lambda^v) \equiv_v a(\mu^v)$. If $a(\lambda^v)(i) = a(\mu^v)(i)$ for all $i \in I$, there is nothing to prove. Suppose that there exists $i \in I$ such that $a(\lambda^v)(i) \neq a(\mu^v)(i)$; then $S_i^v \neq \varnothing$, hence $v \in V_i$. By hypothesis, we have

$$\sum_{r \in I} a(\mu^v)(r) = \sum_{r \in I} a(\lambda^v)(r) = A^v,$$

therefore there exists $j \in I$, $j \neq i$, such that $a(\lambda^v)(j) \neq a(\mu^v)(j)$. This implies that $v \in V_j$, hence $v \in V_i \cap V_j$. The map $(i, j)a(\lambda^v)$ differs from $a(\mu^v)$ at fewer elements than $a(\lambda^v)$ does. Since I is a finite set, continuing this way we see that $a(\lambda^v) \equiv_v a(\mu^v)$. ■

16. Local data – the rational case

We keep the notation of §15; in particular, K is a global field of characteristic $\neq 2$. Let M be an A-module satisfying the hypotheses of §7 with $\mathcal{A}_M = (E_i)_{i \in I}$. Recall that E_i/K is a finite field extension of K and that $\sigma(E_i) = E_i$ for all $i \in I$. In addition, assume that for all $i \in I$, *the restriction of* σ *to* E_i *is non-trivial*. The fixed field of this involution is denoted by F_i; hence E_i/F_i is a quadratic extension, and $E_i = F_i(\sqrt{d_i})$ for some $d_i \in F_i^\times$. Set $F = \prod_{i \in I} F_i$ and $E = \prod_{i \in I} E_i$.

Let $v \in V_K$, and let q be a quadratic form over K_v which is compatible with the module $M \otimes_K K_v$. We now associate to q and M a subset of $T(E^v, \sigma)$.

We have $M \simeq \bigoplus_{i \in I} M_i$ with M_i isotypic, such that M_i is a finite-dimensional E_i-vector space. By Proposition 7.1 there exist quadratic forms q_i^v over K_v compatible with $M_i \otimes_K K_v$ such that $q \simeq \bigoplus_{i \in I} q_i^v$. Set $n_i = \dim_{E_i}(M_i)$. By Proposition 7.4 there exist n_i-dimensional hermitian forms h_i^v over E_i^v such that $q_i^v \simeq \ell_i(h_i^v)$. Set $\lambda_i^v = \det(h_i^v)$, and denote by $\mathcal{LR}_i^v$ the set of $\lambda_i^v \in T(E_i^v, \sigma_i)$ obtained this way. Let $\lambda^v = (\lambda_i^v)$, and denote by $\mathcal{LR}^v$ the set of λ^v with $\lambda_i^v \in \mathcal{LR}_i^v$. Let $\mathcal{CR}^v$ be the set of $a^v = a(\lambda^v) \in C_{T^v}(I)$ with $\lambda^v \in \mathcal{LR}^v$ (cf. §15). Let $d = (d_i)$, and set $q_{n,1} = \bigoplus_{i \in I} q_{n_i,1}$.

Proposition 16.1. *Let* $\lambda^v \in \mathcal{LR}^v$. *Then*

$$w_2(q) = w_2(q_{n,1}) + \mathrm{cor}_{F/K}(\lambda^v, d) \quad \text{in } \mathrm{Br}_2(K_v).$$

Proof. By Proposition 12.8, we have $w_2(q_i^v) = w_2(q_{n_i,1}) + \mathrm{cor}_{F/K}(\lambda_i^v, d_i)$ in $\mathrm{Br}_2(K_v)$ for all $i \in I$ and all $v \in V_K$. Using [Sch 85, Chapter 2, Lemma 12.6] gives the desired result, noting that $\det(q_i^v) = \det(q_{n_i,1})$ for all $i \in I$ and $v \in V_K$. ■

Set $\tilde{A}^v = \mathrm{inv}_v(w_2(q) + w_2(q_{n,1}))$. Recall that for $\lambda^v = (\lambda_i^w) \in T(E^v, \sigma)$, we defined $\tilde{a}(\lambda^v) \in \tilde{C}(I)$ by $\tilde{a}(\lambda^v)(i) = \mathrm{inv}_v(\mathrm{cor}_{F^v/K_v}(\lambda_i^v, d_i))$. Let $\tilde{\mathcal{L}}_{\tilde{A}^v}$ be the set of $\lambda^v = (\lambda_i^w) \in T(E^v, \sigma)$ such that

$$\tilde{A}^v = \sum_{i \in I} \tilde{a}(\lambda^v)(i),$$

and let $\tilde{\mathcal{C}}_{\tilde{A}}$ be the set of $\tilde{a}(\lambda^v)$ for $\lambda^v \in \tilde{\mathcal{L}}_{\tilde{A}^v}$.

Let $\iota : \mathbf{Z}/2\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ be the canonical injection, and let $A \in \mathbf{Z}/2\mathbf{Z}$ be such that $\iota(A) = \tilde{A}$. Recall that $\mathcal{L}_{A^v}$ is the set of $\lambda^v = (\lambda_i^v) \in T(E^v, \sigma)$ such that

$$A^v = \sum_{i \in I} a(\lambda^v)(i),$$

and $\mathcal{C}_{A^v}$ is the set of $a(\lambda^v)$ for $\lambda^v \in \mathcal{L}_{A^v}$.

Proposition 16.2. *The set $\mathcal{CR}^v$ is contained in $\mathcal{C}_{A^v}$.*

Proof. Let us first note that if $\lambda^v \in \mathcal{LR}^v$, then $\tilde{a}(\lambda^v)$ belongs to $\tilde{\mathcal{C}}_{\tilde{A}^v}$. Indeed, since $\mathrm{inv}_v(\mathrm{cor}_{F^v/K_v}(\lambda^v, d)) = \sum_{i \in I} \mathrm{inv}_v(\mathrm{cor}_{F^v/K_v}(\lambda_i^v, d_i))$, this is a consequence of Proposition 16.1; the assertion now follows from Lemma 15.2. ■

Corollary 16.3. *The set $\mathcal{CR}^v$ is contained in an $\equiv_v$-equivalence class of $C(I)$.*

Proof. This follows from Propositions 16.2 and 15.5. ■

Local data – finite places

In the case of finite places, we have more precise information: as we will see, the sets $\mathcal{CR}^v$ and $\mathcal{C}_{A^v}$ coincide, and hence $\mathcal{CR}^v$ is an $\equiv_v$-equivalence class.

If $\lambda^v = (\lambda_i^v) \in T(E^v, \sigma)$ for some $v \in V_K$, set $q_{n,\lambda^v} = \bigoplus_{i \in I} q_{n_i, \lambda_i^v}$.

Proposition 16.4. *Suppose that v is a finite place. Then $\mathcal{L}R^v$ is equal to the set of $\lambda^v \in T(E^v, \sigma)$ such that $q \simeq q_{n,\lambda^v}$.*

Proof. It is clear that if $\lambda^v \in T(E^v, \sigma)$ is such that $q \simeq q_{n,\lambda^v}$, then $\lambda^v \in \mathcal{L}R^v$. Conversely, let $\lambda^v \in \mathcal{L}R^v$, and let h^v be a hermitan form over E^v such that $q \simeq \ell(h^v)$ and $\det(h^v) = \lambda^v$. By Lemma 12.7 we have $h^v \simeq h_{n,\lambda^v}$, hence $q \simeq q_{n,\lambda^v}$. ■

Proposition 16.5. *Suppose that v is a finite place. Let $\lambda^v \in T(E^v, \sigma)$. Then $\lambda^v \in \mathcal{LR}^v$ if and only if*

$$w_2(q) = w_2(q_{n,1}) + \mathrm{cor}_{F/K}(\lambda^v, d) \quad \textit{in } \mathrm{Br}_2(K_v).$$

Proof. One implication is Proposition 16.1. Let us show the converse. If $w_2(q_{n,\lambda^v}) = w_2(q_{n,1}) + \mathrm{cor}_{F/K}(\lambda^v, d)$ in $\mathrm{Br}_2(K_v)$, then $w_2(q_{n,\lambda^v}) = w_2(q)$ in $\mathrm{Br}_2(K_v)$. By Proposition 12.2, $\det(q_{n,\lambda^v}) = \det(q)$ in $K_v^\times/K_v^{\times 2}$, so the quadratic forms q and $q_{n,\lambda}$ have the same dimension, determinant and Hasse–Witt invariant; hence they are isomorphic over K_v. This implies that $\lambda^v \in \mathcal{LR}^v$. ■

Proposition 16.6. *Suppose that v is a finite place. Then $\mathcal{CR}^v = \mathcal{C}_{A^v}$.*

Proof. By Proposition 16.5, we have $\mathcal{CR}^v = \tilde{\mathcal{C}}_{\tilde{A}^v}$; hence the statement follows from Lemma 15.2. ∎

Corollary 16.7. *Suppose that v is a finite place. Then $\mathcal{CR}^v$ is an $\equiv_v$-equivalence class of $C(I)$.*

Proof. This follows from Propositions 16.6 and 15.5. ∎

Local data – real places

Suppose that $v \in V_K$ is a real place. We say that a quadratic form q has *maximal signature at v* (with respect to M) if the signature of q at v is equal to the signature of $q_{n,1}$ or of $-q_{n,1}$ at v.

Proposition 16.8. *Assume that q does not have maximal signature at v, and let $a \in \mathcal{C}R^v$. Then there exist $i, j \in I$ with $v \in V_i \cap V_j$ such that $(i, j)a$ belongs to $\mathcal{C}R^v$.*

Proof. Let $\lambda^v = (\lambda_r^w) \in \mathcal{LR}^v$ be such that $a = a(\lambda^v)$. Since the signature of q at v is not maximal, there exist $i, j \in I$ with $v \in V_i \cap V_j$ and $w_i \in V_{F_i}$, $w_j \in V_{F_j}$ above v such that $\lambda_i^{w_i}$ and $\lambda_j^{w_j}$ have opposite signs ($\lambda_i^{w_i} > 0$ and $\lambda_j^{w_j} < 0$, or vice versa). For all $r \in I$ and $w \in V_{F_r}$ above v, let $\mu_r^w \in T(E_r^w, \sigma)$ be such that $\mu_r^w = \lambda_r^w$ if $(w, r) \neq (w_i, i), (w_j, j)$, while $\mu_i^{w_i} = -\lambda_i^{w_i}$ and $\mu_j^{w_j} = -\lambda_j^{w_j}$. Then $\mu^v = (\mu_r^w) \in \mathcal{CR}^v$, and $a(\mu^v) = (i, j)a(\lambda^v)$. ∎

17. Local-global problem – the rational case

We keep the notation of the previous sections; in particular, M is an A-module satisfying the hypotheses of §16, and $\mathcal{A}_M = (E_i)_{i \in I}$. If (V, q) is a quadratic form over K, we consider the following local and global conditions:

(L1) *For all $v \in V_K$, the quadratic form $(V, q) \otimes_K K_v$ is compatible with the module $M \otimes_K K_v$.*

(G1) *The quadratic form (V, q) is compatible with the module M.*

Proposition 17.1. *Assume that condition* (L1) *is satisfied. Then condition* (G1) *holds if and only if there exists $\lambda = (\lambda_i) \in T(E, \sigma)$ such that $\lambda \in \mathcal{LR}^v$ for all $v \in V_K$.*

Proof. We have $M \simeq \bigoplus_{i \in I} M_i$ with M_i isotypic such that M_i is a finite-dimensional E_i-vector space. If (G1) holds, then $q \simeq \bigoplus_{i \in I} q_i$, where the quadratic form q_i is compatible with M_i (cf. Proposition 7.1). For all $i \in I$, let h_i be a hermitian form over E_i such that $q_i = \ell_i(h_i)$, set $\lambda_i = \det(h_i)$, and $\lambda = (\lambda_i)$; then $\lambda \in \mathcal{LR}^v$ for all $v \in V_K$.

Let us prove the converse. Let $\lambda = (\lambda_i) \in T(E, \sigma)$ be such that $\lambda \in \mathcal{LR}^v$ for all $v \in V_K$, and let h_i be a hermitian form of dimension n_i over E_i with $\det(h_i) = \lambda_i$ and

$\mathrm{sign}_v(h_i) = \mathrm{sign}_v(h_i^v)$ for all real places $v \in V_K$; for the existence of such a form, see for instance [Sch 85, §10.6.9]. Let $q_i = \ell_i(h_i)$ and $q' = \bigoplus_{i \in I} q_i$. The quadratic form q' is compatible with M by construction; its dimension, signatures and determinant are the same as those of q [this is clear for the dimension and the signatures; for the determinant, it follows from Proposition 12.2]. By Proposition 12.8, we have

$$\mathrm{cor}_{F^v/K_v}(\lambda, d) = w_2(q') + w_2(q_{n,1}) \quad \text{in } \mathrm{Br}_2(K_v)$$

for all $v \in V_K$. On the other hand, since $\lambda \in \mathcal{LR}^v$ for all $v \in V_K$, by Proposition 16.1 we have $\mathrm{cor}_{F^v/K_v}(\lambda, d) = w_2(q) + w_2(q_{n,1})$ in $\mathrm{Br}_2(K_v)$ for all $v \in V_K$; therefore $w_2(q') = w_2(q)$ in $\mathrm{Br}_2(K)$. This implies that $q' \simeq q$, hence (G1) holds. ■

Recall from §14 the definition of the group $\text{Ш}_E = \text{Ш}_{E,\sigma}$; recall that for all $v \in V_K$ and $i \in I$, the set S_i^v consists of those places w of F_i such that $E_i \otimes_{F_i} (F_i)_w$ is a field, and if $i \in I$, we denote by V_i the set of places $v \in V_K$ such that $S_i^v \neq \varnothing$. The group Ш_E is the one constructed in §13 using the data I and $V_{i,j} = V_i \cap V_j$; see §14 for details.

Note that Ш_E does not depend on the module M, only on the algebra E with involution.

Theorem 17.2. (i) *Assume that $\text{Ш}_E = 0$, and let q be a quadratic form such that* (L1) *holds. Then* (G1) *holds as well.*

(ii) *If $\text{Ш}_E \neq 0$, then there exists a quadratic form satisfying* (L1) *but not* (G1).

The proof of this theorem will be given later, after the construction of the obstruction homomorphism.

If the obstruction group Ш_E is not trivial, then the validity of the Hasse principle also depends on the choice of the quadratic form.

Local data

Let q be a non-degenerate quadratic form over K, and assume that condition (L1) holds. Recall from Section 16 that a local solution gives rise to sets $\mathcal{LR}^v$ and $\mathcal{CR}^v$ for all $v \in V_K$.

Let $\mathcal{CR}$ be the set of (a^v), $a^v \in \mathcal{CR}^v$, such that $a^v = 0$ for almost all $v \in V_K$. Let us show that this set is not empty.

Proposition 17.3. *Assume that condition* (L1) *holds. Then the set $\mathcal{CR}$ is not empty.*

Proof. Let S be the subset of V_K consisting of the places $v \in V_K$ such that $A^v \neq 0$ and of the infinite places; this is a finite set.

Let $v \in V_K$ be such that $v \notin S$. Let $\lambda^v \in \mathcal{LR}^v$, and assume that there exists $i \in I$ such that $a(\lambda^v)(i) \neq 0$. Recall that $A^v = \sum_{r \in I} a(\lambda^v)(r)$. Since $v \notin S$, by hypothesis $A^v = 0$; therefore there exists $j \in I$, $j \neq i$, with $a(\lambda^v)(j) \neq 0$. Note that since $a(\lambda^v)(i) \neq 0$ and $a(\lambda^v)(j) \neq 0$, we have $S_i^v \neq \varnothing$ and $S_j^v \neq \varnothing$, hence $v \in V_i \cap V_j$.

We know that v is a finite place, since $v \notin S$; hence by Proposition 16.7, the map $(i,j)a(\lambda^v)$ belongs to $\mathcal{CR}^v$. Moreover, this map vanishes at i and j. If $(i,j)a(\lambda^v) = 0$, we stop; otherwise we continue, and after a finite number of steps we obtain the zero element of $C(I)$. Since this holds for all $v \in V_K$ such that $v \notin S$, the proposition is proved. ∎

The homomorphism and the Hasse principle

We apply the results of §13 with the sets $\mathcal{C}^v = \mathcal{CR}^v$, and $\sim_v$ will be the equivalence relation $\equiv_v$ defined in Section 15.

For all $v \in V_K$, set $\tilde{A}^v = \mathrm{inv}_v(w_2(q) + w_2(q_{n,1}))$. Let $\iota : \mathbf{Z}/2\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ be the canonical injection, and let $A^v \in \mathbf{Z}/2\mathbf{Z}$ be such that $\iota(A^v) = \tilde{A}^v$. Note that q and $q_{n,1}$ are quadratic forms over K, hence $\tilde{A}^v = 0$ for almost all $v \in V_K$, and $\sum_{v \in V_K} \tilde{A}^v = 0$; the same properties hold for A^v, therefore condition (i) of §13 holds.

Let V' be the set of finite places, and V'' be the set of infinite places of K. The sets $\mathcal{CR}^v$ satisfy conditions (ii)–(iv) of Section 13: indeed, condition (ii) follows from Proposition 16.2, condition (iii) from Corollary 16.7, and (iv) from Corollary 16.3.

Let $(a(\lambda^v)) \in \mathcal{CR}$. As in §13, we define a homomorphism $\rho : Ш_E \to \mathbf{Z}/2\mathbf{Z}$ as follows. For all $c \in Ш_E$, set

$$\rho(c) = \sum_{v \in V_K} \sum_{i \in I} c(i) a(\lambda^v)(i).$$

By Proposition 13.5, the homomorphism ρ is independent of the choice of $(a(\lambda^v)) \in \mathcal{CR}$.

Theorem 17.4. *Let q be a quadratic form, and assume that condition* (L1) *holds. Then condition* (G1) *holds if and only if $\rho = 0$.*

Proof. If (G1) holds, then by Proposition 17.1 there exists $\lambda = (\lambda_i) \in T(E, \sigma)$ such that $\lambda \in \mathcal{LR}^v$ for all $v \in V_K$; then $\sum_{v \in V_K} a(\lambda)(i) = 0$ for all $i \in I$, hence $\rho = 0$.

Let us prove the converse. Since $\rho = 0$, Corollary 13.6 implies that there exists $b = (b^v) \in \mathcal{CR}$ such that $\sum_{v \in V_K} b^v(i) = 0$ for all $i \in I$. By definition, there exists $(\lambda^v) \in \mathcal{LR}$ such that $b^v = a(\lambda^v)$ for all $v \in V_K$. Recall that $a(\lambda^v)(i) = \sum_{w \in S_v} \theta_i^w(\lambda_i^w)$; therefore for all $i \in I$, we have $\sum_{w \in V_F} \theta_i^w(\lambda_i^w) = 0$. By Theorem 10.1 this implies that for all $i \in I$, there exists $\lambda_i \in T(E_i, \sigma_i)$ mapping to $\lambda_i^w \in T(E_i^w, \sigma_i)$ for all $w \in V_F$. In particular, $(\lambda_i, d_i) = (\lambda_i^v, d_i)$ for all $i \in I$ and $v \in V_K$. Set $\lambda = (\lambda_i)$; since $\lambda^v \in \mathcal{LR}^v$ for all $v \in V_K$, Proposition 17.1 implies that (G1) holds. ∎

We say that a quadratic form q has *maximal signature* (with respect to M) if for all real places $v \in V_K$, the signature of q at v is equal to the signature of $q_{n,1}$ or of $-q_{n,1}$ at v. For the proof of Theorem 17.2, we need the following proposition.

Proposition 17.5. *For all distinct $i, j \in I$, there exists a quadratic form q over K having maximal signature satisfying* (L1)*, and, for all $v \in V_K$, a corresponding local data $\lambda^v \in \mathcal{LR}^v$, such that for some distinct $v_1, v_2 \in V_K$, we have*

$$a(\lambda^{v_1})(i) = a(\lambda^{v_2})(j) = 1,$$
$$a(\lambda^v)(k) = 0 \quad \text{if } (v, k) \neq (v_1, i), (v_2, j).$$

Lemma 17.6. *Let $v \in V_K$ be a finite place, and let Q be a quadratic form over K_v such that* $\dim(Q) = \dim(q)$ *and* $\det(Q) = \mathrm{N}_{F/K}(-d)$*. Then Q is compatible with $M \otimes_K K_v$.*

Proof. Note that $q_{n,1}$ is compatible with M by construction, and its dimension and determinant coincide with those of Q; if $w_2(Q) = w_2(q_{n,1})$ in $\mathrm{Br}_2(K_v)$, then $Q \simeq q_{n,1}$ over K_v, hence we are done. Suppose that $w_2(Q) \neq w_2(q_{n,1})$, and let λ be a non-trivial element of $T(E_v, \sigma)$. By Proposition 12.4, we have $w_2(q_{n,\lambda}) \neq w_2(q_{n,1})$, and therefore $w_2(q_{n,\lambda}) = w_2(Q)$ in $\mathrm{Br}_2(K_v)$. The forms $q_{n,\lambda}$ and Q have the same dimension, determinant and Hasse–Witt invariant, hence they are isomorphic over K_v. Since $q_{n,\lambda}$ is compatible with $M \otimes_K K_v$, so is Q. ■

Proof of Proposition 17.5. For all $k \in I$, let $S(k)$ be the set of places v of V_K such that $w_2(q^v_{n_k,1}) \neq 0$, and let S be the set of places $v \in V_K$ such that either $v \in S(k)$ for some $k \in I$, or the quaternion algebra (d_s, d_r) is not split at v for some $r, s \in I$. Let $v_1, v_2 \in V_K$ be two distinct finite places that are not in the finite set S.

For all $k \in I$ and $v \in V_K$, let q^v_k be a quadratic form over K_v with the following properties: $\dim(q^v_k) = \dim(q_{n,1})$; $\det(q^v_k) = \mathrm{N}_{F_k/K}(-d_k)$; if v is a real place, then the signature of q^v_k is equal to the signature of $q_{n,1}$ at v; and the Hasse–Witt invariants of q^v_k are as follows:

- $\mathrm{inv}(w_2(q_i^{v_1})) = \mathrm{inv}(w_2(q_j^{v_2})) = 1/2$;
- if $(v, k) \neq (v_1, i), (v_2, j)$, then $w_2(q^v_k) = w_2(q_{n_k,1})$ in $\mathrm{Br}_2(K_v)$.

For all $v \in V_K$, set $Q^v = \bigoplus_{k \in I} q^v_k$; the quadratic form Q^v has determinant $\mathrm{N}_{F/K}(-d)$, hence by Lemma 17.6 it is compatible with $M \otimes_K K_v$ if v is a finite place. If v is an infinite place, then Q^v is isomorphic to $q_{n,1}$ over K_v by construction, hence it is compatible with $M \otimes_K K_v$.

We claim that the number of $v \in V_K$ such that $w_2(Q^v) \neq 0$ is even. Indeed, for all $v \in V_K$ and all $k \in I$, we have

$$w_2(Q^v) = \sum_{k \in I} w_2(q^v_k) + \sum_{r<s} (d_r, d_s),$$
$$w_2(q_{n,1}) = \sum_{k \in I} w_2(q_{n_k,1}) + \sum_{r<s} (d_r, d_s).$$

If $v \neq v_1, v_2$, this implies that $w_2(Q^v) = w_2(q_{n,1})$, and since $q_{n,1}$ is a global form, the number of $v \in V_K$ such that $w_2(q_{n,1}) \neq 0$ in $\mathrm{Br}(K_v)$ is even. We have $w_2(q^{v_1}) \neq w_2(q^{v_1}_{n,1})$ and $w_2(q^{v_2}) \neq w_2(q^{v_2}_{n,1})$; hence the number of places v such $w_2(Q^v) \neq 0$ is even.

Let q be a quadratic form over K such that $q^v \simeq Q^v$ over K_v for all $v \in V_K$; the existence of such a form follows from [Sch 85, Theorem 6.6.10]. The form q has maximal signature by construction.

For all $v \in V_K$, let $\lambda^v \in \mathcal{LR}^v$ be the local data corresponding to the quadratic form Q^v. We claim that $a(\lambda^v) \in \mathcal{CR}^v$ satisfies the required conditions. Indeed, recall that for all $v \in V_K$ and all $k \in I$, we have

$$w_2(q^v_k) = w_2(q^v_{n_k,1}) + \mathrm{cor}_{F^v/K_v}(\lambda^v_k, d_k)$$

by Proposition 16.1. Since v_1 and v_2 are not in S, we have $w_2(q^{v_1}_{n_i,1}) = w_2(q^{v_2}_{n_j,1}) = 0$, hence

$$\mathrm{inv}(\mathrm{cor}_{F^v/K_v}(\lambda^{v_1}, d_i)) = \mathrm{inv}(\mathrm{cor}_{F^v/K_v}(\lambda^{v_2}_j, d_j)) = 1/2,$$

in other words, $\tilde{a}(\lambda^{v_1})(i) = \tilde{a}(\lambda^{v_2})(j) = 1$. By Lemma 15.2, this implies that

$$a(\lambda^{v_1})(i) = a(\lambda^{v_2})(j) = 1.$$

If $(v,k) \neq (v_1,i),(v_2,j)$, then $w_2(q^v_k) = w_2(q^v_1(k))$, hence the same argument shows that $\tilde{a}(\lambda^v)(k) = 0$, and therefore by Lemma 15.2, we have $a(\lambda^v)(k) = 0$. ■

Proof of Theorem 17.2. If $Ш_E = 0$, then by Theorem 17.4 the Hasse principle holds for any quadratic form q.

To prove the converse, assume that $Ш_E \neq 0$; we claim that there exists a quadratic form q satisfying (L1) but not (G1). Let $c \in Ш_E$ be non-trivial, and let $i, j \in I$ be such that $c(i) \neq c(j)$. With q and $a \in \mathcal{CR}$ as in Proposition 17.5, we have

$$\rho(c) = \sum_{v \in V_K} \sum_{i \in I} c(i) a(\lambda^v)(i) = c(i) + c(j),$$

hence $\rho(c) \neq 0$; by Theorem 17.4 condition (G1) does not hold. ■

Example 17.7. Let $A = K[\Gamma]$ as in Example 7.2, and assume that all the simple σ-stable factors in $\mathcal{A}_M$ are of type (1). In other words, we have $\mathcal{A}_M = (E_i)_{i\in I}$ with $E_i = K[X]/(f_i)$, where $f_i \in K[X]$ are monic, irreducible, symmetric polynomials of even degree, and $M = \bigoplus_{i\in I} M_i$, with $M_i = [K[X]/(f_i)]^{n_i}$ for some integers $n_i \geqslant 1$. Let q be a quadratic form over K; then q is compatible with M if and only if q has an isometry with minimal polynomial $g = \prod_{i\in I} f_i$ and characteristic polynomial $f = \prod_{i\in I} f_i^{n_i}$; hence Theorem 17.4 gives a necessary and sufficient condition for the Hasse principle to hold for the existence of an isometry with minimal polynomial g and characteristic polynomial f.

Example 17.8. With the notation of Example 17.7, assume that $K = \mathbf{Q}$, and that the polynomials f_i are cyclotomic polynomials for all $i \in I$. Then $E_i = \mathbf{Q}/(f_i)$ is a cyclotomic field for all $i \in I$, hence a CM field; by Example 14.2 this implies that $Ш_E = 0$. By Theorem 17.2, the Hasse principle holds for the existence of an isometry with minimal polynomial g and characteristic polynomial f; if q is a quadratic form having an isometry with minimal polynomial g and characteristic polynomial f locally everywhere, then such an isometry exists over $\mathbf{Q}$ as well.

18. Independent extensions

Recall that two finite extensions K_1 and K_2 of K are *independent over* K if the tensor product $K_1 \otimes_K K_2$ is a field. In this section, we show that the local-global principle of §17 always holds if the extensions E_i/K are pairwise independent over K.

We keep the notation of §17. Recall from Example 13.1 the equivalence relation $\approx$ on I generated by the elementary equivalence

$$i \approx_e j \iff E_i \text{ and } E_j \text{ are independent over } K,$$

and recall that $Ш_{\text{indep}}(E) = Ш_{\approx}(I)$ is the associated obstruction group.

Theorem 18.1. *Assume that* $Ш_{\text{indep}}(E) = 0$ *and condition* (L1) *holds. Then condition* (G1) *holds as well.*

Proof. By Corollary 14.4 the hypothesis implies that $Ш_E = 0$; therefore Theorem 17.2 (i) gives the required result. ■

Corollary 18.2. *Assume that there exists $i \in I$ such that for all $j \in I$ with $j \neq i$ the extensions E_i and E_j are independent over K. If condition* (L1) *is satisfied, then condition* (G1) *also holds.*

Proof. This follows immediately from Theorem 18.1, since the hypothesis implies that $Ш_{\text{indep}}(E) = 0$. ■

The following corollary is an immediate consequence:

Corollary 18.3. *Assume that the extensions E_i/K are pairwise independent over K, and condition* (L1) *holds. Then condition* (G1) *holds as well.*

Example 18.4. Let $f = \prod_{i \in I} f_i^{n_i}$ and $g = \prod_{i \in I} f_i$ be as in Example 17.7, with $E_i = K[X]/(f_i)$. Assume that $Ш_{\text{indep}}(E) = 0$, and let q be a quadratic form over K. Then the Hasse principle holds: if q has an isometry with minimal polynomial g and characteristic polynomial f locally everywhere, then such an isometry exists over K. In particular, this is the case if the extensions E_i/K are pairwise independent over K.

19. Local conditions

We keep the notation of §17. Recall that (V, q) is a quadratic form, M is an A-module satisfying the hypotheses of §16, and $\mathcal{A}_M = (E_i)_{i \in I}$; moreover E_i/F_i is a quadratic extension for all $i \in I$, and $d_i \in F_i^\times$ is such that $E_i = F_i(\sqrt{d_i})$.

The aim of this section is to give a necessary and sufficient condition for $M \otimes_K K_v$ and $(V, q) \otimes_K K_v$ to be compatible for all $v \in V_K$, in other words, for condition (L1) to hold. This complements the Hasse principle results of §17 and will also be used in §20. Since in §20 we need this result for several fields, we use the notation with subscript K:

$(\mathrm{L1})_K$ *For all $v \in V_K$, the quadratic form $(V, q) \otimes_K K_v$ is compatible with the module $M \otimes_K K_v$.*

The validity of $(\mathrm{L1})_K$ will be detected by three conditions, called the determinant condition, the hyperbolicity condition and the signature condition,

Determinant condition:

$$(\det)_K \qquad \det(q) = \prod_{i \in I} \mathrm{N}_{E_i/K}(-d_i)^{n_i} \quad \text{in } K^\times/K^{\times 2}.$$

Remark 19.1. Note that by Proposition 12.2, condition $(\det)_K$ is necessary for (V,q) and M to be compatible for any field K.

Hyperbolicity condition:

$(\mathrm{hyp})_K$ *If* $v \in V_K$ *is such that* $E^v = F^v \times F^v$, *then* $(V,q) \otimes_K K_v$ *is hyperbolic.*

Signature condition: If $v \in V_K$ is a real place, we denote by (r_v, s_v) the signature of $(V,q) \otimes_K K_v$, by $(\rho_i)_v$ the number of real places of F_i above v that extend to complex places of E_i, and set $\sigma_v = \dim(M) - 2\sum_{i \in I} n_i (\rho_i)_v$.

Proposition 19.2. *Let* $v \in V_K$ *be a real place. Then* $(V,q) \otimes_K K_v$ *is compatible with* $M \otimes_K K_v$ *if and only if* $r_v \geqslant \sigma_v$, $s_v \geqslant \sigma_v$, *and* $r_v \equiv s_v \equiv \sigma_v \pmod 2$.

Proof. This is straightforward, using for instance the arguments of the proof of [B 15, Proposition 8.1]. ∎

The signature condition is as follows:

$(\mathrm{sign})_K$ *If* $v \in V_K$ *is a real place, we have*

$$r_v \geqslant \sigma_v,\ s_v \geqslant \sigma_v,\ \text{and } r_v \equiv s_v \equiv \sigma_v \pmod 2.$$

Proposition 19.3. *The following are equivalent:*

(a) *Condition* $(\mathrm{L1})_K$ *holds.*

(b) *Conditions* $(\det)_K$, $(\mathrm{hyp})_K$ *and* $(\mathrm{sign})_K$ *hold.*

Proof. Let us show that (a)⇒(b). Condition $(\mathrm{L1})_K$ implies $(\det)_K$ by Proposition 12.2, $(\mathrm{hyp})_K$ by Proposition 7.1, and $(\mathrm{sign})_K$ by Proposition 19.2. Conversely, let us show that (b)⇒(a). Let $v \in V_K$. If v is a real place, then Proposition 19.2 shows that $(V,q) \otimes_K K_v$ is compatible with $M \otimes_K K_v$. Assume now that v is a finite place. If $E^v = F^v \times F^v$, then by $(\mathrm{hyp})_K$ the form $(V,q) \otimes_K K_v$ is hyperbolic, and by Proposition 7.1 it is compatible with $M \otimes_K K_v$. Suppose that $E^v \neq F^v \times F^v$; then $T(E^v,\sigma)$ is non-trivial. For all $\lambda \in T(E^v,\sigma)$, we have $\det(q_{n,\lambda}) = \det(q)$ by Proposition 12.2 and $(\det)_K$, and by Proposition 12.4 we can choose $\lambda \in T(E^v,\sigma)$ so that $w_w(q_{n,\lambda}) = w_2(q \otimes_K K_v)$ in $\mathrm{Br}(K_v)$. Therefore $(V,q) \otimes_K K_v$ is compatible with $M \otimes_K K_v$, and hence $(\mathrm{L1})_K$ holds. ∎

Example 19.4. Assume that M and E are as in Example 17.7; recall that $E_i = K[X]/(f_i)$ and $M_i = [K[X]/(f_i)]^{n_i}$ with $f_i \in K[X]$ irreducible, symmetric polynomials of even degree. Set $f = \prod_{i \in I} f_i^{n_i}$. In this case, the local conditions can be reformulated as follows:

$$(\det)_K \qquad \det(q) = f(1)f(-1) \quad \text{in } K^\times/K^{\times 2}.$$

We say that a polynomial is *hyperbolic* if it is a product of irreducible polynomials of type (2) (see Example 7.2), and we can write

$(\mathrm{hyp})_K$ *If* $v \in V_K$ *is such that* $f \in K_v[X]$ *is hyperbolic, then* $(V,q) \otimes_K K_v$ *is hyperbolic.*

If $v \in V_K$ is a real place, we denote by $m_v(f)$ the number of roots z of $f \in K_v[X]$ with $|z|_v > 1$ (counted with multiplicity), and we can restate

$(\mathrm{sign})_K$ *If $v \in V_K$ is a real place, we have*

$$r_v \geqslant m_v(f), \quad s_v \geqslant m_v(f), \quad \textit{and} \quad r_v \equiv s_v \equiv m_v(f) \pmod 2.$$

Set $g = \prod_{i \in I} f_i$. We recover a result of [B 15, Theorem 12.1]: the quadratic form $(V, q) \otimes_K K_v$ has an isometry with characteristic polynomial f and minimal polynomial g for all $v \in V_K$ if and only if the above three conditions hold.

20. Odd degree descent

We keep the notation of the previous sections. The aim of this section is to prove an "odd degree descent" result:

Theorem 20.1. *If K' is a finite extension of K of odd degree such that $(V, q) \otimes_K K'$ is compatible with $M \otimes_K K'$, then (V, q) is compatible with M.*

We start with a lemma:

Lemma 20.2. *Let K'/K be a finite extension of odd degree. Then*

$$(\mathrm{L1})_{K'} \implies (\mathrm{L1})_K.$$

Proof. It is clear that $(\mathrm{det})_{K'} \Rightarrow (\mathrm{det})_K$, $(\mathrm{hyp})_{K'} \Rightarrow (\mathrm{hyp})_K$ and $(\mathrm{sign})_{K'} \Rightarrow (\mathrm{sign})_K$. By Proposition 19.3, this implies that $(\mathrm{L1})_{K'} \Rightarrow (\mathrm{L1})_K$. ∎

Proof of Theorem 20.1. By hypothesis, condition $(\mathrm{L1})_{K'}$ holds; let

$$\rho_{K'} : \text{Ш}_{E \otimes_K K'} \to \mathbf{Z}/2\mathbf{Z}$$

be the associated homomorphism of §17. Recall that $\rho_{K'}$ is independent of the chosen local data. By Lemma 20.2, condition $(\mathrm{L1})_K$ holds. Let

$$\rho_K(c) = \sum_{v \in V_K} \sum_{i \in I} c(i) a(\lambda^v)(i)$$

be the associated homomorphism. For all $v \in V_K$, let us choose a place w of K' over v. Let us take the extension a^w of $a^v = a(\lambda^v)$ to $F^v \otimes_{K_v} K'_w$ to define $\rho_{K'}$.

If $[K'_w : K_v]$ is odd, then

$$\mathrm{inv}_v(\mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)) = \mathrm{inv}_w(\mathrm{cor}_{F_i^v \otimes_{K_v} K'_w/K'_w}(a_i^w, d_i)).$$

If $[K'_w : K_v]$ is even, then

$$\mathrm{inv}_w(\mathrm{cor}_{F_i^v \otimes_{K_v} K'_w/K'_w}(a_i^w, d_i)) = 0.$$

Since K' is an odd degree extension of K, the degree $[K'_w : K_v]$ is odd for an odd number of places w of K' over v. Hence

$$\mathrm{inv}_v(\mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)) = \sum_{w|v} \mathrm{inv}_w(\mathrm{cor}_{F_i^v \otimes_{K_v} K'_w/K'_w}(a_i^w, d_i)).$$

Recall from §14 that we have an injective homomorphism

$$\pi' : Ш_E \to Ш_{E \otimes_K K'}$$

(see Proposition 14.5). Let $c \in Ш_E$, and let $c' = \pi'(c)$; in other words, with the notation of §14, we have $c'(i,j) = c(i)$. Let $a_{i,j}^{v'}$ be the image of a_i^v in $F'_{i,j} \otimes_{K'} K'_{v'}$; then $(a_{i,j}^{v'})$ is a local data over K'. Denote by $d_{i,j}$ the image of d_i in $F'_{i,j}$. Note that $F_i \otimes_K K' \otimes_{K'} K'_w \simeq F_i^v \otimes_{K_v} K'_w$.

By hypothesis, condition $(\mathrm{G1})_{K'}$ holds, hence by Theorem 17.4 we have $\rho_{K'} = 0$. Therefore $\rho_{K'}(c') = 0$, and this implies that

$$\sum_{v' \in V_{K'}} \sum_{(i,j) \in I'} c'(i,j)\, \mathrm{inv}_{v'}(\mathrm{cor}_{F_{i,j}^{v'}/K'_{v'}}(a_{i,j}^{v'}, d_{i,j})) = 0.$$

By the above observations, we have

$$\begin{aligned}
&\sum_{v' \in V_{K'}} \sum_{(i,j) \in I'} c'(i,j)\, \mathrm{inv}_{v'}(\mathrm{cor}_{F_{i,j}^{v'}/K'_{v'}}(a_{i,j}^{v'}, d_{i,j})) \\
&\quad = \sum_{v' \in V_{K'}} \sum_{i \in I} c(i) \sum_{j \in S(i)} \mathrm{inv}_{v'}(\mathrm{cor}_{F_{i,j}^{v'}/K'_{v'}}(a_{i,j}^{v'}, d_{i,j})) \\
&\quad = \sum_{v' \in V_{K'}} \sum_{i \in I} c(i)\, \mathrm{inv}_{v'}(\mathrm{cor}_{F_i^v \otimes_{K_v} K'_{v'}/K'_{v'}}(a_i^{v'}, d_i)) \\
&\quad = \sum_{v \in V_K} \sum_{i \in I} c(i)\, \mathrm{inv}_v(\mathrm{cor}_{F^v/K_v}(a_i^v, d_i)).
\end{aligned}$$

Hence $\rho_K(c) = 0$, and this implies that $\rho_K = 0$; therefore by Theorem 17.4 the quadratic form (V, q) is compatible with M. ∎

21. Obstruction group – the integral case

As in the previous sections, K is a global field; let O be a ring of integers of K with respect to a finite, non-empty set Σ of places of K, containing the infinite places if K is a number field. Let V_Σ be the set of places of K that are not in Σ. If $v \in V_\Sigma$, we denote by O_v the ring of integers of K_v, and by k_v its residue field. Let Λ be an O-algebra, and let $\sigma : \Lambda \to \Lambda$ be an O-linear involution; set $A = \Lambda_K = \Lambda \otimes_O K$. If $v \in V_\Sigma$, set $\Lambda_{K_v} = \Lambda \otimes_O K_v$ and $\Lambda_{k_v} = \Lambda \otimes_O k_v$.

Let $(M_i)_{i \in I}$ be a finite set of A-modules, let $M = \bigoplus_{i \in I} M_i$, and let Λ_M be the image of Λ in $\mathrm{End}(M)$. We assume that the kernel of the homomorphism $\Lambda \to \Lambda_M$ is stable by the involution σ, and we also denote by $\sigma : \Lambda_M \to \Lambda_M$ the induced involution.

The aim of this section is to define a group $Ш_{\Lambda_M,(M_i)_{i\in I}}$ that will be useful in §23. In general, this group depends on $(M_i)_{i\in I}$ and on Λ_M. However, in our main case of interest, namely when $\Lambda = O[\Gamma]$, it only depends on Λ_M.

The group $Ш_{\Lambda_M,(M_i)_{i\in I}}$ is defined using the general framework of §13 using the set I and for all $i, j \in I$, the subsets $V_{i,j}$ of V_Σ defined as follows.

Notation 21.1. For all $i, j \in I$, we denote by $V_{i,j}$ the set of places of $v \in V_\Sigma$ such that $v \in V_i \cap V_j$ and there exists a self-dual Λ_{k_v}-module appearing in the reductions mod π_v of both M_i^v and M_j^v.

Example 21.2. Assume that $\Lambda = O[\Gamma]$, hence $A = \Lambda \otimes_O K = K[\Gamma]$. We keep the notation of Example 17.7, and assume that $f_i \in O[X]$ for all $i \in I$. The homomorphism $O_v \to k_v$ induces $p_v : O_v[X] \to k_v[X]$. For all $i, j \in I$, the set $V_{i,j}$ defined above is the set of places $v \in V_\Sigma$ such that $v \in V_i \cap V_j$ and the polynomials $p_v(f_i)$ and $p_v(f_j)$ have a common irreducible and symmetric factor; this follows from Example 9.2.

Assume now that the A-module M and its decomposition $M = \bigoplus_{i\in I} M_i$ are as in §16, with $A_M = \prod_{i\in I} E_i$ and $M_i \simeq E_i^{n_i}$ for all $i \in I$; set $Ш_{\Lambda_M,(M_i)_{i\in I}} = Ш_{\Lambda_M,M}$.

Recall that S_i is the set of places w of F_i that are inert or ramified in E_i, and if $v \in V_K$, then S_i^v is the set of places $w \in S_i$ above v.

Notation 21.3. If $w_i \in S_i$, we denote by O^{w_i} the ring of integers of $E_i^{w_i}$, and by κ_{w_i} its residue field.

Recall that if N is a self-dual Λ_{k_v}-module, we denote by $\sigma_N : \kappa(N) \to \kappa(N)$ the induced involution of $\kappa(N) = (\Lambda_{k_v})_N$.

Proposition 21.4. *Let $v \in V_\Sigma$, and let $i, j \in I$. Assume that $v \in V_{i,j}$. Then there exists a simple, self-dual Λ_{k_v}-module N and places $w_i \in S_i^v$, $w_j \in S_j^v$ such that*

(i) *the Λ_{k_v}-modules κ_{w_i}, κ_{w_j} and N are isomorphic,*

(ii) *the fields with involution (κ_{w_i}, σ_i) and (κ_{w_j}, σ_j) are isomorphic to $(\kappa(N), \sigma_N)$.*

Proof. (i) follows from Proposition 9.1. To prove (ii), note that $(\Lambda_{k_v})_{\kappa_{w_i}} \simeq \kappa_{w_i}$ and $(\Lambda_{k_v})_{\kappa_{w_j}} \simeq \kappa_{w_j}$. Since all the involutions are induced by σ, this implies (ii). ■

Proposition 21.5. $Ш_E$ *is a subgroup of* $Ш_{\Lambda_M,M}$.

Proof. Let us denote by $\sim$ the equivalence relation on I generated by

$$i \sim j \iff V_{i,j} \neq \varnothing,$$

and by $\approx$ the equivalence relation generated by

$$i \approx j \iff V_i \cap V_j \neq \varnothing.$$

We have $V_{i,j} \subset V_i \cap V_j$ for all $i, j \in I$, hence $i \sim j \Rightarrow i \approx j$. Since $Ш_{\Lambda_M,M}$ is defined by the equivalence relation $\sim$ and $Ш_E$ by $\approx$, this implies that $Ш_E$ is a subgroup of $Ш_{\Lambda_M,M}$. ■

22. Local data and residue maps

We keep the notation of §21; in particular, $M = \bigoplus_{i \in I} M_i$ is a module with $M_i \simeq E_i^{n_i}$ for all $i \in I$.

Let $v \in V_\Sigma$. If $w_i \in S_i^v$ and $\lambda_i^{w_i} \in T(E_i^{w_i}, \sigma_i)$, we obtain a bounded $E_i^{w_i}$-quadratic form $((E_i^{w_i})^{n_i}, q_{n_i, \lambda_i^{w_i}})$ (see §11). Set $M_i^{w_i} = M_i \otimes_{E_i} E_i^{w_i}$. Choosing an isomorphism $M_i \to E_i^{n_i}$, we obtain a bounded A-form on $M_i^{w_i}$, denoted by $(M_i^{w_i}, q_{\lambda_i^{w_i}})$.

Recall from §4 that we have a homomorphism

$$\partial_v : W^b_{\Lambda_{K_v}}(K_v) \to W_{\Lambda_{k_v}}(k_v).$$

Let $\lambda^v = (\lambda_i^{w_i})$. Set

$$\partial_v(\lambda_i^{w_i}) = \partial_v[(M_i^{w_i}, q_{\lambda_i^{w_i}})], \quad \partial_v(\lambda_i^v) = \bigoplus_{w_i \in S_i^v} \partial_v(\lambda_i^{w_i}), \quad \partial_v(\lambda^v) = \bigoplus_{i \in I} \partial_v(\lambda_i^v).$$

Proposition 22.1. *Let $v \in V_\Sigma$, and let $\lambda^v, \mu^v \in \mathcal{LR}^v$ be such that $a(\mu^v) = (i,j)(a(\lambda^v))$ for some $i, j \in I$ with $v \in V_{i,j}$. Then $\partial_v(\mu^v) = \partial_v(\lambda^v)$.*

Proof. Since $v \in V_{i,j}$, by Proposition 21.4 there exists a simple, self-dual Λ_{k_v}-module N and places $w_i \in V_{F_i}$, $w_j \in V_{F_j}$ such that the Λ_{k_v}-modules $\kappa_{w_i}, \kappa_{w_j}$ and N are isomorphic, and the fields with involution (κ_{w_i}, σ_i) and (κ_{w_j}, σ_j) are isomorphic to $(\kappa(N), \sigma_N)$.

Set

$$Q = (\partial_v(\lambda_i^{w_i})) \oplus (\partial_v(\lambda_j^{w_j})) \oplus (-\partial_v(\mu_i^{w_i})) \oplus (-\partial_v(\mu_j^{w_j})).$$

We claim that $Q = 0$ in $W_{\Lambda_{k_v}}(k_v)$; note that Q belongs to the subgroup $W_{\Lambda_{k_v}}(k_v, N)$ of $W_{\Lambda_{k_v}}(k_v)$, and $W_{\Lambda_{k_v}}(k_v, N) \simeq W_{\kappa(N)}(k_v)$.

Let us first assume that w_i and w_j are inert in $E_i^{w_i}$, respectively $E_j^{w_j}$. In this case, the involution σ_N is non-trivial. By Proposition 11.1 (a), we know that $\partial_v : T(E_i^{w_i}, \sigma_i) \to W_{\kappa(N)}(k_v)$ and $\partial_v : T(E_j^{w_j}, \sigma_j) \to W_{\kappa(N)}(k_v)$ are bijective. Therefore $\partial_v(\lambda_i^{w_i}) \neq \partial_v(\mu_i^{w_i})$ and $\partial_v(\lambda_i^{w_i}) \neq \partial_v(\mu_j^{w_j})$. This implies that two of the four elements $\partial_v(\lambda_i^{w_i})$, $\partial_v(\lambda_j^{w_j})$, $\partial_v(\mu_i^{w_i})$, $\partial_v(\mu_j^{w_j})$ are trivial, and two are non-trivial. Since $W_{\kappa(N)}(k_v)$ is of order 2, this implies that the class of Q is trivial in $W_{\kappa(N)}(k_v)$, hence in $W_{\Lambda_{k_v}}(k_v)$.

Assume now that w_i and w_j are ramified in $E_i^{w_i}$, respectively $E_j^{w_j}$, and that $\mathrm{char}(k_v) \neq 2$. In this case, σ_N is the identity, and $W_{\kappa(N)}(k_v) \simeq W(k_v)$. Proposition 11.1 (b) implies that $\partial_v : T(E_i^{w_i}, \sigma_i) \to W_{\kappa(N)}(k_v)$ and $\partial_v : T(E_j^{w_j}, \sigma_j) \to W_{\kappa(N)}(k_v)$ are injective, and their images consist of the classes of forms of dimension $\equiv [\kappa(N) : k_v] \bmod 2$. The injectivity part of the statement implies that $\partial_v(\lambda_i^{w_i}) \neq \partial_v(\mu_i^{w_i})$ and $\partial_v(\lambda_j^{w_j}) \neq \partial_v(\mu_j^{w_j})$. The forms $\partial_v(\lambda_i^{w_i})$, $\partial_v(\lambda_j^{w_j})$, $\partial_v(\mu_i^{w_i})$, $\partial_v(\mu_j^{w_j})$ all have the same dimension mod 2; therefore $\det(\partial_v(\lambda_i^{w_i})) \neq \det(\partial_v(\mu_i^{w_i}))$ and $\det(\partial_v(\lambda_j^{w_j})) \neq \det(\partial_v(\mu_j^{w_j}))$. Hence the forms $\partial_v(\lambda_i^{w_i}) \oplus \partial_v(\lambda_j^{w_j})$ and $\partial_v(\mu_i^{w_i}) \oplus \partial_v(\mu_j^{w_j})$ have the same dimension mod 2 and the same determinant, therefore they are equal in $W(k_v)$. This implies that $Q = 0$ in $W(k_v)$.

Finally, assume that w_i and w_j are ramified in $E_i^{w_i}$, respectively $E_j^{w_j}$, and that $\mathrm{char}(k_v) = 2$. Proposition 11.1 (c) implies that $\partial_v : T(E_i^{w_i}, \sigma_i) \to W_{\kappa(N)}(k_v)$ and

$\partial_v : T(E_i^{w_i}, \sigma_i) \to W_{\kappa(N)}(k_v)$ are constant, hence $\partial_v(\lambda_i^{w_i}) = \partial_v(\mu_i^{w_i})$ and $\partial_v(\lambda_j^{w_j}) = \partial_v(\mu_j^{w_j})$. Since $W_{\kappa(N)}(k_v)$ is of order 2, this implies that $Q = 0$ in $W_{\kappa(N)}(k_v)$, hence in $W_{\Lambda_{k_v}}(k_v)$.

This holds for any pair w_i, w_j with the above properties, therefore the form

$$(\partial_v(\lambda_i^v)) \oplus (\partial_v(\lambda_j^v)) \oplus (-\partial_v(\mu_i^v)) \oplus (-\partial_v(\mu_j^v))$$

is trivial in $W_{\Lambda_{k_v}}(k_v)$; this completes the proof of the proposition. ∎

Notation 22.2. For all $v \in V_\Sigma$, let us fix $\delta = (\delta_v)$ with $\delta_v \in W_{\Lambda_{k_v}}(k_v)$ such that $\delta_v = 0$ for almost all v. Let $\mathcal{L}_\delta^v$ be the set of $\lambda^v \in \mathcal{LR}^v$ such that $\partial_v(\lambda^v) = \delta_v$, and let $\mathcal{C}_\delta^v$ be the set of $a(\lambda^v) \in C(I)$ such that $\lambda^v \in \mathcal{L}_\delta^v$.

Let $\sim_v$ be the equivalence relation on $C(I)$ generated by

$$c \sim_v c' \iff c = (i, j)(c') \text{ for some } i, j \in I \text{ with } v \in V_{i,j}.$$

Corollary 22.3. *Let $v \in V_\Sigma$ and let $a(\lambda^v), a(\mu^v) \in \mathcal{CR}^v$ be such that $a(\mu^v) \sim_v a(\lambda^v)$. If $a(\lambda^v) \in \mathcal{C}_\delta^v$, then $a(\mu^v) \in \mathcal{C}_\delta^v$.*

Proof. It suffices to show that if $a(\mu^v) = (i, j)(a(\lambda^v))$ for some $i, j \in I$ with $v \in V_{i,j}$, then $a(\mu^v) \in \mathcal{C}_\delta^v$; this follows from Proposition 22.1. ∎

Proposition 22.4. *Let $v \in V_\Sigma$. Then the set $\mathcal{C}_\delta^v$ is a $\sim_v$-equivalence class of $C(I)$.*

Proof. Let us prove that if an element of $C(I)$ is $\sim_v$-equivalent to an element of $\mathcal{C}_\delta^v$, then it is in $\mathcal{C}_\delta^v$. By Proposition 16.7, this element belongs to $\mathcal{CR}^v$, and Corollary 22.3 implies that it is in $\mathcal{C}_\delta^v$.

Let $a(\lambda^v), a(\mu^v) \in \mathcal{C}_\delta^v$, and let us show that $a(\lambda^v) \sim_v a(\mu^v)$. Let $J \subset I$ be the set of $i \in I$ such that $a(\lambda^v)(i) \neq a(\mu^v)(i)$. Since

$$\sum_{r \in I} a(\mu^v)(r) = \sum_{r \in I} a(\lambda^v)(r) = A^v,$$

the set J has an even number of elements.

Suppose first that v is non-dyadic. This implies that if $i \in J$, then $\partial_v(\lambda_i^v) \neq \partial_v(\mu_i^v)$. We have $a(\lambda^v), a(\mu^v) \in \mathcal{C}_\delta^v$ by hypothesis, hence $\partial_v(\lambda^v) = \partial_v(\mu^v)$, and therefore there exists $j \in J$ such that $\partial_v(W_{\Lambda_{K_v}}(K_v, M_i^v))$ and $\partial_v(W_{\Lambda_{K_v}}(K_v, M_j^v))$ have a non-zero intersection, and hence $v \in V_{i,j}$. The map $(i, j)a(\lambda^v)$ differs from $a(\mu^v)$ in fewer elements than $a(\lambda^v)$ does. Since I is a finite set, continuing this way we see that $a(\lambda^v) \sim_v a(\mu^v)$.

Assume now that v is dyadic, and let J' be the set of J such that $\partial_v(\lambda_i^v) = \partial_v(\mu_i^v)$. Since $\partial_v(\lambda^v) = \partial_v(\mu^v)$, the set J' also has an even number of elements. Let us write $J = J' \cup J''$; then J'' has an even number of elements. If $i, j \in J'$, then $v \in V_{i,j}$. The map $(i, j)a(\lambda^v)$ differs from $a(\mu^v)$ in fewer elements than $a(\lambda^v)$ does. After applying (i, j) for all $j, j \in J'$ with $i \neq j$, we may assume that J' is empty. Now we have $J = J''$, and the same argument as in the non-dyadic case shows that $a(\lambda^v) \sim_v a(\mu^v)$. ∎

23. Local-global problem – the integral case

We keep the notation of the previous sections.

Let q be a quadratic form over K. For all $v \in V_\Sigma$, let us fix $\delta = (\delta_v)$ with $\delta_v \in W_{\Lambda_{k_v}}(k_v)$ such that $\delta_v = 0$ for almost all v. Recall the following terminology from §6:

We say that the *local conditions are satisfied* if conditions (L1) and $(\mathrm{L2})_\delta$ below hold:

(L1) *For all $v \in V_K$, the quadratic form $(V, q) \otimes_K K_v$ is compatible with the module $M^v = M \otimes_K K_v$*

$(\mathrm{L2})_\delta$ *For all $v \in V_\Sigma$, the quadratic form $(V, q) \otimes_K K_v$ contains an almost unimodular Λ^v-lattice with discriminant form δ_v.*

We say that the *global conditions are satisfied* if conditions (G1) and $(\mathrm{G2})_\delta$ below hold:

(G1) *The quadratic form (V, q) is compatible with the module M.*

$(\mathrm{G2})_\delta$ *The quadratic form (V, q) contains an almost unimodular Λ-lattice with discriminant form δ.*

Proposition 23.1. *Assume that the local conditions are satisfied. Then the global conditions hold if and only if there exists $\lambda = (\lambda_i) \in T(E, \sigma)$ such that $\lambda \in \mathcal{L}^v_\delta$ for all $v \in V_K$.*

Proof. If (G1) holds, then by Proposition 17.1 here exists $\lambda = (\lambda_i) \in T(E, \sigma)$ such that $\lambda \in \mathcal{L}\mathcal{R}^v$ or all $v \in V_K$. Condition $(\mathrm{G2})_\delta$ implies that one can choose λ such that $\lambda \in \mathcal{L}^v_\delta$ for all $v \in V_\Sigma$.

To prove the converse, let $\lambda = (\lambda_i) \in T(E, \sigma)$ be such that $\lambda \in \mathcal{L}^v_\delta$ for all $v \in V_\Sigma$. By Proposition 17.1, this implies that (G1) holds. Moreover, since $\lambda \in \mathcal{L}^v_\delta$ for all $v \in V_\Sigma$, we have $\partial_v(\lambda) = \delta_v$ for all $v \in V_\Sigma$, hence condition $(\mathrm{G2})_\delta$ is also satisfied. ■

Recall that the equivalence relation $\sim_v$ on $C(I)$ is generated by

$$c \sim_v c' \iff c = (i, j)(c') \text{ for some } i, j \in I \text{ with } v \in V_{i,j}.$$

Let $\mathcal{C}_\delta$ be the set of all (a^v), $a^v \in \mathcal{C}^v_\delta$, such that $a^v = 0$ for almost all $v \in V_\Sigma$.

Proposition 23.2. *Assume that the local conditions are satisfied. Then there exists $(\lambda^v) \in \mathcal{L}_\delta$ such that $(a(\lambda^v)) \in \mathcal{C}_\delta$.*

Proof. Let S be the subset of V_K consisting of the dyadic places, the infinite places, the places that are ramified in E_i/K for some $i \in I$, the places $v \in V_K$ such that $w_2(q) \neq w_2(q_{n,1})$ in $\mathrm{Br}_2(k_v)$, and the places $v \in V_\Sigma$ for which $\delta_v \neq 0$. Let us show that if $v \notin S$, then there exists $\lambda^v \in \mathcal{L}^v_\delta$ such that $a(\lambda^v) = 0$.

Let $v \in V_K$ be such that $v \notin S$, and let $i \in I$. If $S^v_i = \varnothing$, then $T(E^v_i, \sigma_i) = 0$, hence there is nothing to prove. Assume that $S^v_i \neq \varnothing$; recall that for all $w \in S^v_i$ we have an isomorphism

$$\theta^w_i : T(E^w_i, \sigma_i) \to \mathbf{Z}/2\mathbf{Z},$$

and for all $\lambda^v = (\lambda_i^w) \in T(E^v, \sigma)$, we have

$$a(\lambda^v)(i) = \sum_{w \in S_i^v} \theta_i^w(\lambda_i^w).$$

For all $i \in I$ such that $S_i^v \neq \varnothing$ and for all $w \in S_i^v$, let $\lambda_i^w = 1$ in $T(E_i^w, \sigma_i)$. We claim that $a(\lambda_i^v) \in \mathcal{C}_\delta^v$ and $a(\lambda^v) = 0$. It is clear that $a(\lambda^v)(i) = 0$ for all $i \in I$; it remains to show that $(\lambda_i^v) \in \mathcal{L}_\delta^v$.

We first show that $(\lambda_i^v) \in \mathcal{L}R^v$. Since $v \notin S$, we have $w_2(q) = w_2(q_{n,1})$ in $\mathrm{Br}_2(K_v)$. The quadratic form q is compatible with the module $M \otimes_K K_v$ by hypothesis, hence $\det(q) = \mathrm{N}_{F/K}(-d)$ in $K_v^\times / K_v^{\times 2}$ (see Proposition 12.2). Since also $\det(q_{n,1}) = \mathrm{N}_{F/K}(-d)$, the quadratic forms q and $q_{n,1}$ have the same dimension, determinant and Hasse–Witt invariant over K_v, therefore they are isomorphic over K_v; this implies that $(\lambda_i^v) \in \mathcal{L}R^v$.

Since $v \notin S$, it is unramified in E_i; hence Lemma 11.2 implies $\partial_v(1) = \partial_v(\lambda^v) = 0$; as $\delta_v = 0$ for $v \notin S$, we have $(\lambda_i^v) \in \mathcal{L}_\delta^v$. ∎

Necessary and sufficient conditions

Let V' be the set of finite places of K.

Proposition 23.3. *Let $(a(\lambda^v)), (a(\mu^v)) \in \mathcal{C}_\delta$, and let $c \in \text{Ш}_{\Lambda_M, M}$. Then*

$$\sum_{v \in V'} \sum_{i \in I} c(i) a(\lambda^v)(i) = \sum_{v \in V'} \sum_{i \in I} c(i) a(\mu^v)(i).$$

Proof. This follows from Corollary 22.4 and Proposition 13.5. ∎

Let

$$\epsilon : \text{Ш}_{\Lambda_M, M} \to \mathbf{Z}/2\mathbf{Z}$$

be the homomorphism defined by

$$\epsilon(c) = \sum_{v \in V'} \sum_{i \in I} c(i) a(\lambda^v)(i)$$

for some $(a(\lambda^v)) \in \mathcal{C}_\delta$. By Proposition 23.3, the homomorphism ϵ is independent of the choice of $(a(\lambda^v)) \in \mathcal{C}_\delta$.

Let V'' be the set of infinite places of K, and let $\mathcal{C}(V'')$ be the set of $(a(\lambda^v))$ with $v \in V''$ and $a(\lambda^v) \in \mathcal{C}^v$. Note that since V'' is finite, the set $\mathcal{C}(V'')$ is also finite. If $V'' = \varnothing$, we set $\mathcal{C}(V'') = 0$.

For all $a \in \mathcal{C}(V'')$ with $a = (a(\lambda^v))$, we define a homomorphism

$$\epsilon_a : \text{Ш}_{\Lambda_M, M} \to \mathbf{Z}/2\mathbf{Z}$$

by setting

$$\epsilon_a(c) = \sum_{v \in V''} \sum_{i \in I} c(i) a(\lambda^v)(i).$$

Theorem 23.4. *Assume that the local conditions hold. Then the global conditions are satisfied if and only if there exists $a \in \mathcal{C}(V'')$ such that $\epsilon + \epsilon_a = 0$.*

Proof. Assume that the global conditions are satisfied. Then by Proposition 23.1 there exists $\lambda = (\lambda_i) \in T(E,\sigma)$ such that $\lambda \in \mathcal{L}_\delta^v$ for all $v \in V_K$. We have $\sum_{v \in V_K} a(\lambda)(i) = 0$ for all $i \in I$. Set $a = (a(\lambda^v))$ for $v \in V''$; then $\epsilon + \epsilon_a = 0$.

Let us prove the converse. Since the local conditions hold, Proposition 23.2 implies that there exists $(\mu^v) \in \mathcal{L}_\delta$ such that $(a(\mu^v)) \in \mathcal{C}_\delta$. By hypothesis, there exists $a \in \mathcal{C}(V'')$ such that $\epsilon + \epsilon_a = 0$. Therefore Theorem 13.4 implies that there exists $b = (b^v) \in \mathcal{C}_\delta$ such that $\sum_{v \in V_K} b^v(i) = 0$. By definition, there exists $(\lambda^v) \in \mathcal{L}_\delta$ such that $b^v = a(\lambda^v)$ for all $v \in V_K$. Recall that $a(\lambda^v)(i) = \sum_{w \in S_v} \theta_i^w(\lambda_i^w)$; therefore for all $i \in I$, we have $\sum_{w \in V_F} \theta_i^w(\lambda_i^w) = 0$. By Theorem 10.1 this implies that for all $i \in I$, there exists $\lambda_i \in T(E_i,\sigma_i)$ mapping to $\lambda_i^w \in T(E_i^w,\sigma_i)$ for all $w \in V_F$. Set $\lambda = (\lambda_i)$; we have $\lambda \in \mathcal{L}_\delta^v$ for all $v \in V_K$, hence by Proposition 23.1 the global conditions hold. ■

Example 23.5. Suppose that $\Lambda = O[\Gamma]$, and let f and g be as in Example 21.2. Assume that for all $v \in V_\Sigma$, the quadratic form q contains a unimodular O_v-lattice having an isometry with minimal polynomial g and characteristic polynomial f; Theorem 23.4 gives a necessary and sufficient condition for such a lattice to exists globally.

Recall that a quadratic form q has maximal signature if for all real places $v \in V_K$, the signature of q at v is equal to the signature of $q_{1,n}$ or of $-q_{1,n}$ at v.

Lemma 23.6. *Assume that q has maximal signature. Then $\mathcal{C}(V'')$ has at most one element.*

Proof. If V'' does not contain any real places, there is nothing to prove. Let v be a real place of K, and let (r_v, s_v) be the signature of q at v. Let us assume that the signature of q at v is equal to the signature of $q_{1,n}$; the argument is the same if it is equal to the signature of $-q_{1,n}$. For all $i \in I$, let $(r_{n_i,1}^v, s_{n_i,1}^v)$ be the signature of $q_{n_i,1}$ and let $(r_{n,1}, s_{n,1})$ be the signature of $q_{n,1}$. By hypothesis, we have $s_v = s_{n,1}^v$. In all splittings of q over K_v into the orthogonal sum of quadratic forms q_i^v over K_v with signature (r_i^v, s_i^v) compatible with the module $M_i \otimes_K K_v$, we have $s_i^v \geqslant s_{n_i,1}^v$ for all $i \in I$. Note that $s_{n,1}^v = \sum_{i \in I} s_{n_i,1}^v$ and $s_v = \sum_{ki \in I} s_i^v$; therefore $s_i^v = s_{n_i,1}^v$ for all $i \in I$, and this implies that the local solution is unique. This holds for all real places $v \in V_K$, hence $\mathcal{C}(V'')$ has at most one element. ■

Assume that q has maximal signature and the local conditions hold; let $a \in C(V'')$, and set $\epsilon' = \epsilon + \epsilon_a$. The following is an immediate consequence of Theorem 23.4:

Corollary 23.7. *Assume that q has maximal signature and the local conditions hold. Then the global conditions hold if and only if $\epsilon' = 0$.*

Theorem 23.8. *The Hasse principle holds for all quadratic forms q and all $\delta = (\delta_v)$ if and only if $Ш_{\Lambda_M,M} = 0$.*

Proof. If $Ш_{\Lambda_M,M} = 0$, then Theorem 23.4 implies that the Hasse principle holds for any q and δ. To prove the converse, assume that $Ш_{\Lambda_M,M} \neq 0$; we claim that there exists a quadratic form q and $\delta = (\delta_v)$ satisfying (L1) and $(\mathrm{L2})_\delta$ but not (G1) and $(\mathrm{G2})_\delta$. Let $c \in Ш_{\Lambda_M,M}$ be a non-trivial element, and let $i, j \in I$ be such that $c(i) \neq c(j)$. Let the quadratic form q and $a \in \mathcal{CR}$ be as in Proposition 17.5, and set $\delta_v = \partial_v[q]$ for all $v \in V_\Sigma$. Since q is a global form, $\delta_v = 0$ for almost all $v \in V_\Sigma$. By construction, q and δ satisfy conditions (L1) and $(\mathrm{L2})_\delta$. Moreover, the form q has maximal signature. We have

$$\epsilon'(c) = \sum_{v \in V_K} \sum_{i \in I} c(i) a(\lambda^v)(i) = c(i) + c(j),$$

hence $\epsilon'(c) \neq 0$; Corollary 23.7 implies that the global conditions are not satisfied. ■

24. The integral case – Hasse principle with additional conditions

Given integers $r, s \geqslant 0$ and a polynomial $f \in \mathbf{Z}[X]$, does there exist an even, unimodular lattice of signature (r, s), and having an isometry with characteristic polynomial f? This is one of the motivating questions of the paper. We can be more ambitious, and fix an element of $\mathrm{SO}_{r,s}(\mathbf{R})$ with characteristic polynomial f; does it stabilize an even, unimodular lattice?

The above question leads to a modified local-global problem: we impose the local behaviour at the real places. As in the previous section, we fix a module M and a quadratic form (V, q). Moreover, for all real places $v \in V_K$ we also fix an $A \otimes_K K_v$-quadratic form $(M \otimes_K K_v, b_v)$.

Example 24.1. Let $A = K[\Gamma]$, $f \in K[X]$ and M be as in Example 17.7. Fixing an $A \otimes_K K_v$-quadratic form $(M \otimes_K K_v, b_v)$ for all real places $v \in V_K$ amounts to fixing a signature for all irreducible, symmetric factors of $f \in K_v[X]$, as in §8 (cf. Example 8.5).

We consider the following modified local and global conditions. Condition (L1) is unchanged:

(L1) *For all $v \in V_K$, the quadratic form $(V, q) \otimes_K K_v$ is compatible with the module $M^v = M \otimes_K K_v$.*

We have the new condition $(\mathrm{L1})_{b_v}$:

$(\mathrm{L1})_{b_v}$ *For all real places $v \in V_K$, there exists an isomorphism*

$$\varphi_v : V \otimes_K K_v \to M \otimes_K K_v$$

such that $(M \otimes_K K_v, b_{\varphi_v}) \simeq (M \otimes_K K_v, b_v)$.

We also fix $\delta = (\delta_v)$ with $\delta_v \in W_{\Lambda_{k_v}}(k_v)$ such that $\delta_v = 0$ for almost all v, and we have the (unchanged) condition

$(\mathrm{L2})_\delta$ *For all $v \in V_\Sigma$, the quadratic form $(V, q) \otimes_K K_v$ contains an almost unimodular Λ^v-lattice with discriminant form δ_v.*

We say that the *local conditions* $(\mathrm{L})_{b_v,\delta}$ *are satisfied* if the three conditions (L1), $(\mathrm{L1})_{b_v}$ and $(\mathrm{L2})_\delta$ hold.

We say that the *global conditions* $(\mathrm{G})_{b_v,\delta}$ *are satisfied* if there exists an isomorphism of vector spaces $\varphi : V \to M$ such that

- (M, b_φ) is an A-quadratic form;
- for all real places $v \in V_K$, we have $(M \otimes_K K_v, b_\varphi) \simeq (M \otimes_K K_v, b_v)$;
- for all $v \in V_\Sigma$, we have $\partial_v(M \otimes_K K_v, b_{\varphi_v}) = \delta_v$.

(In particular, conditions (G1) and $(\mathrm{G2})_\delta$ of the previous section hold).

Assume that the local conditions $(\mathrm{L})_{b_v,\delta}$ are satisfied. The obstruction group $Ш_{A_M,M}$ is as in §23, and so is the homomorphism $\epsilon : Ш_{A_M,M} \to \mathbf{Z}/2\mathbf{Z}$; indeed, this homomorphism only depends on the finite places of K.

If $v \in V_K$ is a real place, then condition $(\mathrm{L1})_{b_v}$ determines the local data λ^v uniquely; therefore $C(V'')$ has exactly one element, namely $a = (a(\lambda^v))$. We define the homomorphism ϵ_a as in §23. Setting $\epsilon' = \epsilon + \epsilon_a$, we obtain a homomorphism

$$\epsilon' : Ш_{A_M,M} \to \mathbf{Z}/2\mathbf{Z}.$$

Theorem 24.2. *Assume that the local conditions* $(\mathrm{L})_{b_v,\delta}$ *hold. Then the global conditions* $(\mathrm{G})_{b_v,\delta}$ *are satisfied if and only if* $\epsilon' = 0$.

To prove this theorem, we need an analog of Proposition 23.1. Let us denote by $\mathcal{L}^v_{b_v,\delta}$ the subset of $\mathcal{L}^v_\delta$ in which the components λ^v for v real are determined by $(M \otimes_K K_v, b_v)$.

Proposition 24.3. *Assume that the local conditions* $(\mathrm{L})_{b_v,\delta}$ *are satisfied. Then the global conditions* $(\mathrm{G})_{b_v,\delta}$ *hold if and only if there exists* $\lambda = (\lambda_i) \in T(E,\sigma)$ *such that* $\lambda \in \mathcal{L}^v_{b_v,\delta}$ *for all* $v \in V_K$.

Proof. If the global conditions $(\mathrm{G})_{b_v,\delta}$ hold, then by Proposition 17.1 there exists $\lambda = (\lambda_i) \in T(E,\sigma)$ such that $\lambda \in \mathcal{LR}^v$ for all $v \in V_K$. Moreover, the conditions imply that one can choose λ such that $\lambda \in \mathcal{L}^v_{b_v,\delta}$ for all $v \in V_K$.

To prove the converse, let $\lambda = (\lambda_i) \in T(E,\sigma)$ be such that $\lambda \in \mathcal{L}^v_{b_v,\delta}$ for all $v \in V_K$. By Proposition 17.1, this implies that (G1) holds. Moreover, since $\lambda \in \mathcal{L}^v_{b_v,\delta}$ for all $v \in V_K$, we have $\partial_v(M \otimes_K K_v, b_{\varphi_v}) = \delta_v$ for all $v \in V_\Sigma$, and $(M \otimes_K K_v, b_\varphi) \simeq (M \otimes_K K_v, b_v)$ for all real places $v \in V_K$, hence the global conditions $(\mathrm{G})_{b_v,\delta}$ hold. ■

Proof of Theorem 24.2. The proof goes along the lines of the one of Theorem 23.4, applying Proposition 24.3 instead of Proposition 23.1. ■

25. Lattices over Z

Let $f \in \mathbf{Z}[X]$ be a monic, symmetric polynomial without linear factors; we start by recalling from [GM 02] some necessary conditions for the existence of an even, unimodular lattice to have an isometry with characteristic polynomial f. We then apply the results of §23 to give sufficient conditions as well. Set $2n = \deg(f)$.

Definition 25.1. We say that f satisfies condition (C1) if the integers $|f(1)|$, $|f(-1)|$ and $(-1)^n f(1)f(-1)$ are all squares.

Let $m(f)$ be the number of roots z of f with $|z| > 1$ (counted with multiplicity).

Definition 25.2. Let (r, s) be a pair of non-negative integers. We say that condition (C2) holds if $r + s = 2n$, $r \equiv s \pmod 8$, $r \geqslant m(f)$, $s \geqslant m(f)$, and $m(f) \equiv r \equiv s \pmod 2$.

The following lemma is well-known (see for instance [GM 02]).

Lemma 25.3. *Assume that there exists an even, unimodular lattice with signature* (r, s) *having an isometry with characteristic polynomial* f. *Then conditions* (C1) *and* (C2) *hold.*

Proof. It is clear that $r + s = 2n$, and the property $r \equiv s \pmod 8$ is well-known (see for instance [S 77, Chapitre V, Théorème 2]). For the last part of condition (C2), see [B 15, Corollary 8.2] (in the case where f is separable, this is also proved in [GM 02, Corollary 2.3]). It is well-known that $(-1)^n f(1)f(-1)$ is a square; see for instance [B 15, Corollary 5.2]. The fact that $|f(1)|$ and $|f(-1)|$ are squares is proved in [GM 02, Theorem 6.1] (the hypothesis that f is separable is not needed in the proof).

Let

$$f = \prod_{i \in I} f_i^{n_i} \quad \text{and} \quad g = \prod_{i \in I} f_i$$

where $f_i \in \mathbf{Z}[X]$ are distinct irreducible, symmetric polynomials of even degree. Set $E_i = \mathbf{Q}[X]/(f_i) = \mathbf{Q}(\tau_i)$, and let $\sigma_i : E_i \to E_i$ be the $\mathbf{Q}$-linear involution sending τ_i to τ_i^{-1}; let F_i be the fixed field of E_i.

The following is essentially contained in [BT 20].

Theorem 25.4. *Assume that condition* (C1) *holds. Then for each prime number* p *there exists an even, unimodular* $\mathbf{Z}_p$*-lattice having an isometry with characteristic polynomial* f *and minimal polynomial* g.

Proof. Let $E_{0,i}$ be an extension of degree n_i of F_i, linearly disjoint from E_i. Set $\tilde{E}_i = E_i \otimes E_{0,i}$; then the characteristic polynomial of multiplication by τ_i on $\tilde{E}_i$ is $f_i^{n_i}$, and its minimal polynomial is f_i. Set $\tilde{E} = \prod_{i \in I} \tilde{E}_i$, $\tilde{E}_0 = \prod_{i \in I} \tilde{E}_{0,i}$, and let $T : \tilde{E} \to \tilde{E}$ be the linear transformation acting on $\tilde{E}_i$ by multiplication with τ_i; the characteristic polynomial of T is f, and its minimal polynomial is g. The argument of [BT 20, proof of Theorem A] shows that for every prime number p there exists a quadratic form on $\tilde{E} \otimes \mathbf{Q}_p$ containing an even, unimodular $\mathbf{Z}_p$-lattice stable by T. ■

The following lemma is well-known:

Lemma 25.5. (i) *Let* (r, s) *be a pair of non-negative integers with* $r \equiv s \pmod 8$. *Then there exists an even, unimodular lattice of signature* (r, s).

(ii) *Two even, unimodular lattices of the same signature become isomorphic over* $\mathbf{Q}$.

Proof. (i) Let $m = (r - s)/8$; the orthogonal sum of m copies of the E_8-lattice with s hyperbolic planes has the required property.

(ii) Let q be a quadratic form over $\mathbf{Q}$ containing an even, unimodular lattice of signature (r, s). Then the dimension of q is $r + s$, its signature is (r, s) and its determinant is $(-1)^s$. The Hasse–Witt invariant of q at a prime $\neq 2$ is trivial (see for instance [O'M 73, §92:1]), and at infinity it is 0 if $s \equiv 0$ or $1 \pmod 4$, and 1 if $s \equiv 2$ or $3 \pmod 4$. By reciprocity, this also determines the Hasse–Witt invariant of q at the prime 2 (one can also prove this directly: see for instance [BT 20, Proposition 8.3]). Therefore the dimension, determinant, signatures and Hasse–Witt invariant of q are uniquely determined by (r, s); hence q is unique up to isomorphism. ■

Notation. If (r, s) is a pair of integers with $r, s \geqslant 0$ and $r \equiv s \pmod 8$, let $(V, q_{r,s})$ be a quadratic form containing an even, unimodular lattice of signature (r, s); such a form exists by Lemma 25.5 (i) and is unique up to isomorphism by Lemma 25.5 (ii).

Let $\Lambda = \mathbf{Z}[\Gamma]$, where Γ is the infinite cyclic group, and set $A = \mathbf{Q}[\Gamma]$; let us denote by σ the involution of Λ and A sending γ to γ^{-1} for all $\gamma \in \Gamma$. Set $M_i = [\mathbf{Q}[X]/(f_i)]^{n_i}$ and $M = \bigoplus_{i \in I} M_i$. Let (V, q) be a quadratic form over $\mathbf{Q}$. Recall from §23 the local and global conditions (L1), $(\text{L2})_\delta$ and (G1), $(\text{G2})_\delta$, and note that (for Λ and M as above, and for $\delta = 0$) they can be reformulated as follows:

(L1) For all $v \in V_{\mathbf{Q}}$, the quadratic form $(V, q) \otimes_{\mathbf{Q}} \mathbf{Q}_v$ has an isometry with minimal polynomial g and characteristic polynomial f.

(G1) The quadratic form (V, q) has an isometry with minimal polynomial g and characteristic polynomial f.

(L2) For all finite places $v \in V_{\mathbf{Q}}$, the quadratic form $(V, q) \otimes_{\mathbf{Q}} \mathbf{Q}_v$ has an isometry with minimal polynomial g and characteristic polynomial f that stabilizes a unimodular lattice of $V \otimes_{\mathbf{Q}} \mathbf{Q}_v$.

(G2) The quadratic form (V, q) has an isometry with minimal polynomial g and characteristic polynomial f that stabilizes a unimodular lattice of V.

Theorem 25.6. *Assume that conditions* (C1) *and* (C2) *hold. Then the local conditions* (L1) *and* (L2) *are satisfied for the quadratic form* $q_{r,s}$.

Proof. Since (C1) holds, Theorem 25.4 implies that for each prime number p there exists an even, unimodular $\mathbf{Z}_p$-lattice having an isometry with characteristic polynomial f and minimal polynomial g; we denote by q^p the quadratic form over $\mathbf{Q}_p$ obtained from this lattice by extension of scalars. If $p \neq 2$, this is the diagonal form $\langle 1, \dots, (-1)^s \rangle$ (see for instance [O'M 73, §92:1]); if $p = 2$, it is an orthogonal sum of hyperbolic planes (see [BT 20, Proposition 8.3]). This implies that $q^p \simeq q_{r,s} \otimes_{\mathbf{Q}} \mathbf{Q}_p$ for all prime numbers p. In particular, the quadratic form $q_{r,s}$ has an isometry with characteristic polynomial f and minimal polynomial g over $\mathbf{Q}_p$ for every prime number p. This implies that the local condition (L1) holds for every prime number p. Moreover, since $q_{r,s} \otimes_{\mathbf{Q}} \mathbf{Q}_p$ contains a unimodular $\mathbf{Z}_p$-lattice stable by this isometry, the local condition $(\text{L2})_\delta$ holds for $\delta = 0$.

On the other hand, condition (C2) implies that $q_{r,s} \otimes_{\mathbf{Q}} \mathbf{R}$ has an isometry with characteristic polynomial f and minimal polynomial g over $\mathbf{R}$ (cf. [B 15, Corollary 8.2]). Therefore the local conditions hold for the quadratic form $q_{r,s}$. ∎

Proposition 25.7. *The following properties are equivalent:*

(i) *There exists an even, unimodular lattice of signature* (r, s) *having an isometry with characteristic polynomial* f *and minimal polynomial* g.

(ii) *The global conditions* (G1) *and* (G2) *are fulfilled for* $(V, q_{r,s})$.

Proof. Let us prove that (i) implies (ii). The base change to $\mathbf{Q}$ of the lattice is isomorphic to $(V, q_{r,s})$ by Lemma 25.5 (ii); hence $(V, q_{r,s})$ has an isometry with characteristic polynomial f and minimal polynomial g, and it contains a unimodular lattice stable by this isometry. This implies that the global conditions (G1) and $(\text{G2})_\delta$ are fulfilled for $(V, q_{r,s})$ and $\delta = 0$, and therefore (ii) holds.

Conversely, assume that (ii) holds. Let $t : V \to V$ be an isometry of $q_{r,s}$ with characteristic polynomial f and minimal polynomial g, and such that $(V, q_{r,s}) \otimes_{\mathbf{Q}} \mathbf{Q}_p$ contains a unimodular $\mathbf{Z}_p$-lattice L_p with $t(L_p) = L_p$ for all prime numbers p. For $p = 2$, let us choose L_2 to be even; we claim that this is possible by [BT 20, Theorem 8.1]. Indeed, condition (i) of that theorem is satisfied, since $(V, q_{r,s}) \otimes_{\mathbf{Q}} \mathbf{Q}_2$ contains a unimodular $\mathbf{Z}_2$-lattice; condition (ii) follows from the fact that $(V, q_{r,s}) \otimes_{\mathbf{Q}} \mathbf{Q}_2$ is an orthogonal sum of hyperbolic planes; and condition (iii) holds by a result of Zassenhaus (see for instance [BT 20, Theorem 8.5]), since $|f(-1)|$ is a square. Let

$$L = \{x \in V \mid x \in L_p \text{ for all } p\}.$$

The lattice L is even, unimodular, and $t(L) = L$; hence L has an isometry with characteristic polynomial f and minimal polynomial g. ∎

Recall from §21 the construction of the group $Ш_{\Lambda_M, M}$. By Example 21.2 the sets $V_{i,j}$ consist of the prime numbers $p \in V_i \cap V_j$ such that f_i mod p and f_j mod p have a common irreducible, symmetric factor. Hence the group $Ш_{\Lambda_M, M}$ only depends on the polynomial g, and will be denoted by $Ш_g$.

We next give some examples of groups $Ш_g$. For all integers $d \geqslant 1$, recall that Φ_d denotes the d-th cyclotomic polynomial.

Example 25.8. Let $f_1(X) = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$, and $f_2 = \Phi_{14}$. Set $f = f_1 f_2^2$ and $g = f_1 f_2$.

The resultant of f_1 and f_2 is 169, and the polynomials f_1 mod 13 and f_2 mod 13 have the irreducible, symmetric common factor $X^2 + 7X + 1 \in \mathbf{F}_{13}[X]$. Moreover, we have $13 \in V_1 \cap V_2$. Therefore $V_{1,2} = \{13\}$ and $Ш_g = 0$.

Example 25.9. Let p and q be distinct prime numbers such that $p \equiv q \equiv 3 \pmod 4$. Let $n, m, t \in \mathbf{Z}$ with $n, m, t \geqslant 1$ and $m \neq t$, and set

$$f_1 = \Phi_{p^n q^m}, \quad f_2 = \Phi_{p^n q^t}, \quad \text{and} \quad f = g = f_1 f_2.$$

If $(\frac{p}{q}) = 1$, then $V_{1,2} = \{q\}$ and $Ш_g = 0$.
If $(\frac{p}{q}) = -1$, then $V_{1,2} = \varnothing$ and $Ш_g \simeq \mathbf{Z}/2\mathbf{Z}$.

Example 25.10. Let p be a prime number with $p \equiv 3 \pmod 4$, and set $f_1 = \Phi_p$, $f_2 = \Phi_{2p}$, $g = f_1 f_2$, and $f = f_1^2 f_2^2$.
If $p \equiv 3 \pmod 8$, then $V_{1,2} = \{2\}$ and $Ш_g = 0$.
If $p \equiv 7 \pmod 8$, then $V_{1,2} = \varnothing$ and $Ш_g \simeq \mathbf{Z}/2\mathbf{Z}$.

More generally, the group $Ш_g$ can be determined for any product of cyclotomic polynomials Φ_d with $d \geqslant 3$ (recall that the polynomials we consider here do not have any linear factors, hence Φ_1 and Φ_2 are excluded); see §31 for more details and examples.

Assume now that conditions (C1) and (C2) hold; by Theorem 25.6 the local conditions (L1) and (L2)$_\delta$ are then satisfied for the quadratic form $q_{r,s}$ and $\delta = 0$. Hence $\mathcal{C}_0$ is not empty (where $\mathcal{C}_0$ is the set $\mathcal{C}_\delta$ for $\delta = 0$).

Recall from §23 that V' is the set of finite primes, and V'' the set of infinite primes; in our case, V' is the set of valuations v_p, where p is a prime number, and $V'' = \{v_\infty\}$, where v_∞ is the unique infinite place. Since $\mathcal{C}_0$ is not empty, we define as in §23 a homomorphism $\epsilon : Ш_g \to \mathbf{Z}/2\mathbf{Z}$; this homomorphism does not depend on the choice of the local data $a \in \mathcal{C}_0$ (see Proposition 23.3).

Moreover, for all $a \in \mathcal{C}(V'')$, we have a homomorphism $\epsilon_a : Ш_g \to \mathbf{Z}/2\mathbf{Z}$ (see §23); note that $C(V'')$ is a finite set, hence we obtain a finite number of such homomorphisms.

Theorem 25.11. *Assume that conditions* (C1) *and* (C2) *hold. Then the following properties are equivalent:*

(i) *There exists an even, unimodular lattice of signature* (r, s) *having an isometry with characteristic polynomial* f *and minimal polynomial* g.

(ii) *There exists* $a \in \mathcal{C}(V'')$ *such that* $\epsilon + \epsilon_a = 0$.

Proof. Since conditions (C1) and (C2) hold, the local conditions (L1) and (L2)$_\delta$ are satisfied for the quadratic form $q_{r,s}$ and $\delta = 0$ (see Theorem 25.6); therefore we can apply Theorem 23.4, and find that (ii) is equivalent to

(ii′) The global conditions (G1) and (G2)$_\delta$ are fulfilled for $(V, q_{r,s})$ and $\delta = 0$.

By Proposition 25.7, (ii′) and (i) are equivalent. This completes the proof of the theorem. ∎

If moreover the quadratic form $(V, q_{r,s})$ has maximal signature, we can define the homomorphism $\epsilon' : Ш_g \to \mathbf{Z}/2\mathbf{Z}$ and apply Corollary 23.7. Note that $(V, q_{r,s})$ has maximal signature if and only if $s = m(f)$ or $r = m(f)$. Hence we obtain the following

Corollary 25.12. *Assume that conditions* (C1) *and* (C2) *hold, and that* $s = m(f)$ *or* $r = m(f)$. *Then there exists an even, unimodular lattice of signature* (r, s) *having an isometry with characteristic polynomial* f *and minimal polynomial* g *if and only if* $\epsilon' = 0$.

Proof. This follows from Theorem 25.11 and Corollary 23.7. ∎

Corollary 25.13. *Assume that f satisfies condition* (C1), *and that* $Ш_g = 0$. *Then for each pair* (r, s) *of integers such that condition* (C2) *holds there exists an even, unimodular lattice with signature* (r, s) *having an isometry with characteristic polynomial f and minimal polynomial g.*

Proof. This follows from Theorem 25.11. ■

Example 25.14. Let $f_1 = \Phi_{p^n q^m}$, $f_2 = \Phi_{p^n q^t}$, and $f = g = f_1 f_2$ be as in Example 25.9. We have $f(1) = f(-1) = 1$ and $m(f) = 0$. Therefore conditions (C1) and (C2) are satisfied for all pairs (r, s) of integers with $r, s \geqslant 0$ such that $r \equiv s \pmod 8$ and $r + s = \deg(f)$. Since $\deg(f)$ is divisible by 8, the choice $r = \deg(f)$ and $s = 0$ satisfies conditions (C1) and (C2).

If $(\frac{p}{q}) = 1$, then $Ш_g = 0$ (see Example 25.9). Therefore by Corollary 25.13, for all pairs (r, s) as above, there exists an even, unimodular lattice with signature (r, s) having an isometry with characteristic polynomial f (and minimal polynomial $g = f$). In particular, there exists a *definite* even, unimodular lattice with this property.

If $(\frac{p}{q}) = -1$, then $Ш_g \simeq \mathbf{Z}/2\mathbf{Z}$ (see Example 25.9). Since conditions (C1) and (C2) are satisfied (for a choice of (r, s) as above), the local conditions are satisfied, and we have $\mathcal{C}_0 \neq \varnothing$.

We denote by v_p the finite place of $\mathbf{Q}$ corresponding to the prime number p, and by v_∞ the unique real place. Let us choose $a \in C(V')$ as follows: $a^v(i) = 0$ for all $i \in I = \{1, 2\}$ if $v \neq v_p$, and $a^{v_p}(1) = a^{v_p}(2) = 1$.

Let $c : I \to \mathbf{Z}/2\mathbf{Z}$ represent the unique non-trivial element of $Ш_g$: we can take c such that $c(1) = 1$ and $c(2) = 0$; we have $\epsilon(c) = 1$.

Let $(r, s) = (\deg(f), 0)$. Then $C(V'')$ has only one element, namely the identically zero one, $a = 0$, hence $\epsilon_a(c) = 0$. This implies that $\epsilon + \epsilon_a \neq 0$; therefore by Theorem 25.11 (or Corollary 25.12) there does not exist any definite, even, unimodular lattice having an isometry with characteristic polynomial f.

The method of Example 25.14 can be used to decide which products of cyclotomic polynomials Φ_d (with $d \geqslant 3$) occur as characteristic polynomials of isometries of definite even, unimodular lattices; this completes the results of [B 84].

Example 25.15. With the notation of Example 25.14, set $p = 3$, $q = 7$, $n = m = 1$ and $t = 2$. We have

$$f_1 = \Phi_{21}, \quad f_2 = \Phi_{147}, \quad \text{and} \quad f = g = f_1 f_2.$$

Since $(\frac{3}{7}) = -1$, we have $Ш_g \simeq \mathbf{Z}/2\mathbf{Z}$ (see Example 25.9). We have also seen (see Example 25.14) that conditions (C1) and (C2) are satisfied for all pairs of integers (r, s) with $r, s \geqslant 0$ such that $r \equiv s \pmod 8$ and $r + s = \deg(f) = 96$.

This gives rise to 25 possible pairs (r, s). We have already seen that the signatures $(96, 0)$ and $(0, 96)$ are impossible (see Example 25.14). Assume that $(r, s) = (92, 4)$.

The homomorphism $\epsilon : Ш_g \to \mathbf{Z}/2\mathbf{Z}$ is already computed in Example 25.14: namely, if $c : I \to \mathbf{Z}/2\mathbf{Z}$ represents the unique non-trivial element of $Ш_g$, we have $\epsilon(c) = 1$.

The homomorphism ϵ_a depends on the choice of $a \in \mathcal{C}(V'') = \mathcal{C}^{v_\infty}$. There are two possibilities: $a(1) = a(2) = 0$ and $a'(1) = a'(2) = 1$. Hence $\epsilon + \epsilon_a \neq 0$, but $\epsilon + \epsilon_{a'} = 0$; by Theorem 25.11, this implies that there exists an even, unimodular lattice of signature $(92, 4)$ having an isometry with characteristic polynomial f.

It is easy to check that all the other signatures (r, s), with the exception of $(96, 0)$ and $(0, 96)$, occur as signatures of even, unimodular lattices having an isometry with characteristic polynomial f; this also follows from Proposition 25.18 below.

We now give some details concerning the counter-example to the Hasse principle of the introduction:

Example 25.16. Let $f_1 = \Phi_p$, $f_2 = \Phi_{2p}$, $g = f_1 f_2$, and $f = f_1^2 f_2^2$ be as in Example 25.10. We have $f(1) = f(-1) = p^2$, hence condition (C1) holds.

Let $p = 7$, and note that f is the polynomial

$$(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)^2 (X^6 - X^5 + X^4 - X^3 + X^2 - X + 1)^2$$

of the introduction. We have $m(f) = 0$, $\deg(f) = 24$, and condition (C2) holds for $(r, s) = (24, 0)$. This implies that the local conditions are satisfied for $q_{24,0}$ and $\delta = 0$. We denote by v_2 the finite place of $\mathbf{Q}$ corresponding to the prime number 2, and by v_∞ the unique real place. Let us choose $a \in \mathcal{C}(V')$ as follows: $a^v(i) = 0$ for all $i \in I = \{1, 2\}$ if $v \neq v_2$, and $a^{v_2}(1) = a^{v_2}(2) = 1$.

By Example 25.10, we know that $Ш_g \simeq \mathbf{Z}/2\mathbf{Z}$. Let $c : I \to \mathbf{Z}/2\mathbf{Z}$ represent the unique non-trivial element of $Ш_g$: we can take c such that $c(1) = 1$ and $c(2) = 0$; we have $\epsilon(c) = 1$. On the other hand, $\mathcal{C}(V'')$ has only one element, $a = 0$, hence $\epsilon_a = 0$. Therefore $\epsilon + \epsilon_a \neq 0$, and by Corollary 25.12 this implies that there does not exist any positive definite, unimodular and even lattice having an isometry with characteristic polynomial f.

It is well-known that there exist exactly 24 isomorphism classes of even, unimodular, positive definite lattices of rank 24, including the Leech lattice, and that they are isomorphic over $\mathbf{Z}_\ell$ for all prime numbers ℓ. The above argument shows that none of them has an isometry with characteristic polynomial f, and they all have such an isometry locally everywhere.

The following examples involve indefinite forms. Let (r, s) be a pair of integers with $r, s \geqslant 1$ such that $r \equiv s \pmod 8$, and let $L_{r,s}$ be an even, unimodular lattice of signature (r, s); it is well-known that such a lattice is unique up to isomorphism (see for instance [S 77, Chapitre V, Théorème 5]).

Recall that a *Salem polynomial* is a monic, irreducible and symmetric polynomial in $\mathbf{Z}$[X] with exactly two roots outside the unit circle, both real and positive.

Example 25.17. Let $f_1(X) = X^6 - 3X^5 - X^4 + 5X^3 - X^2 - 3X + 1$ and $f_2 = \Phi_{12}$; set $f = g = f_1 f_2$. This example is taken from [GM 02, Proposition 5.2], where it is shown that f does not arise as the characteristic polynomial of an isometry of $L_{9,1}$.

With the point of view of the present paper, this can be shown as follows. The polynomials f_1 and f_2 are relatively prime, hence $V_{1,2} = \varnothing$, and this implies that $Ш_g \simeq \mathbf{Z}/2\mathbf{Z}$.

We have $f(1) = -1$, $f(-1) = 1$, and $m(f) = 1$; hence conditions (C1) and (C2) are fulfilled with $(r, s) = (9, 1)$ or $(1, 9)$, and with $(r, s) = (5, 5)$. Let $c : I \to \mathbf{Z}/2\mathbf{Z}$ represent the unique non-trivial element of Ш_g; let us choose c so that $c(1) = 1$ and $c(2) = 0$. It is easy to check that the homomorphism $\epsilon : \text{Ш}_g \to \mathbf{Z}/2\mathbf{Z}$ associated to the finite places satisfies $\epsilon(c) = 1$.

Let $(r, s) = (9, 1)$ or $(1, 9)$. In this case, the set $\mathcal{C}^{v_\infty}$ has a unique element, namely $a = 0$; hence $\epsilon_a = 0$, and $\epsilon + \epsilon_a \neq 0$. Therefore by Theorem 25.11, f does not arise as the characteristic polynomial of an isometry of $L_{9,1}$ or $L_{1,9}$.

Assume now that $(r, s) = (5, 5)$. In this case, we can choose a such that $\epsilon_a \neq 0$ and $\epsilon + \epsilon_a = 0$. Therefore by Theorem 25.11, the lattice $L_{5,5}$ has an isometry with characteristic polynomial f.

Proposition 25.18. *Let $f = f_1^{n_1} f_2^{n_2}$ and let (r, s) be a pair of non-negative integers such that (r, s) is not a maximal signature for f. Set $g = f_1 f_2$. If conditions* (C 1) *and* (C2) *hold, then $L_{r,s}$ has an isometry with characteristic polynomial f and minimal polynomial g.*

Proof. If $\text{Ш}_g = 0$, then this follows from Corollary 25.13. Assume that $\text{Ш}_g \neq 0$; hence $\text{Ш}_g \simeq \mathbf{Z}/2\mathbf{Z}$. Let $I = \{0, 1\}$, and let $c : I \to \mathbf{Z}/2\mathbf{Z}$ represent the unique non-trivial element of Ш_g; choose c so that $c(1) = 1$ and $c(2) = 0$. Note that $\mathcal{C}^{v_\infty} = \mathcal{CR}^{v_\infty}$. We claim that there exists $a \in \mathcal{CR}^{v_\infty}$ such that $\epsilon + \epsilon_a = 0$. Let $b \in \mathcal{CR}^{v_\infty}$. If $b(1) = \epsilon(c)$, set $a = b$. If $b(1) \neq \epsilon(c)$, set $a = (1, 2)b$; by Proposition 16.8, we have $a \in \mathcal{CR}^{v_\infty}$. We have $(\epsilon + \epsilon_a)(c) = \epsilon(c) + a(1)c(1) = 0$, hence $\epsilon + \epsilon_a = 0$. By Theorem 25.11, this implies that $L_{r,s}$ has an isometry with characteristic polynomial f and minimal polynomial g. ■

Proposition 25.19. *Let $f = f_1 f_2$ where f_1 is a Salem polynomial and f_2 is a power of a cyclotomic polynomial Φ_d with $d \geqslant 3$. Let (r, s) be a pair of integers with $r, s \geqslant 3$, and assume that conditions* (C1) *and* (C2) *hold. Set $g = f_1 \Phi_d$. Then $L_{r,s}$ has an isometry with characteristic polynomial f and minimal polynomial g.*

Proof. This follows from Proposition 25.18, since for $r, s \geqslant 3$, the signature (r, s) is not maximal for f. ■

The following example might be interesting in the perspective of constructing automorphisms of K3 surfaces with given entropy (cf. McMullen [McM 02, McM 11, McM 16]).

Example 25.20. As in Example 25.8, let $f_1(X) = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$ and $f_2 = \Phi_{14}$. Set $f = f_1 f_2^2$ and $g = f_1 f_2$.

Note that f_1 is a Salem polynomial, so $m(f_1) = 1$. We have $f(1) = -1$, $f(-1) = 49$, $m(f) = 1$. Therefore conditions (C1) and (C2) hold for all pairs (r, s) of integers with $r, s \geqslant 1$ such that $r \equiv s \pmod 8$ and $r + s = \deg(f) = 22$.

We have seen that $\text{Ш}_g = 0$ (see Example 25.8). By Theorem 25.11 this implies that for all pairs (r, s) as above, the lattice $L_{r,s}$ has an isometry with characteristic polynomial f

and minimal polynomial g. For instance, the signature $(r, s) = (3, 19)$ is possible (the other possible signatures are $(19, 3)$, $(15, 7)$, $(11, 11)$ and $(7, 15)$).

26. Milnor signatures and Milnor indices

In 1968, Milnor defined a signature invariant for knot cobordism (see [M 68, §5]). The aim of this section is to relate this invariant to the one defined in §8 (see Example 8.6).

First, a question of terminology: the word "signature" has two possible meanings, namely a pair (r, s) or the difference $r - s$. The convention of the present paper is to call the pair (r, s) the signature, whereas in knot theory the difference $r - s$ is used. To avoid confusion, we call the difference $r - s$ the *index* (see Notation 8.2).

Let (V, q) be a non-degenerate quadratic form over $\mathbf{R}$, let $t : V \to V$ be an isometry of q, and let $f \in \mathbf{R}[X]$ the characteristic polynomial of t. To each irreducible, symmetric factor $\mathcal{P}$ of f, Milnor associates an index $\tau_{\mathcal{P}}$ (see [M 68, §5]), as follows. Let $V_{\mathcal{P}(t)}$ be the $\mathcal{P}(t)$-primary subspace of V, consisting of all $v \in V$ with $\mathcal{P}(t)^N v = 0$ for N large. The *Milnor index* $\tau_{\mathcal{P}}(t)$ is by definition the index of the restriction of q to the subspace $V_{\mathcal{P}(t)}$.

We define the *Milnor signature* at $\mathcal{P}$ as the signature of the restriction of q to $V_{\mathcal{P}(t)}$. If the minimal polynomial of t is square-free, these indices and signatures are the same as those defined in §8 (see Example 8.6).

More generally, we associate to $t : V \to V$ an isometry $t' : V \to V$ of q with characteristic polynomial f and square-free minimal polynomial (see [M 69, §3]). It follows from [M 69, Theorem 3.3] that $\tau_{\mathcal{P}}(t') = \tau_{\mathcal{P}}(t)$ for all irreducible, symmetric factors $\mathcal{P}$ of f.

27. Lattices and Milnor indices

We keep the notation of §25. Let $f \in \mathbf{Z}[X]$ be a monic, symmetric polynomial of degree $2n$ without linear factors satisfying condition (C1); let $r, s \geqslant 0$ be integers such that condition (C2) holds for f and (r, s).

Theorem 25.11 gives a necessary and sufficient condition for the existence of an even, unimodular lattice of signature (r, s) having an isometry with characteristic polynomial f and square-free minimal polynomial. In this section, we ask a more precise question:

Question. Let $t \in \mathrm{SO}_{r,s}(\mathbf{R})$ be a semisimple isometry with characteristic polynomial F. Does t preserve an even, unimodular lattice?

Theorem 27.4 below gives a necessary and sufficient condition for this to hold. We consider this as a Hasse principle problem; Condition (C1) implies that the local conditions hold at the finite places. Condition (C2) ensures the existence of a semisimple element of $\mathrm{SO}_{r,s}(\mathbf{R})$ with characteristic polynomial f; fixing such an element t determines the local data at $\mathbf{R}$. This is also the point of view of §24, the results of which will be applied here.

Let us write $f = \prod_{i \in I} f_i^{n_i}$, where $f_i \in \mathbf{Z}[X]$ are distinct monic, irreducible, symmetric polynomials of even degree. Set $2n = \deg(f)$, and $g = \prod_{i \in I} f_i$. For all $i \in I$, let $M_i = [\mathbf{Q}[X]/(f_i)]^{n_i}$, and set $M = \bigoplus_{i \in I} M_i$.

Recall that V' is the set of finite places of $\mathbf{Q}$, and $V'' = \{v_\infty\}$, where v_∞ is the unique infinite place of $\mathbf{Q}$.

We start by introducing some notation.

Notation 27.1. Let $\mathrm{Irr}_{\mathbf{R}}(f)$ be the set of irreducible, symmetric factors of $f \in \mathbf{R}[X]$. If $\mathcal{P} \in \mathrm{Irr}_{\mathbf{R}}(f)$, let $n_{\mathcal{P}} > 0$ be the integer such that $\mathcal{P}^{n_{\mathcal{P}}}$ is the power of $\mathcal{P}$ dividing f.

We denote by $\mathrm{Mil}(f)$ the set of maps $\tau : \mathrm{Irr}_{\mathbf{R}}(f) \to \mathbf{2Z}$ such that the image of $\mathcal{P} \in \mathrm{Irr}_{\mathbf{R}}(f)$ belongs to the set $\{-2n_{\mathcal{P}}, \dots, 2n_{\mathcal{P}}\}$. Let $\mathrm{Mil}_{r,s}(f)$ be the subset of $\tau \in \mathrm{Mil}(f)$ such that

$$\sum_{\mathcal{P} \in \mathrm{Irr}_{\mathbf{R}}(f)} \tau_{\mathcal{P}} = r - s.$$

Definition 27.2. An element of $\mathrm{Mil}(f)$ is called a *Milnor index*.

Recall from the previous sections that the following sets are in bijective correspondance:

(a) Conjugacy classes of semisimple elements of $\mathrm{SO}_{r,s}(\mathbf{R})$ with characteristic polynomial f.

(b) Isomorphism classes of $\mathbf{R}[\Gamma]$-quadratic forms on $M \otimes_{\mathbf{Q}} \mathbf{R}$ of signature (r, s).

(c) $\mathrm{Mil}_{r,s}(f)$.

To a semisimple isometry $t \in \mathrm{SO}_{r,s}(\mathbf{R})$ with characteristic polynomial f, the above bijection associates an $\mathbf{R}[\Gamma]$-quadratic form $b(t)$ on the module $M \otimes_{\mathbf{Q}} \mathbf{R}$. With the notation of §24 we have

Proposition 27.3. *Let $t \in \mathrm{SO}_{r,s}(\mathbf{R})$ be a semisimple isometry with characteristic polynomial f. The following properties are equivalent:*

(i) *The isometry t preserves an even, unimodular lattice.*

(ii) *The global condition $(\mathrm{G})_{b(t),0}$ is fulfilled for $(V, q_{r,s})$.*

Proof. By Proposition 25.7, the existence of an even, unimodular lattice having an isometry with characteristic polynomial f and square-free minimal polynomial implies conditions (G1) and $(\mathrm{G2})_0$. Since $t \in \mathrm{SO}_{r,s}(\mathbf{R})$ preserves the lattice, $(\mathrm{G})_{b(t),0}$ holds; therefore (i) implies (ii). Conversely, let us show that (ii) implies (i). By Proposition 25.7, there exists an even, unimodular lattice having an isometry with characteristic polynomial f and square-free minimal polynomial; condition $(\mathrm{G})_{b(t),0}$ implies that it is preserved by $t \in \mathrm{SO}_{r,s}(R)$. ■

As in §25, we obtain a homomorphism

$$\epsilon : \text{Ш}_g \to \mathbf{Z}/2\mathbf{Z},$$

defined in terms of finite places, that is, $C(V')$. Moreover, to all elements $a \in C(V'')$, we associate a homomorphism

$$\epsilon_a : \text{Ш}_g \to \mathbf{Z}/2\mathbf{Z}.$$

Recall from §16 that an $\mathbf{R}[\Gamma]$-quadratic form on $M \otimes_{\mathbf{Q}} \mathbf{R}$ gives rise to an element $\lambda^{v_\infty} \in \mathcal{LR}^{v_\infty}$, and hence also to $a(\lambda^{v_\infty}) \in C(V'')$. The above bijection allows us to associate

- to $t \in \mathrm{SO}_{r,s}(\mathbf{R})$ an element $a_t \in C(V'')$;
- to $\tau \in \mathrm{Mil}_{r,s}(f)$ an element $a_\tau \in C(V'')$.

Theorem 27.4. *Let $t \in \mathrm{SO}_{r,s}(\mathbf{R})$ be a semisimple isometry with characteristic polynomial f. The following are equivalent:*

(a) *The isometry t preserves an even, unimodular lattice.*

(b) $\epsilon + \epsilon_{a_t} = 0$.

Proof. By Proposition 27.3, property (a) holds if and only if the global condition $(\mathrm{G})_{b(t),0}$ is fulfilled for $(V, q_{r,s})$. On the other hand, this is equivalent to (b) by Theorem 24.2. ∎

Corollary 27.5. *If $Ш_g = 0$, then all semisimple elements of $\mathrm{SO}_{r,s}(\mathbf{R})$ with characteristic polynomial f preserve an even, unimodular lattice.*

Proof. This is an immediate consequence of Theorem 27.4. ∎

Note that this is a generalization of Theorem 1.3 of [GM 02]; indeed, if f is irreducible, then $Ш_g = 0$.

If L is a lattice of signature (r, s) having an isometry t with characteristic polynomial f and minimal polynomial g, then t extends to a semisimple element of $\mathrm{SO}_{r,s}(\mathbf{R})$, and this element gives rise to an element of $\mathrm{Mil}_{r,s}(f)$; this element will be called the *Milnor index* of the pair (L, t).

The following results are reformulations of Theorem 27.4 and Corollary 27.5.

Theorem 27.6. *Let $\tau \in \mathrm{Mil}_{r,s}(f)$. The following are equivalent:*

(a) *There exists an even, unimodular lattice having an isometry with characteristic polynomial f and Milnor index τ.*

(b) $\epsilon + \epsilon_{a_\tau} = 0$.

Corollary 27.7. *Assume that $Ш_g = 0$. Then every $\tau \in \mathrm{Mil}_{r,s}(f)$ occurs as the Milnor index of an even, unimodular lattice with an isometry of characteristic polynomial f.*

As shown by the following example, if $Ш_g \neq 0$, then Theorem 27.6 allows us to determine which Milnor indices occur.

Example 27.8. As in Example 25.15, let

$$f_1 = \Phi_{21}, \quad f_2 = \Phi_{147}, \quad \text{and} \quad f = g = f_1 f_2.$$

We have already seen that conditions (C1) and (C2) are satisfied for all pairs of integers (r, s) with $r, s \geqslant 0$ such that $r \equiv s \pmod 8$ and $r + s = \deg(f) = 96$, and that $Ш_g \simeq \mathbf{Z}/2\mathbf{Z}$; let $c \in Ш_g$ be the only non-trivial element.

The homomorphism $\epsilon : Ш_g \to \mathbf{Z}/2\mathbf{Z}$ satisfies $\epsilon(c) = 1$. The homomorphism ϵ_a depends on the choice of $a \in \mathcal{C}(V'') = \mathcal{C}^{v_\infty}$. There are two possibilities: $a(1) = a(2) = 0$ and $a'(1) = a'(2) = 1$. Hence $\epsilon + \epsilon_a \neq 0$ and $\epsilon + \epsilon_{a'} = 0$.

By Theorem 27.6, there exists an even, unimodular lattice having an isometry with characteristic polynomial f and Milnor index τ if and only if $a_\tau = a'$.

Let $r, s \geqslant 0$ be integers such that $r \equiv s \pmod 8$ and $r + s = \deg(f) = 96$. Since $n_{\mathcal{P}} = 2$ for all $\mathcal{P} \in \mathrm{Irr}_{\mathbf{R}}(f)$, the set $\mathrm{Mil}_{r,s}(f)$ consists of the maps

$$\tau : \mathrm{Irr}_{\mathbf{R}}(f) \to \{-2, 2\} \quad \text{with} \quad \sum_{\mathcal{P} \in \mathrm{Irr}_{\mathbf{R}}(f)} \tau_{\mathcal{P}} = r - s.$$

The Milnor index map τ is determined by the two maps

$$\tau_1 : \mathrm{Irr}_{\mathbf{R}}(f_1) \to \{-2, 2\} \quad \text{and} \quad \tau_2 : \mathrm{Irr}_{\mathbf{R}}(f_2) \to \{-2, 2\}.$$

For $i = 1, 2$, let N_i be the number of $\mathcal{P} \in \mathrm{Irr}_{\mathbf{R}}(f_i)$ such that $\tau_i(\mathcal{P}) = -2$. Since $r \equiv s \pmod 8$ and $r + s = 96 \equiv 0 \pmod 8$, we have $s \equiv 0 \pmod 4$. Therefore $N_1 + N_2$ is even, hence $N_1 \equiv N_2 \pmod 2$.

We have $a_\tau = a$ if N_1 is even, and $a_\tau = a'$ if N_1 is odd. Set

$$N(\tau) = N_1 \pmod 2.$$

In summary, we obtain:

There exists an even, unimodular lattice having an isometry with characteristic polynomial f and Milnor index τ if and only if $N(\tau) = 1$.

28. Knots

A *knot* is a smooth, oriented submanifold of S^3, homeomorphic to S^1. One of the classical knot invariants is the *Alexander polynomial*, another is the *signature*.

The results of the previous sections can be applied to decide for which pair (r, s) there exists a knot with Alexander polynomial Δ and signature (r, s). For simplicity, we restrict to monic polynomials Δ such that $\Delta(-1) = \pm 1$; these polynomials will be called *unramified*. Moreover, we assume that Δ is a product of distinct irreducible, symmetric polynomials. The general case will be treated elsewhere.

Still assuming that Δ is unramified and square-free, we deal with a more precise question. To each irreducible, symmetric factor $\mathcal{P}$ of $\Delta \in \mathbf{R}[X]$, one associates a *Milnor signature* $\sigma_{\mathcal{P}} = (2, 0)$ or $(0, 2)$. Given Δ and $\sigma_{\mathcal{P}}$ as above, we give a necessary and sufficient criterion for the existence of a knot with Alexander polynomial Δ and Milnor signatures $\sigma_{\mathcal{P}}$.

As usual in knot theory, the results are expressed in terms of the *index* $r - s$ rather than the signature (r, s), and the *Milnor indices* $\tau_{\mathcal{P}}$ rather than the Milnor signatures $\sigma_{\mathcal{P}}$.

For background information on the various notions of knot signatures (that is, indices), see the survey paper of Ghys and Ranicki [GR 16], explaining the history of the topic and its connection to other aspects of geometry and topology; see also the more recent survey of Anthony Conway [C 19].

We start by recalling some facts on Seifert forms, and then come back to the applications to knot theory.

29. Seifert forms

A *Seifert form* is by definition a $\mathbf{Z}$-bilinear form $\mathcal{A} : \mathcal{L} \times \mathcal{L} \to \mathbf{Z}$, where $\mathcal{L}$ is a free $\mathbf{Z}$-module of finite rank such that the skew-symmetric form $\mathcal{I} : \mathcal{L} \times \mathcal{L} \to \mathbf{Z}$ given by

$$\mathcal{I}(x, y) = \mathcal{A}(x, y) - \mathcal{A}(y, x)$$

has determinant 1. The symmetric form $\mathcal{Q} : \mathcal{L} \times \mathcal{L} \to \mathbf{Z}$ defined by

$$\mathcal{Q}(x, y) = \mathcal{A}(x, y) + \mathcal{A}(y, x)$$

is called the *quadratic form* associated to the Seifert form $\mathcal{A}$.

The *index* (or signature) of $\mathcal{A}$ is by definition the index (or signature) of the quadratic form $\mathcal{Q}$ (see Trotter [T 62, Proposition 5.1], or Murasugi [Mu 65]).

The *Alexander polynomial* of $\mathcal{A}$, denoted by $\Delta_{\mathcal{A}}$, is by definition the determinant of the form $\mathcal{L} \times \mathcal{L} \to \mathbf{Z}[X]$ given by

$$(x, y) \mapsto \mathcal{A}(x, y)X - \mathcal{A}(y, x).$$

Note that $\Delta_{\mathcal{A}}(1) = 1$, $\Delta_{\mathcal{A}}(0) = \det(\mathcal{A})$, and $\Delta_{\mathcal{A}}(-1) = \det(\mathcal{Q})$.

We say that a polynomial $\Delta \in \mathbf{Z}[X]$ is *unramified* if Δ is monic, $\Delta(1) = 1$, and $\Delta(-1) = \pm 1$. In what follows, we only consider Seifert forms with unramified Alexander polynomials. Note that this implies that $\det(\mathcal{A}) = 1$ and $\det(\mathcal{Q}) = \pm 1$; in particular, $\mathcal{Q}$ is a unimodular lattice. Let $\mathcal{T} : \mathcal{L} \to \mathcal{L}$ be defined by $\mathcal{A}(\mathcal{T}(x), y) = \mathcal{A}(y, x)$. We have $\mathcal{Q}(\mathcal{T}(x), \mathcal{T}(y)) = \mathcal{Q}(x, y)$ for all $x, y \in \mathcal{L}$, in other words, $\mathcal{T}$ is an isometry of $\mathcal{Q}$. Note that the characteristic polynomial of $\mathcal{T}$ is equal to $\Delta_{\mathcal{A}}$.

Assume in addition that $\Delta_{\mathcal{A}}$ is a product of distinct irreducible, symmetric polynomials of $\mathbf{Z}[X]$.

For all irreducible, symmetric factors $\mathcal{P} \in \mathbf{R}[X]$ of $\Delta_{\mathcal{A}}$, we define a *Milnor index* (and Milnor signature) of $(\mathcal{Q}, \mathcal{T})$ as in [M 68, §5]; see also §26. These will be called Milnor indices (and signatures) of $\mathcal{A}$.

Given a pair $(\mathcal{Q}, \mathcal{T})$ consisting of a unimodular lattice $\mathcal{Q}$ and an isometry $\mathcal{T}$ of characteristic polynomial Δ, we recover a Seifert form $\mathcal{A}$ with $\mathcal{Q}(x, y) = \mathcal{A}(x, y) + \mathcal{A}(y, x)$ for all $x, y \in \mathcal{L}$ (see for instance Levine [Le 69, §9] for a similar argument).

Recall from Notation 27.1 that $\mathrm{Irr}_{\mathbf{R}}(\Delta_{\mathcal{A}})$ is the set of irreducible, symmetric factors of $\Delta_{\mathcal{A}} \in \mathbf{R}[X]$. Since $\Delta_{\mathcal{A}}$ is square-free, we have $n_{\mathcal{P}} = 1$ for all $\mathcal{P}$ in $\mathrm{Irr}_{\mathbf{R}}(\Delta_{\mathcal{A}})$. Moreover, recall that we denote by $\mathrm{Mil}(\Delta_{\mathcal{A}})$ the set of maps $\tau : \mathrm{Irr}_{\mathbf{R}}(\Delta_{\mathcal{A}}) \to \{-2, 2\}$, and by $\mathrm{Mil}_{r,s}(\Delta_{\mathcal{A}})$ the subset of $\mathrm{Mil}(\Delta_{\mathcal{A}})$ such that $\sum_{\mathcal{P} \in \mathrm{Irr}_{\mathbf{R}}(\Delta_{\mathcal{A}})} \tau_{\mathcal{P}} = r - s$.

Hence we have the following

Proposition 29.1. *Let $r, s \geqslant 0$ be integers, and let $\Delta \in \mathbf{Z}[X]$ be an unramified polynomial that is a product of distinct irreducible, symmetric polynomials of $\mathbf{Z}[X]$. Let $\tau \in \mathrm{Mil}_{r,s}(\Delta)$. The following are equivalent:*

(a) *There exists a Seifert form with Alexander polynomial* Δ *and Milnor index* τ.

(b) *There exists an even, unimodular lattice* L *having an isometry* t *of characteristic polynomial* Δ *such that the Milnor index of* (L, t) *is* τ.

In particular, there exists a Seifert form with Alexander polynomial Δ and index $r - s$ if and only if there exists an even, unimodular lattice of index $r - s$ having an isometry with characteristic polynomial Δ.

30. Knots and Seifert forms

We keep the notation of Sections 28 and 29. To every knot Σ in S^3, we associate a Seifert form $\mathcal{A}_\Sigma$ (see for instance [K 87, Chapter VII], [Lick 97, Definition 6.4], [Liv 93, Chapter 6, §1]). It is well-known that the Alexander polynomial of $\mathcal{A}_\Sigma$ is an invariant of the knot; the same is true for the index (see Trotter [T 62, Proposition 5.1]) and the Milnor indices (see Milnor [M 68, §5]).

The following result of Seifert shows that all Seifert forms are realized by knots (see [Se 34]).

Theorem 30.1. *Let* $\mathcal{A}$ *be a Seifert form. Then there exists a knot* Σ *in* S^3 *such that* $\mathcal{A}$ *is the Seifert form of* Σ.

Combining this result with Theorem 29.1, we obtain the following

Proposition 30.2. *Let* $r, s \geqslant 0$ *be integers, and let* $\Delta \in \mathbf{Z}[X]$ *be an unramified polynomial that is a product of distinct irreducible, symmetric polynomials of* $\mathbf{Z}[X]$. *Let* $\tau \in \mathrm{Mil}_{r,s}(\Delta)$. *The following are equivalent:*

(a) *There exists a knot with Alexander polynomial* Δ *and Milnor index* τ.

(b) *There exists an even, unimodular lattice* L *having an isometry* t *of characteristic polynomial* Δ *such that the Milnor index of* (L, t) *is* τ.

In particular, there exists a knot with Alexander polynomial Δ and index $r - s$ if and only if there exists an even, unimodular lattice of index $r - s$ having an isometry with characteristic polynomial Δ. Using this result, we can apply Theorem 27.6 to answer the questions of §28.

We start by recalling some definitions from §25 and §27. Let $\Delta \in \mathbf{Z}[X]$ be an unramified polynomial as above, and set $2n = \deg(\Delta)$.

Conditions (C1) *and* (C2)

Recall from §25 that the local conditions for the existence of an even, unimodular lattice of signature (r, s) and characteristic polynomial Δ can be translated into two conditions (C1) and (C2). We now recall these conditions in our situation.

- Since Δ is unramified, condition (C1) becomes: $\Delta(-1) = (-1)^n$.

Recall that $m(\Delta)$ is the number of roots z of Δ with $|z| > 1$.

- Let (r, s) be a pair of non-negative integers. Condition (C2) holds if $r + s = 2n$, $r \equiv s \pmod 8$, $r \geqslant m(\Delta)$, $s \geqslant m(\Delta)$, and $m(\Delta) \equiv r \equiv s \pmod 2$.

It follows from Lemma 25.3 that conditions (C1) and (C2) are necessary for the existence of a knot with Alexander polynomial Δ and index $r - s$.

Example 30.3. Assume moreover that Δ is a product of cyclotomic polynomials ϕ_m with $m \geq 3$. Then $m(\Delta) = 0$, hence if $r + s = 2n,\ r \equiv s \pmod 8$, then condition (C2) holds.

The obstruction group

Recall from §21 and §25 the definition of the "obstruction group" $Ш_\Delta$. Let I be the set of irreducible factors of Δ. For all $f, g \in I$, let $V_{f,g}$ be the set of prime numbers $p \in V_f \cap V_g$ such that f and g have a common irreducible, symmetric factor mod p. Consider the equivalence relation on I generated by the elementary equivalence

$$f \sim_e g \iff V_{f,g} \neq \varnothing,$$

and let $\bar{I}$ be the set of equivalence classes; the group $Ш_\Delta$ is the quotient of $C(\bar{I})$ by the constant maps.

By Corollary 27.7, we have

Corollary 30.4. *Assume that conditions* (C1) *and* (C2) *hold. If* $Ш_\Delta = 0$*, then for all* $\tau \in \mathrm{Mil}_{r,s}(f)$ *there exists a knot with Milnor index* τ*. In particular, there exists a knot with index* $r - s$*.*

If $Ш_\Delta \neq 0$, then we obtain a necessary and sufficient condition for $\tau \in \mathrm{Mil}_{r,s}(f)$ to be the Milnor index of a knot (cf. Theorem 27.6). The aim of the next section is to illustrate this by some examples.

31. Alexander polynomials of torus knots and indices

Let $u, v > 1$ be odd integers, and assume that u and v are prime to each other. Set

$$\Delta_{u,v} = \frac{(X^{uv} - 1)(X - 1)}{(X^u - 1)(X^v - 1)}.$$

It is well-known that $\Delta_{u,v}$ is the Alexander polynomial of the (u, v)-torus knot; the indices of torus knots have been studied in many papers (see for instance [Bo 11, BO 10, C 10, GLM 81, HM 68], [K 87, Chapter XII], [Ke 79, KM 94, Lith 79, Liv 18, Mat 77, Mu 06]).

The aim of this section is to determine which indices occur for knots with Alexander polynomial $\Delta_{u,v}$.

The polynomial $\Delta_{u,v}$ is a product of cyclotomic polynomials

$$\Delta_{u,v} = \prod \Phi_{\alpha\beta}$$

where the product is over the set of all pairs (α, β) for which α is a factor of u, β is a factor of v, and both are greater than 1 (see for instance [Liv 18, Lemma 2.1]). Set $\deg(\Delta_{u,v}) = 2n$, and note that n is even and $\Delta_{u,v}(1) = \Delta_{u,v}(-1) = 1$; hence condition (C1) holds.

Let (r, s) be a pair of non-negative integers such that

$$r + s = 2n \quad \text{and} \quad r \equiv s \pmod 8.$$

By Example 30.3, condition (C2) holds for $\Delta_{u,v}$ and (r, s). In order to apply the Hasse principle results of §25 and §27, the next step is to determine the obstruction group $Ш_{\Delta_{u,v}}$.

The group $Ш_{\Delta_{u,v}}$

If f and g are monic polynomials in $\mathbf{Z}[X]$, let $V_{f,g}$ be the set of prime numbers p such that $f \pmod p$ and $g \pmod p$ have a common irreducible and symmetric factor in $\mathbf{F}_p[X]$. Let I be the set of irreducible factors of $\Delta_{u,v}$, and recall that the definition of the group $Ш_{\Delta_{u,v}}$ involves the equivalence relation on I generated by the elementary equivalence

$$f \sim_e g \iff V_{f,g} \neq \varnothing.$$

Therefore in order to determine the group $Ш_{\Delta_{u,v}}$, we need to decide when $V_{f,g} \neq \varnothing$ for two cyclotomic polynomials f and g. We start with a lemma:

Lemma 31.1. *Let m and m' be odd integers with $m \geqslant 3$ and $m' > m$. Let p be a prime number. The cyclotomic polynomials Φ_m and $\Phi_{m'}$ have a common factor mod p if and only if $m' = mp^e$ for some integer $e \geqslant 1$.*

Proof. The resultant of the cyclotomic polynomials Φ_m and $\Phi_{m'}$ is divisible by p if and only if $m' = mp^e$ for some integer $e \geqslant 1$ (see for instance [Ap 70, Theorem 4]). By a well-known property of the resultant, this is equivalent for Φ_m and $\Phi_{m'}$ having a common factor mod p. ∎

We need a criterion for the existence of *symmetric* irreducible factors mod p; this will be done in the following proposition, relying on well-known properties of cyclotomic polynomials and cyclotomic fields. For all integers $m \geqslant 2$, let ζ_m be a primitive m-th root of unity, and let $\mathbf{Q}(\zeta_m)$ be the corresponding cyclotomic field.

Proposition 31.2. *Let $m \geqslant 3$ be an odd integer, and let p be an odd prime number. The following properties are equivalent:*

(a) *The polynomial Φ_m has a symmetric irreducible factor mod p.*

(b) *The prime ideals above p in $\mathbf{Q}(\zeta_m + \zeta_m^{-1})$ are inert in $\mathbf{Q}(\zeta_m)$.*

(c) *The subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$ generated by p contains -1.*

Proof. The equivalence (a)⇔(b) is well-known: see for instance [W 97, Proposition 2.14]. Let us show that (a)⇔(c). Let A be the group $(\mathbf{Z}/m\mathbf{Z})^\times$ written additively, let $m_p : A \to A$ be multiplication by p, and let $\epsilon : A \to A$ be the map sending a to $-a$. Both (a) and (c) are equivalent to

(d) There exists an orbit of m_p stable by ϵ.

This concludes the proof of the proposition. ■

Proposition 31.2 and Lemma 31.1 suffice to determine the obstruction group of a product of cyclotomic polynomials, in particular the group $Ш_{\Delta_{u,v}}$. A full description would be rather heavy, so we only give some simple special cases and examples. The first remark is that if moreover m is a prime and $m \equiv 3 \pmod 4$, property (c) of Proposition 31.2 takes a very simple form.

Corollary 31.3. *Let m be a prime number with $m \equiv 3 \pmod 4$, and let p be an odd prime number. Then*

$$\Phi_m \text{ has a symmetric irreducible factor mod } p \iff \left(\tfrac{p}{m}\right) = -1.$$

Proof. Indeed, it is easy to see that the subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$ generated by p contains -1 if and only if p is not a square mod m, in other words, $(\frac{p}{m}) = -1$. Therefore the corollary follows from Proposition 31.2. ■

Example 31.4. Let p and q be distinct odd prime numbers with $q \equiv 3 \pmod 4$. Let $e \geqslant 1$ be an integer, and set $\Delta = \Delta_{p^e,q}$. Then

$$Ш_\Delta = 0 \quad \text{if } \left(\tfrac{p}{q}\right) = -1, \quad \text{and} \quad Ш_\Delta \simeq (\mathbf{Z}/2\mathbf{Z})^{e-1} \quad \text{if } \left(\tfrac{p}{q}\right) = 1.$$

Indeed, let I be the set of irreducible factors of Δ; the set I consists of the cyclotomic polynomials $\Phi_{p^k q}$ for $1 \leqslant k \leqslant e$. If $(\frac{p}{q}) = -1$, then by Corollary 31.3 and Lemma 31.1 all these polynomials have common symmetric, irreducible factors mod p, hence $V_{f,g} = \{p\}$ for all $f, g \in I$. Therefore all the polynomials are equivalent, and the set $\overline{I}$ of equivalence classes has one element; $C(\overline{I})$ modulo the constant maps is trivial, hence $Ш_\Delta = 0$.

On the other hand, if $(\frac{p}{q}) = 1$, then by the above results $V_{f,g} = \varnothing$ for all $f, g \in I$. All the polynomials are in different equivalence classes, hence $\overline{I}$ has e elements, $C(\overline{I}) \simeq (\mathbf{Z}/2\mathbf{Z})^e$, and $Ш_\Delta \simeq (\mathbf{Z}/2\mathbf{Z})^{e-1}$.

Example 31.5. Let p, p_1 and p_2 be distinct prime numbers with $p \equiv p_1 \equiv p_2 \equiv 3 \pmod 4$, and set $\Delta = \Delta_{p,p_1p_2}$. Since p_1 and p_2 play symmetric roles and $(\frac{p_2}{p_1}) = -(\frac{p_1}{p_2})$, we may assume that $(\frac{p_1}{p_2}) = 1$. We have

$$Ш_\Delta \simeq (\mathbf{Z}/2\mathbf{Z})^2 \iff \left(\tfrac{p_2}{p}\right) = 1,$$
$$Ш_\Delta \simeq \mathbf{Z}/2\mathbf{Z} \iff \left(\tfrac{p_2}{p}\right) = -1.$$

In particular, $Ш_\Delta$ cannot be trivial.

Indeed, let I be the set of irreducible factors of Δ; the set I consists of the cyclotomic polynomials Φ_{pp_1}, Φ_{pp_2} and $\Phi_{pp_1p_2}$. The first two are not equivalent (see Lemma 31.1).

Note that since $(\frac{p_1}{p_2}) = 1$, the polynomials Φ_{pp_2} and $\Phi_{pp_1p_2}$ are not equivalent; this follows from Proposition 31.2. Hence $\overline{I}$ has at least two elements, and therefore $Ш_\Delta \neq 0$. On the other hand, since $(\frac{p_2}{p_1}) = -1$, Proposition 31.2 shows that Φ_{pp_1} and $\Phi_{pp_1p_2}$ are equivalent if and only if $(\frac{p_2}{p}) = -1$.

We already know that if $Ш_{\Delta_{u,v}} = 0$, then all signatures (r, s) as above (hence all indices $r - s$) are possible, as also are all Milnor indices (see Corollary 30.4). If however $Ш_{\Delta_{u,v}} \neq 0$, then we need further information, in particular the homomorphism ϵ.

The homomorphism $\epsilon : Ш_{\Delta_{u,v}} \to \mathbf{Z}/2\mathbf{Z}$

Recall that V' is the set of finite places of $\mathbf{Q}$, that is, the set of prime numbers, and $\epsilon : Ш_{\Delta_{u,v}} \to \mathbf{Z}/2\mathbf{Z}$ is defined in terms of the local data associated to V'. Since $\Delta_{u,v}$ is a product of cyclotomic polynomials, ϵ can be described explicitly as follows.

As above, we denote by I the set of irreducible factors of $\Delta_{u,v}$. If $f \in I$ with $f = \Phi_m$ and if p is a prime number, set

$$\delta_f^p = \begin{cases} 1 & \text{if } p \text{ divides } m,\ p \equiv 3 \pmod 4, \text{ and } \Phi_m \text{ has a symmetric} \\ & \text{irreducible factor mod } p, \\ 0 & \text{otherwise.} \end{cases}$$

For all prime numbers p, let $a^p : I \to \mathbf{Z}/2\mathbf{Z}$ be defined by $a^p(f) = \delta_f^p$.

Proposition 31.6. *The homomorphism* $\epsilon : Ш_{\Delta_{u,v}} \to \mathbf{Z}/2\mathbf{Z}$ *is given by*

$$\epsilon(c) = \sum_{p \in V'} \sum_{f \in I} c(f) a^p(f).$$

Proof. For all $f \in I$, set $E_f = \mathbf{Q}[X]/(f)$ and let $\sigma_f : E_f \to E_f$ be the involution induced by $X \mapsto X^{-1}$; note that E_f is a cyclotomic field, and σ_f is complex conjugation. Let F_f be the fixed field of σ_f. Let d_f be the discriminant of E_f, and let $p^{e_p(f)}$ be the power of p dividing d_f. Then $e_p(f) \equiv \delta_f^p \pmod 2$ (see for instance [W 97, Propositions 2.1 and 2.7]).

Since $f = \Phi_m$ for some integer m that is not a prime power, no finite places of F_f ramify in E_f (see for instance [W 97, Proposition 2.15 (b)]). Moreover, the prime ideals of F_f above p are inert in E_f if and only if Φ_m has a symmetric irreducible factor mod p (see Proposition 31.2). Hence Corollary 6.2 and Proposition 6.4 of [BT 20] imply that we can take $a^p(f) = \delta_f^p$. The proposition now follows from the definition of $\epsilon : Ш_{\Delta_{u,v}} \to \mathbf{Z}/2\mathbf{Z}$ in §23, where it is also shown that the homomorphism is independent of the choice of local data. ∎

Milnor indices and the homomorphism $\epsilon_\tau : Ш_{\Delta_{u,v}} \to \mathbf{Z}/2\mathbf{Z}$

Let $\tau \in \mathrm{Mil}_{r,s}(\Delta_{u,v})$; the homomorphism $\epsilon_\tau : Ш_{\Delta_{u,v}} \to \mathbf{Z}/2\mathbf{Z}$ is as follows. For all $f \in I$, let $n(f)$ be the number of $\mathcal{P} \in \mathrm{Irr}(\mathbf{R})$ dividing f such that $\tau(\mathcal{P}) = -2$. Let $a_\tau : I \to \mathbf{Z}/2\mathbf{Z}$

be defined by $a_\tau(f) = n(f) \pmod 2$. Then $\epsilon_\tau : Ш_{\Delta_{u,v}} \to \mathbf{Z}/2\mathbf{Z}$ is by definition

$$\epsilon_\tau(c) = \sum_{f\in I} c(f)a_\tau(f).$$

A necessary and sufficient criterion

Applying Theorem 27.6, we get

Theorem 31.7. *Let* $\tau \in \mathrm{Mil}_{r,s}(\Delta_{u,v})$. *There exists a knot with Alexander polynomial* $\Delta_{u,v}$ *and Milnor index* τ *if and only if* $\epsilon + \epsilon_\tau = 0$.

Proof. This is an immediate consequence of Theorem 27.6, noting that the local conditions always hold. ■

We illustrate this result by the following example:

Example 31.8. We keep the notation of Example 31.4; in particular, p and q are distinct odd prime numbers with $q \equiv 3 \pmod 4$, $e \geqslant 1$ is an integer, and $\Delta = \Delta_{p^e,q}$.

- If $(\frac{p}{q}) = -1$, then $Ш_\Delta = 0$. This implies that all $\tau \in \mathrm{Mil}_{r,s}(\Delta)$ occur as Milnor indices of knots. An integer ι is the index of a knot with Alexander polynomial Δ if and only if $\iota \equiv 0 \pmod 8$, and $|\iota| \leqslant 2n$ (see Example 31.4 and Corollary 30.4).
- If $(\frac{p}{q}) = 1$, then $Ш_\Delta \simeq (\mathbf{Z}/2\mathbf{Z})^{e-1}$ (see Example 31.4). Let $\tau \in \mathrm{Mil}_{r,s}(\Delta)$. In order to decide whether τ occurs as the Milnor index of a knot, we determine the homomorphisms ϵ and ϵ_τ.

Recall that I is the set of irreductible factors of Δ, and I consists of the cyclotomic polynomials $\Phi_{p^k q}$ for $1 \leqslant k \leqslant e$.

Still assuming $(\frac{p}{q}) = 1$, the result depends on the congruence class of p mod 4:

- Assume first that $p \equiv 3 \pmod 4$, and note that $(\frac{q}{p}) = -(\frac{p}{q}) = -1$.

If $f \in I$, we have $\delta_f^q = 1$ and $\delta_f^\ell = 0$ for all prime numbers $\ell \neq q$.

For all prime numbers ℓ, let $a^\ell : I \to \mathbf{Z}/2\mathbf{Z}$ be defined by $a^\ell(f) = \delta_f^\ell$, hence $a^q(f) = 1$ and $a^\ell(f) = 0$ if $\ell \neq q$. The associated homomorphism $\epsilon : Ш_\Delta \to \mathbf{Z}/2\mathbf{Z}$ is given by

$$\epsilon(c) = \sum_{\ell\in V'}\sum_{f\in I} c(f)a^\ell(f) = \sum_{f\in I} c(f).$$

On the other hand, we have

$$\epsilon_\tau(c) = \sum_{f\in I} c(f)a_\tau(f).$$

Therefore

$$\epsilon + \epsilon_\tau = 0 \iff a_\tau(f) = 1 \text{ for all } f \in I.$$

By definition, this means that $n(f)$ is odd for all $f \in I$, in other words, each $f \in I$ is divisible by an odd number of $\mathcal{P} \in \mathrm{Irr}(\mathbf{R})$ with $\tau(\mathcal{P}) = -2$. In summary:

An element $\tau \in \mathrm{Mil}_{r,s}(\Delta)$ occurs as the Milnor index of a knot if and only if for all $f \in I$, the number of $\mathcal{P} \in \mathrm{Irr}(\mathbf{R})$ dividing f such that $\tau(\mathcal{P}) = -2$ is odd.

In particular, an integer ι is the index of a knot with Alexander polynomial Δ if and only if $\iota \equiv 0 \pmod 8$, and $|\iota| \leqslant 2n - 4(e-1)$.

• Assume now that $p \equiv 1 \pmod 4$, and note that $(\frac{q}{p}) = (\frac{p}{q}) = 1$. In this case, $\delta_f^\ell = 0$ for all prime numbers ℓ and for all $f \in I$. This implies that $\epsilon(c) = 0$ for all $c \in Ш_\Delta$. Recall that $\epsilon_\tau : Ш_\Delta \to \mathbf{Z}/2\mathbf{Z}$ is given by

$$\epsilon_\tau(c) = \sum_{f \in I} c(f) a_\tau(f).$$

Therefore

$$\epsilon + \epsilon_\tau = 0 \iff a_\tau(f) = 0 \text{ for all } f \in I.$$

This means that $n(f)$ is even for all $f \in I$, in other words, each $f \in I$ is divisible by an even number of $\mathcal{P} \in \mathrm{Irr}(\mathbf{R})$ with $\tau(\mathcal{P}) = -2$. This imposes a condition on the possible Milnor indices. However, this does not gives rise to additional conditions on the index; an integer ι is the index of a knot with Alexander polynomial Δ if and only if $\iota \equiv 0 \pmod 8$ and $|\iota| \leqslant 2n$.

References

[Ap 70] Apostol, T. M.: Resultants of cyclotomic polynomials. Proc. Amer. Math. Soc. **24**, 457–462 (1970) Zbl 0188.34002 MR 251010

[Ar 75] Arason, J. K.: Cohomologische Invarianten quadratischer Formen. J. Algebra **36**, 448–491 (1975) Zbl 0314.12104 MR 389761

[AEJ 84] Arason, J. K., Elman, R., Jacob, B.: The graded Witt ring and Galois cohomology. I. In: Quadratic and Hermitian Forms (Hamilton, Ont., 1983), CMS Conf. Proc. 4, Amer. Math. Soc., Providence, RI, 17–50 (1984) Zbl 0554.10013 MR 776446

[B 84] Bayer-Fluckiger, E.: Definite unimodular lattices having an automorphism of given characteristic polynomial. Comment. Math. Helv. **59**, 509–538 (1984) Zbl 0558.10029 MR 780074

[B 15] Bayer-Fluckiger, E.: Isometries of quadratic spaces. J. Eur. Math. Soc. **17**, 1629–1656 (2015) Zbl 1326.11008 MR 3361725

[BLP 18] Bayer-Fluckiger, E., Lee, T.-Y., Parimala, R.: Embeddings of maximal tori in classical groups and explicit Brauer–Manin obstruction. J. Eur. Math. Soc. **20**, 137–163 (2018) Zbl 1452.11037 MR 3743239

[B 20] Bayer-Fluckiger, E., Lee, T.-Y., Parimala, R.: Embeddings of maximal tori in classical groups, odd degree descent and Hasse principles. Matematica **1**, 115–130 (2022) Zbl 1318.11054 MR 4482728

[BT 20] Bayer-Fluckiger, E., Taelman, L.: Automorphisms of even unimodular lattices and equivariant Witt groups. J. Eur. Math. Soc. **22**, 3467–3490 (2020) Zbl 1458.11111 MR 4167013

[Bo 11] Borodzik, M.: Abelian ρ-invariants of iterated torus knots. In: Low-Dimensional and Symplectic Topology, Proc. Sympos. Pure Math. 82, Amer. Math. Soc., Providence, RI, 29–38 (2011) Zbl 1268.57003 MR 2768651

[BO 10] Borodzik, M., Oleszkiewicz, K.: On the signatures of torus knots. Bull. Polish Acad. Sci. Math. **58**, 167–177 (2010) Zbl 1219.57003 MR 2733048

[C 10] Collins, J.: The L^2 signature of torus knots. arXiv:1001.1329v3 (2010)

[C 19] Conway, A.: The Levine–Tristram signature: a survey. In: 2019–20 MATRIX Annals, MATRIX Book Ser. 4, Springer, Cham, 31–56 Zbl 1481.57007 MR 4294761

[GR 16] Ghys, É., Ranicki, A.: Signatures in algebra, topology and dynamics. In: Six Papers on Signatures, Braids and Seifert Surfaces, Ensaios Mat. 30, Soc. Brasil. Mat., Rio de Janeiro, 1–173 (2016) Zbl 1372.57001 MR 3617347

[GLM 81] Gordon, C. McA., Litherland, R. A., Murasugi, K.: Signatures of covering links. Canad. J. Math. **33**, 381–394 (1981) Zbl 0469.57004 MR 617628

[GM 02] 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

[HM 68] Hirzebruch, F., Mayer, K. H.: O(n)-Mannigfaltigkeiten, exotische Sphären und Singularitäten. Lecture Notes in Math. 57, Springer, Berlin (1968) Zbl 0172.25304 MR 0229251

[K 87] Kauffman, L. H.: On Knots. Ann. of Math. Stud. 115, Princeton Univ. Press, Princeton, NJ (1987) Zbl 0627.57002 MR 907872

[Ke 79] Kearton, C.: Signatures of knots and the free differential calculus. Quart. J. Math. Oxford Ser. (2) **30**, 157–182 (1979) Zbl 0406.57006 MR 534830

[KM 94] Kirby, R., Melvin, P.: Dedekind sums, μ-invariants and the signature cocycle. Math. Ann. **299**, 231–267 (1994) Zbl 0809.11027 MR 1275766

[K 19] Kirschmer, M.: Automorphisms of even unimodular lattices over number fields. J. Number Theory **197**, 121–134 (2019) Zbl 1412.11081 MR 3906493

[L 05] Lam, T. Y.: Introduction to Quadratic Forms over Fields. Grad. Stud. Math. 67, Amer. Math. Soc., Providence, RI (2005) Zbl 1068.11023 MR 2104929

[Le 69] Levine, J.: Invariants of knot cobordism. Invent. Math. **8**, 98–110, 355 (1969) Zbl 0179.52401 MR 253348

[Lick 97] Lickorish, W. B. R.: An Introduction to Knot Theory. Grad. Texts in Math. 175, Springer, New York (1997) Zbl 0886.57001 MR 1472978

[Lith 79] Litherland, R. A.: Signatures of iterated torus knots. In: Topology of Low-Dimensional Manifolds (Chelwood Gate, 1977), Lecture Notes in Math. 722, Springer, Berlin, 71–84 (1979) Zbl 0412.57002 MR 547456

[Liv 93] Livingston, C.: Knot Theory. Carus Math. Monogr. 24, Math. Assoc. of America, Washington, DC (1993) Zbl 0887.57008 MR 1253070

[Liv 18] Livingston, C.: Concordances from connected sums of torus knots to L-space knots. New York J. Math. **24**, 233–239 (2018) Zbl 1386.57011 MR 3778502

[Mat 77] Matumoto, T.: On the signature invariants of a non-singular complex sesquilinear form. J. Math. Soc. Japan **29**, 67–71 (1977) Zbl 0376.15013 MR 437456

[McM 02] 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

[McM 11] McMullen, C. T.: K3 surfaces, entropy and glue. J. Reine Angew. Math. **658**, 1–25 (2011) Zbl 1228.14031 MR 2831510

[McM 16] McMullen, C. T.: Automorphisms of projective K3 surfaces with minimum entropy. Invent. Math. **203**, 179–215 (2016) Zbl 1364.37103 MR 3437870

[M 68] Milnor, J. W.: Infinite cyclic coverings. In: Conference on the Topology of Manifolds (East Lansing, MI, 1967), Prindle, Weber & Schmidt, Boston, MA, 115–133 (1968) Zbl 0179.52302 MR 0242163

[M 69] Milnor, J.: On isometries of inner product spaces. Invent. Math. **8**, 83–97 (1969) Zbl 0177.05204 MR 249519

[Mu 65] Murasugi, K.: On a certain numerical invariant of link types. Trans. Amer. Math. Soc. **117**, 387–422 (1965) Zbl 0137.17903 MR 171275

[Mu 06] Murasugi, K.: Classical knot invariants and elementary number theory. In: Primes and Knots, Contemp. Math. 416, Amer. Math. Soc., Providence, RI, 167–196 (2006) Zbl 1141.57007 MR 2276141

[O'M 73] O'Meara, O. T.: Introduction to Quadratic Forms. Classics in Math., Springer, Berlin (2000) Zbl 1034.11003 MR 1754311

[Sch 85] Scharlau, W.: Quadratic and Hermitian Forms. Grundlehren Math. Wiss. 270, Springer, Berlin (1985) Zbl 0584.10010 MR 770063

[Se 34] Seifert, H.: Über das Geschlecht von Knoten. Math. Ann. **110**, 571–592 (1935) Zbl 0010.13303 MR 1512955

[S 77] Serre, J.-P.: Cours d'arithmétique. Presses Universitaires de France, Paris (1977) Zbl 0376.12001 MR 0498338

[S 18] 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 1455.20009 MR 3890220

[T 62] Trotter, H. F.: Homology of group systems with applications to knot theory. Ann. of Math. (2) **76**, 464–498 (1962) Zbl 0108.18302 MR 143201

[W 97] Washington, L. C.: Introduction to Cyclotomic Fields. 2nd ed., Grad. Texts in Math. 83, Springer, New York (1997) Zbl 0966.11047 MR 1421575