Isometries of quadratic spaces over global fields

Eva Bayer–Fluckiger

Introduction

Let k be a field of characteristic not 2. An *quadratic space* is a non–degenerate symmetric bilinear form $q : V \times V \to k$ defined on a finite dimensional k–vector space V, and an *isometry* of (V, q) is an element of $SO(q)$, in other words an isomorphism $t : V \to V$ such that $q(tx, ty) = q(x, y)$ for all $x, y \in V$ and that $\det(t) = 1$. In [7], Milnor investigated isometries of quadratic spaces, and raised the following question :

Question. Let q be a quadratic space over k, and let $f \in k[X]$ be an irreducible polynomial. How can we tell whether q has an isometry with minimal polynomial f ?

He gave an answer in the case of local fields. The main purpose of the present paper is to study this question for global fields.

Suppose that k is a global field, let q be an quadratic space, let $f \in k[X]$ be an irreducible polynomial, and let $F = f^m$ for some $m \in \mathbf{N}$. The following Hasse principle is proved in section 5 :

Theorem. *The quadratic space q has an isometry with characteristic polynomial F and minimal polynomial f if and only if such an isometry exists over all the completions of k.*

For $m = 1$, this is a consequence of a result of Prasad and Rapinchuk, cf. [9], th. 7.3. In order to obtain a necessary and sufficient criterion, we need to consider the case of *separable* minimal polynomials over local fields and the field of real numbers. This is done in §3 and §4, and leads for two necessary conditions over global fields, the *hyperbolicity condition* and the *signature condition* (cf. §5).

Let us suppose that F is symmetric, that $F(1)F(-1) \neq 0$ and that $\dim(V) = \deg(F)$. We have (see 5.2) :

Theorem. *The quadratic space q has an isometry with minimal polynomial f if and only if the signature condition and the hyperbolicity conditions are satisfied, and*

$$\det(q) = F(1)F(-1) \in k^*/k^{*2}.$$

The first two sections are devoted to some definitions and useful lemmas, most of them based on Milnor's paper [7]. Section 6 contains an application of the results of the paper to isometries of quadratic spaces extended from unimodular, even lattices, in relationship with a question of Gross and McMullen [5].

§1. Definitions, notation and basic facts.

Let k be a field of characteristic not 2. An *quadratic space* is a pair (V, q), where V is a finite dimensional k–vector space, and $q : V \times V \to k$ is a symmetric bilinear form of non–zero determinant. The *determinant* of (V, q) is denoted by $\det(q)$; it is an element of k^*/k^{*2}. For basic facts concerning quadratic spaces, see [8] and [9].

An *isometry* of the quadratic space (V, q) is an isomorphism $t : V \to V$ such that $q(tx, ty) = q(x, y)$ for all $x, y \in V$ and that $\det(t) = 1$.

The answer to Milnor's question is obvious if $f(X) = X + 1$ or $X - 1$, hence we can exclude these cases. This means that we can assume that $f(1)f(-1) \neq 0$. Therefore, throughout the paper the isometries are supposed to have *neither* 1 *nor* -1 *as an eigenvalue.*

The following results are well–known, see for instance Levine [6] and Milnor [7], as well as the appendix of [5].

A polynomial $f \in k[X]$ is said to be *symmetric* if $f(X) = X^{\deg(f)} f(X^{-1})$.

Proposition 1.1 *The minimal polynomials of isometries of quadratic spaces are symmetric of even degree.*

Proof. Let (V, q) be an quadratic space, and let $t : V \to V$ be an isometry of q. By definition, we have $q(tx, y) = q(x, t^{-1}y)$ for all $x, y \in V$. This implies that for any polynomial $p \in k[X]$, we have $q(p(t)x, y) = q(x, p(t^{-1})y)$ for all $x, y \in V$. Let $f \in k[X]$ be the minimal polynomial of t. Applying the above equality to $p = f$, we see that the endomorphism $t^{\deg f} f(t^{-1})$ annihilates V. As f is the minimal polynomial of t, this implies that f divides $X^{\deg f} f(X^{-1})$, therefore we have $f(X) = \epsilon X^{\deg f} f(X^{-1})$ for some $\epsilon = \pm 1$. Note that if $\epsilon = -1$, then $f(1) = 0$, hence f is divisible by $X - 1$. This is impossible, as we have supposed that 1 is not an eigenvalue of t. Therefore $\epsilon = 1$, hence f is symmetric. If $\deg(f)$ is odd, then this implies that $f(-1) = 0$, which contradicts the assumption that -1 is not an eigenvalue of t. Therefore $\deg(f)$ is even.

A basic observation is that there is a relationship between the determinant of an quadratic space, and the values of the characteristic polynomials of its isometries, as follows :

Proposition 1.2 *Let (V, q) be an quadratic space, and let $F \in k[X]$ be the characteristic polynomial of an isometry of q.Then*

$$\det(q) = F(1)F(-1) \in k^*/k^{*2}.$$

Proof. Let us define $q' : V \times V \to k$ by $q'(x,y) = q(x,(t-t^{-1})(y))$. Then q' is skew–symmetric, hence $\det(q') \in k^2$. On the other hand, we have $\det(q') = \det(q)F(1)F(-1)$, so the proposition is proved.

Proposition 1.3 *The characteristic polynomials of isometries of quadratic spaces are symmetric of even degree.*

Proof. This follows from a straightforward computation, see for instance [6], I. 7, Lemma (a).

§2. Primary decomposition and transfer

The aim of this section is to recall some results of Milnor [7], as well as to introduce some terminology that will be used later on. Let $f \in k[X]$ be a monic, irreducible polynomial. Let us define the *dual* of f as the monic, irreducible polynomial $f^* \in k[X]$ defined by $f^*(X) = \frac{1}{f(0)}X^m f(X^{-1})$. Note that f is symmetric if and only if it is equal to its dual polynomial.

Let (V,q) be an quadratic space of dimension $2n$, let t be an isometry of q and let F be the characteristic polynomial of t. For each monic, irreducible factor f of F, set

$$V_f = \{v \in V \mid f^i(t)(v) = 0 \text{ for some } i \in \mathbf{N}\}.$$

Let U and W be two subspaces of V. We say that U and W are *orthogonal* to each other if $q(u,w) = 0$ for all $u \in U$ and $w \in W$. We say that (V,q) is *hyperbolic* if V has a self–orthogonal subspace of dimension n.

Proposition 2.1 *Let f and g be two monic, irreducible factors of F. If $f \neq g^*$, then V_f and V_g are orthogonal to each other.*

Proof. See Milnor [7], Lemma 3.1.

Corollary 2.2 *If f is not symmetric, then $(V_f \oplus V_{f^*}, q)$ is hyperbolic.*

Proof. See [7], §3, Case 3.

Proposition 2.3 *We have the following orthogonal decomposition*

$$(V,q) \simeq \bigoplus (V_f, q) \oplus H$$

where the sum is taken over all distinct monic, symmetric and irreducible factors of F, and where H is a hyperbolic space.

Proof. This follows from prop. 2.1 and cor. 2.2.

Definition. A symmetric polynomial is said to be *hyperbolic* if none of its irreducible factors is symmetric.

Corollary 2.4 *A quadratic space having an isometry with hyperbolic characteristic polynomial is hyperbolic*

Proof. This is an immediate consequence of 2.3.

Proposition 2.5 *Let $f \in k[X]$ be a monic, symmetric, separable and irreducible polynomial, and set $K = k[X]/(f)$. Then sending X to X^{-1} induces a k–linear involution $\bar{\ }: K \to K$. Moreover, for every quadratic space (V, q) over k and every isometry having minimal polynomial f, there exists a non–degenerate hermitian form (V, h) over K such that for all $x, y \in V$*

$$q(x, y) = \mathrm{Tr}_{K/k}(h(x, y)).$$

Conversely, if V is a finite dimensional vector space over K and if $h : V \to V$ is a non–degenerate hermitian form, then setting

$$q(x, y) = \mathrm{Tr}_{K/k}(h(x, y))$$

for all $x, y \in V$ we obtain an quadratic space (V, q) over k together with an isometry with minimal polynomial f.

Proof. See [7], Lemma 1.1 and Lemma 1.2.

Lemma 2.6 *Let (V, q) be a hyperbolic quadratic space of dimension $2n$. Let $f \in k[X]$ be monic, separable and irreducible polynomial of degree d, and suppose that $f \neq f^*$. Set $m = \frac{n}{d}$. Then (V, q) has an isometry with minimal polynomial ff^* and characteristic polynomial $(ff^*)^m$.*

Proof. Let $A = k[X]/(ff^*)$, and let $\bar{\ } : A \to A$ be the involution induced by $X \mapsto X^{-1}$. Let us define a quadratic space $q_0 : A \times A \to k$ by setting $q_0(x, y) = \mathrm{Tr}_{A/k}(x\overline{y})$. This space is hyperbolic of dimension $2d$, and has an isometry of minimal (and characteristic) polynomial ff^* by construction. Note that the quadratic space q is isomorphic to the orthogonal sum of m copies of q_0, hence q has an isometry with minimal polynomial ff^* and characteristic polynomial $(ff^*)^m$.

Finally, we give a construction and a terminology that will be used repeatedly in the paper.

Let $F \in k[X]$ be a monic, symmetric polynomial such that $F(1) \neq 0$ and $F(-1) \neq 0$. Let $f_1, \dots, f_p \in k[X]$ be the distinct monic, irreductible and symmetric factors of F, and let $g_1, \dots, g_q$ be the monic, irreducible factors of F such that $g_i* \neq g_i$ for all $i = 1, \dots, q$. Set $f = f_1 \dots f_p g_1 g_1^* \dots g_q g_q^*$, and note that $F = f_1^{n_1} \dots f_r^{n_p} (g_1 g_1^*)^{m_1} \dots (g_q g_q^*)^{m_q}$ for some integers n_i, m_j.

Set $A = k[X]/(f)$, and let $\bar{\ } : K \to K$ be the involution induced by $X \mapsto X^{-1}$. We have $A = K_1 \times \dots \times K_r \times A_1 \times \dots \times A_s$, where $K_i = k[X]/(f_i)$ and $A_i = k[X]/(g_i g_i^*)$.

Then the K_i's and the A_i's are stable by the involution. The fields K_i will be called the *fields with involution associated to* F.

Set $V_i = K_i^{n_i}$ for $i = 1, \dots, p$. Let (V_0, q_0) be a hyperbolic quadratic space with minimal polynomial $g_1 g_1^* \dots g_s g_s^*$ and characteristic polynomial $(g_1 g_1^*)^{m_1} \dots (g_s g_s^*)^{m_s}$. This is possible by lemma 2.6. The vector spaces V_i will be called the *vector spaces associated to* F, and the (V_0, q_0) the *hyperbolic space associated to* F.

§3. The field of real numbers

In this section the ground field k is the field of real numbers $\mathbf{R}$. Let (V, q) be a quadratic space over $\mathbf{R}$. It is well–known that q is isomorphic to

$$X_1^2 + \dots + X_r^2 - X_{r+1}^2 - \dots - X_{r+s}^2$$

for some natural numbers r and s. These are uniquely determined by q, and we have $r + s = \dim(V)$. The couple (r, s) is called the *signature* of q.

Let $F \in \mathbf{R}[X]$ be a symmetric polynomial, and suppose that $F(1) \neq 0$ and $F(-1) \neq 0$. Let $\deg(F) = 2n$, and let 2σ be the number roots of F off the unit circle. The following result is proved by Gross and McMullen in [5], cor. 2.3, in the case where F is separable.

Proposition 3.1 *The quadratic space (V, q) has an isometry with characteristic polynomial F and separable minimal polynomial if and only if $r + s = 2n$, $(r, s) \geq (\sigma, \sigma)$, and $(r, s) \equiv (\sigma, \sigma) \pmod 2$.*

Proof. Suppose that q has an isometry with characteristic polynomial F and separable minimal polynomial. Let $f_1, \dots, f_p \in \mathbf{R}[X]$ be the distinct monic, irreducible and symmetric factors of F. We have $F = F_1 F_2$, where F_1 is a product of powers of the f_i's and F_2 is a product of non–symmetric polynomials. By definition, we have $\deg(F_2) = 2\sigma$.

By prop. 2.3, we have

$$(V, q) \simeq \bigoplus_{i=1,\dots,m} (V_{f_i}, q_{f_i}) \oplus H$$

with H hyperbolic of dimension 2σ. The signature of H is (σ, σ), so this implies that $(r, s) \geq (\sigma, \sigma)$.

By prop. 2.5, there exists a hermitian form (V_{f_i}, h_{f_i}) such that

$$q_{f_i}(x, y) = \mathrm{Tr}_{K/k}(h_{f_i}(x, y))$$

for all $x, y \in V_{f_i}$. Let (u_i, v_i) be the signature of h_{f_i}. Then the signature of q_{f_i} is $(2u_i, 2v_i)$. This implies that $(r, s) \equiv (\sigma, \sigma) \pmod 2$.

Conversely, suppose that $r + s = 2n$, $(r, s) \geq (\sigma, \sigma)$, and $(r, s) \equiv (\sigma, \sigma) \pmod 2$. Let K_i be the fields with involution, V_i the K_i–vector spaces, and (V_0, q_0) the hyperbolic quadratic space associated to F (cf. end of §2). Then $\dim_k(V_0) = 2\sigma$. Let $2u = r - \sigma$, and $2v = s - \sigma$. Note that $u + v = n - \sigma$. Let $u_i, v_i \in \mathbf{N}$ such that $0 \leq u_i, v_i \leq \dim_{K_i}(V_i)$ and that $u_1 + \ldots + u_p = u$ and $v_1 + \ldots + v_q = v$.

Let $h_i : V_i \times V_i \to K_i$ be the hermitian form of signature (u_i, v_i) over V_i, and let $q_{h_i} : V_i \times V_i \to k$ the quadratic space defined by $q_{h_i}(x, y) = \mathrm{Tr}_{K_i/k}(h_i(x, y))$ for all $x, y \in V_i$. Then the signature of q_{h_i} is $(2u_i, 2v_i)$. Let $W = V_0 \oplus V_1 \oplus \ldots \oplus V_p$, and let $q' : W \times W \to k$ be the orthogonal sum of $q_0, q_1, \ldots, q_p$. Then q' has an isometry with separable minimal polynomial and characteristic polynomial F by construction. The signature of q' is (r, s), hence $q' \simeq q$. This completes the proof of the proposition.

4. Local fields

Suppose that k is a local field, and let $F \in k[X]$ be a monic, symmetric polynomial. If F is hyperbolic, then we know from cor. 2.4 that only hyperbolic quadratic spaces admit isometries with characteristic polynomial F. Hence, from now on we suppose that F is *not hyperbolic*. Let q be a quadratic space.

Theorem 4.1 *The quadratic space q has an isometry with characteristic polynomial F and separable minimal polynomial if and only if* $\deg(F) = \dim(V)$*, and*

$$\det(q) = F(1)F(-1) \in k^*/k^{*2}.$$

The proof of th. 4.1 relies on the following result of Milnor. Let K be a separable extension of k of finite degree endowed with a non–trivial k–linear involution $^- : K \to K$. For any non–degenerate hermitian form $h : U \times U \to K$, let us denote by $q_h : U \times U \to k$ the quadratic space defined by $q_h(x, y) = \mathrm{Tr}_{K/k}(h(x, y))$ for all $x, y \in U$. We have

Theorem 4.2 *If the hermitian spaces h and h' have the same dimension but different determinants, then the quadratic spaces q_h and $q_{h'}$ have the same dimension and determinant but different Hasse invariants.*

Proof. See Milnor, [7], th. 2.7.

Proof of 4.1 The necessity of the condition follows from prop. 1.2. Conversely, suppose that $\dim(V) = \deg(F)$, and that $\det(q) = F(1)F(-1) \in k^*/k^{*2}$. Let K_i be the fields with involution and V_i the K_i–vector spaces associated to F (cf. §2). Let $h_i : V_i \times V_i \to K_i$ be the unit hermitian form over V_i, and let $q_{h_i} : V_i \times V_i \to k$ the quadratic space defined by $q_{h_i}(x, y) = \mathrm{Tr}_{K_i/k}(h_i(x, y))$ for all $x, y \in V_i$. Let (V_0, q_0) be the hyperbolic quadratic space associated to F. Let $W = V_0 \oplus V_1 \oplus \ldots \oplus V_p$, and let $q' : W \times W \to k$ be the orthogonal sum of $q_0, q_1, \ldots, q_p$. Then q' has an isometry with separable minimal polynomial and characteristic polynomial F by construction, and we have $\det(q') = F(1)F(-1)$. If the Hasse invariants of q and q' are equal, then we are finished. If not, let E_1 be the fixed field of the involution in K_1, and let $\alpha \in E_1^*$ be such that $\alpha \notin \mathrm{N}_{K_1/E_1}(K_1^*)$. Let h'_1 :

$V_1 \times V_1 \to K_1$ be a hermitian form over K_1 of determinant α, and let $q_{h'_1} : V_1 \times V_1 \to k$ the quadratic space defined by $q_{h'_1}(x,y) = \mathrm{Tr}_{K_1/k}(h'_1(x,y))$ for all $x, y \in V_1$.Then by th. 4.2 the quadratic spaces $q_{h'_1}$ and q_{h_1} have equal determinants but different Hasse invariants. Let $q'' : W \times W \to k$ be the orthogonal sum of q_0, q'_1, q_2, $\dots$, q_r. Then q'' has an isometry with separable minimal polynomial and characteristic polynomial F. Moreover, q and q'' have equal dimension, determinant and Hasse invariant, hence they are isomorphic. This completes the proof .

§5. Global fields

Suppose that k is a global field. The aim of this section is to give an answer to the question of Milnor quoted in the introduction in the case of global fields.

Let (V, q) be an quadratic space over k, and let $f \in k[X]$ be a monic, symmetric, irreducible polynomial. We have the following local-global principle :

Theorem 5.1 *The quadratic space q has an isometry with minimal polynomial f if and only if such an isometry exists over every completion of k.*

Note that a result of Prasad and Rapinchuk (cf. [9], 7.3) implies 5.1 in the case of an irreducible characteristic polynomial. Before proving th. 5.1, let us use the results of the previous two sections to obtain necessary and sufficient conditions for an isometry to exist. Let F be a power of f such that $\deg(F) = \dim(V) = 2n$.

For every real place v of k, let (r_v, s_v) denote the signature of q over k_v, and let σ_v be the number of roots of F that are not on the unit circle.

We say that the *signature condition* is satisfied for q and F if for every real place v of k, we have $(r_v, s_v) \geq (\sigma_v, \sigma_v)$, and $(r_v, s_v) \equiv (\sigma_v, \sigma_v) \pmod 2$.

We say that the *hyperbolicity condition* is satisfied for q and F if for all places v of k such that $F \in k_v[X]$ is a hyperbolic polynomial, the quadratic form q_v over k_v is hyperbolic.

Corollary 5.2 *The quadratic space q has an isometry with minimal polynomial f if and only if the signature condition and the hyperbolicity conditions are satisfied, and*

$$\det(q) = F(1)F(-1) \in k^*/k^{*2}.$$

Proof. The necessity of the conditions follows from prop. 3.1 and prop. 1.2. Conversely, suppose that the signature condition is satisfied and that $\det(q) = F(1)F(-1) \in k^*/k^{*2}$. Then by prop. 3.1 and th. 4.1, the quadratic space q has an isometry with minimal polynomial f over k_v for every place v of k. By th. 5.1, this implies that q has an isometry with minimal polynomial f.

The following reformulation of cor. 5.2 shows that it suffices to check a finite number of conditions. Let q and F be as above, with $\dim(q) = \deg(F) = 2n$. Let S be the set of places of k at which the Hasse–Witt invariant of q is not equal to the Hasse–Witt invariant of the $2n$ dimensional hyperbolic form. Note that S is a finite set.

Corollary 5.3 *The quadratic space q has an isometry with minimal polynomial f if and only if the following conditions are satisfied :*

(i) $F(1)F(-1) = \det(q) \in k^*/k^{*2}$;
(ii) The signature condition holds;
(iii) If $v \in S$, then $F \in k_v[X]$ is not hyperbolic.

Proof. It suffices to prove that the conditions (i) and (iii) imply the hyperbolicity condition. Let v be a place of k such that $F \in k_v[X]$ is hyperbolic. Then there exists a polynomial $G \in k_v[X]$ such that $F = GG^*$. Note that $\deg(G) = n$. We have $F(1) = G(1)^2$, and $F(-1) = (-1)^n G(-1)$. By condition (i), we have $F(1)F(-1) = \det(q)$, hence $(-1)^n \det(q) = \mathrm{disc}(q) \in k_v^2$. On the other hand, condition (iii) implies that $v \notin S$. Therefore over k_v, the quadratic space q has the same dimension, discriminant and Hasse–Witt invariant as the $2n$–dimensional hyperbolic form. Hence q is hyperbolic over k_v, in other words the hyperbolicity condition is satisfied.

The following will be used in the proof of th. 5.1. Let $f \in k[X]$ be an irreducible, symmetric polynomial, and let $K = k[X]/(f)$. Let $^- : K \to K$ be the k–linear involution induced by $X \mapsto X^{-1}$, and let E be the fixed field of this involution. Let (W, Q) be a quadratic space over k.

Lemma 5.4 *Let v be a finite place of k such that every place of E above v splits in K. Suppose that over k_v the quadratic space Q has an isometry with minimal polynomial f. Then Q is hyperbolic over k_v.*

Proof. Let $w_1, \dots, w_r$ be the places of E above v. Then $k_v[X]/(f) \simeq K_1 \times \dots \times K_r$, where K_i is a field if w_i is inert or ramified in K and a product of two fields if w_i is split in K. Here we are supposing that every w_i splits in K, hence all the K_i's are products of two fields. This implies that $f = f_1 f_1^* \dots f_r f_r^*$ with $f_i \in k_v[X]$ monic and irreducible and $f_i \neq f_i^*$ for all $i = 1, \dots, r$. By prop. 2.4, the quadratic space Q is hyperbolic over k_v.

Proof of th. 5.1 Let $F = f^m$ and $\deg(f) = 2d$. Let $K = k[X]/(f)$, and let $^- : K \to K$ be the involution induced by $X \mapsto X^{-1}$. Let E be the fixed field of the involution. Let $\theta \in E^*$ such that $K = E(\sqrt{\theta})$, and for any place w of E, let $(\ , \ )_w$ denote the Hilbert symbol at E_w.

Let v be a real place of k. Then the signature (r_v, s_v) of q at k_v satisfies $(r_v, s_v) \geq (\sigma_v, \sigma_v)$ and $(r_v, s_v) \equiv (\sigma_v, \sigma_v) \pmod 2$. In particular, $s_v - \sigma_v$ is even. Set $s_v - \sigma_v = 2u_v$, and note that $0 \leq u_v \leq n - \sigma_v$. Let us denote by $2\tau_v$ the number of roots of f that are not on the unit circle. Then we have $\sigma_v = m\tau_v$. Let us write $u_v = u_v^1 + \ldots + u_v^m$ for some integers u_v^i such that $0 \leq u_v^i \leq d - \tau_v$.

Let $w_1, \ldots, w_{d-\tau_v}$ be the real places of E above v that extend to a complex place of K. Let $\alpha_i \in E^*$ such that $(\alpha_i, \theta)_{w_j} = -1$ if $j = 1, \ldots u_i$, and that $(\alpha_i, \theta)_{w_j} = 1$ if $j = u_i + 1, \ldots, d - \tau_i$.

Let $h' : V \times V \to K$ be the hermitian form defined by $h' =< \alpha_1, \ldots, \alpha_m >$ and let let $q_{h'} : V \times V \to k$ be the quadratic space defined by $q_{h'}(x, y) = \mathrm{Tr}_{K/k}(h'(x, y))$ for all $x, y \in V$. By construction, the signature at v of $q_{h'}$ is (r_v, s_v).

Let T be the set of finite places of k such that every place of E above v splits in K. The local conditions imply that q has an isometry of minimal polynomial f over every completion of k. By lemma 5.4 this implies that if $v \in T$, then q is hyperbolic over k_v.

Let S be the set of finite places of k at which the Hasse invariants of q and $q_{h'}$ are not equal. This is a finite set of even cardinality. Note that the quadratic space $q_{h'}$ has an isometry of minimal polynomial f by construction, therefore lemma 5.4 implies that $q_{h'}$ is hyperbolic over k_v if $v \in T$. This implies T and S are disjoint.

For each $v \in S$, let us choose a place w of E which does not split in K; this is possible because S and T are disjoint. Let us denote by S_E the set of these places. Then S_E is a finite set of even cardinality.

For all $w \in S_E$, let $\beta_w \in E_w^*$ such that $(\beta_w, \theta)_w = -1$; note that such an β_w exists as w is does not split in K. By Hilbert reciprocity, there exists $\beta \in E^*$ such that $(\beta, \theta)_w = (\beta_w, \theta)_w = -1$ if $w \in S_E$, and that $(\beta_w, \theta)_w = 1$ for all the other places w of E. Let $h : V \times V \to K$ be the hermitian form defined by $h =< \beta\alpha_1, \ldots, \alpha_d >$ and let $q_h : V \times V \to k$ be the quadratic space defined by $q_h(x, y) = \mathrm{Tr}_{K/k}(h(x, y))$ for all $x, y \in V$. Then by th. 4.2, the Hasse invariants of q_h and q are equal. This implies that q and of q_h have equal dimension, determinant, signatures and Hasse invariants, therefore these quadratic spaces are isomorphic. Note that q_h has an isometry with minimal polynomial f by construction, hence q also has such an isometry, and this concludes the proof of the theorem.

§6. Isometries of even, unimodular lattices

An *integral lattice* is a pair (L, q_0), where L is a free **Z**–module of finite rank, and $q : L \times L \to \mathbf{Z}$ is a symmetric bilinear form. We say that the lattice q_0 is *unimodular* if $\det(q_0) = \pm 1$, and *even* if $q_0(x, x) \equiv 0 \pmod 2$ for all $x \in L$. Which polynomials $F \in \mathbf{Z}[X]$ can be realized as isometries of even, unimodular lattices ? This question was raised in [1], [2], [3], as well as in the paper of Gross and McMullen [5]. More precisely, Gross and McMullen [5] concentrate on the case of irreducible characteristic polynomials and indefinite lattices (see also [4]), and the case where F is a power of an irreducible polynomial and the lattice is definite is handled in [1].

Let (L, q_0) be an even, unimodular lattice, let $V = L \otimes_{\mathbf{Z}} \mathbf{Q}$, and let $q : V \times V \to \mathbf{Q}$ be the extension of q_0 to $\mathbf{Q}$. Let $f \in \mathbf{Z}[X]$ be an irreducible polynomial, let $F = f^m$ and suppose that $\deg(F) = \dim(V) = 2n$. The results of §5 imply the following :

Theorem 6.1 *The quadratic space q has an isometry with minimal polynomial f if and only if the signature condition is satisfied, and*

$$F(1)F(-1) = (-1)^n \in \mathbf{Q}^*/\mathbf{Q}^{*2}.$$

Proof. This is a consequence of cor. 5.3. Indeed, it is well–known that the signature of an even, unimodular lattice is divisible by 8. This implies that q_0 is an orthogonal sum of a definite form of rank divisible by 8 with a certain number of hyperbolic planes. The number of these planes is congruent to n modulo 2, hence $\det(q_0) = (-1)^n$. Therefore the conditions of the theorem are necessary. On the other hand, as q_0 is an orthogonal sum of a definite form of rank divisible by 8 and of a hyperbolic form, the Hasse–Witt invariant of q coincides with the Hasse–Witt invariant of the $2n$–dimensional hyperbolic form. Therefore the set S of cor. 5.3 is empty. This shows that the conditions are also sufficient, hence the theorem is proved.

Bibliography

[1] E. Bayer–Fluckiger, Definite unimodular lattices having an automorphism of given characteristic polynomial. *Comment. Math. Helv.* **59** (1984), 509–538.

[2] E. Bayer–Fluckiger, Réseaux unimodulaires. *Sém. Théor. Nombres Bordeaux* (1989) **1**, 189–196.

[3] E. Bayer–Fluckiger, Lattices and number fields. Algebraic geometry: Hirzebruch 70 (Warsaw, 1998), 69–84, *Contemp. Math.* **241**, Amer. Math. Soc., Providence, RI, 1999.

[4] E. Bayer–Fluckiger, Determinants of integral ideal lattices and automorphisms of given characteristic polynomial. *J. Algebra* **257** (2002), no. 2, 215–221.

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

[6] J. Levine, Invariants of knot cobordism. *Invent. Math* **8** (1969), 98–110.

[7] J. Milnor, Isometries of inner product spaces, *Invent. Math.* **8** (1969), 83–97.

[8] O.T. O'Meara, *Introduction to quadratic forms*, reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[9] G. Prasad and A.S. Rapinchuk, Local–global principles for embedding of fields with involution into simple algebras with involution, *Comment. Math. Helv.* **85** (2010), 583–645.

[10] W. Scharlau, *Quadratic and hermitian forms*, Grundlehren der Mathematischen Wissenschaften **270**, Springer-Verlag, Berlin, 1985.