On the norm principle for quadratic forms

M.Ojanguren, I.Panin, K.Zainoulline

September 6, 2004

Abstract

We prove a version of Knebusch's Norm Principle for finite étale extensions of semi-local Noetherian domains with infinite residue fields of characteristic different from 2. As an application we prove Grothendieck's conjecture on principal homogeneous spaces for the spinor group of a quadratic space.

Keywords: quadratic space, spinor group, local ring
MSC: 20G35, 13H05

1 Introduction

Let E/F be a finite field extension and $q : V \to F$ a quadratic space over F. Let $D_q(F) \subset F^*$ (resp. $D_q(E)$) be the subgroup generated by the set of non-zero elements of the field F (resp. E) represented by the form q (resp. $q_E = q \otimes_F E$). The well-known Knebusch's Norm Principle for quadratic forms over fields [5], [4, VII.5.1] says that $N_F^E(D_q(E)) \subset D_q(F)$, where $N_F^E : E^* \to F^*$ is the norm map. The goal of the present article is to show that the Knebusch's Norm Principle holds for finite étale extensions of semi-local Noetherian domains with infinite residue fields of characteristic different from 2 (see Theorem 3.2). Previously, the Norm Principle for quadratic spaces over semi-local rings was proved for F of characteristic 0 in [9]. As an application we prove Grothendieck's conjecture on principal homogeneous spaces for the spinor group of a quadratic space (see Theorem 4.1).

This article is organized as follows. Section 2 is devoted to some preliminary results. In Section 3 we prove the Norm Principle for quadratic spaces over local rings. Finally, we prove Grothendieck's conjecture (Sect. 4).

Acknowledgments The second author thanks very much for the support the RTN-Network HPRN-CT-2002-00287, the grant of the years 2001 to 2003 of the "Support Fund of National Science" at the Russian Academy of Science, the RFFI-grant 03-01-00633a and the Swiss National Science Foundation. The last author is also grateful to SFB478, Münster and AvH Foundation for hospitality and support.

2 Preliminary Lemmas

In the present section we state and prove few auxiliary results which are the main tools in the proof of Theorem 3.2.

2.1. Let F be an infinite field of characteristic different from 2. Let E be a finite étale F-algebra of degree n. Let (V, q) be a quadratic space over F of rank m. Let (V_E, q_E) be the base change of (V, q) via the extension E/F, i.e., $V_E = V \otimes_F E$ and $q_E = q \otimes_F E$. Sometimes we identify the vector space V_E with the set $\mathbb{A}^m_E(E)$ of E-points of the affine space $\mathbb{A}^m_E$.

2.2. Since E is étale over F, there exists an element $\alpha \in E^*$ such that the powers $1, \alpha, \ldots, \alpha^{n-1}$ form a basis of the F-vector space E. Such an element is called *primitive*. In other words, E can be written as the quotient $F[t]/(f_\alpha(t))$ of the polynomial ring $F[t]$ modulo the ideal generated by a monic separable polynomial $f_\alpha(t)$ of degree n. In this case α is identified with the image of t by means of the quotient map $F[t] \to F[t]/(f_\alpha(t))$. The polynomial $f_\alpha(t)$ is called a *minimal polynomial* of α.

2.3. Observe that the subset of primitive elements of E is big enough in the following sense: Let $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ with $b_0, \ldots, b_{n-1} \in F$ be an element of E. Then, for every integer i with $0 \le i \le n-1$,

$$\beta^i = b_0^{(i)} + b_1^{(i)}\alpha + \cdots + b_{n-1}^{(i)}\alpha^{n-1}, \text{ with } b_j^{(i)} \in F.$$

Clearly, each $b_j^{(i)}$ is a polynomial in $b_0, \ldots, b_{n-1}$. The condition that β be primitive is the non-vanishing of the determinant of $\big(b_j^{(i)}\big)$ and can, thus, be expressed by the non-vanishing of a polynomial $d(b_0, \ldots, b_{n-1})$. We define an open subset P of the Weil restriction $R_{E/F}(\mathbb{G}_{m,E})$ of the multiplicative group $\mathbb{G}_{m,E}$ by

$$P = \{(b_0, \ldots, b_{n-1}) \mid d(b_0, \ldots, b_{n-1}) \neq 0\}\ .$$

By definition, the set $P(F)$ of the F-points of P is the subset of primitive invertible elements of E.

2.4 Lemma. *Let X be an F-rational variety. Then any non-empty open subset U of X has a rational point.*

Proof. The proof follows from the fact that F is infinite. □

From this point onwards we will use the following notations and terminology.

2.5. *Assume there is given an element $\alpha \in P(E)$ and a vector $v \in V_E$ such that $\alpha q(v) = 1$. Denote by $f_\alpha(t) \in F[t]$ the minimal polynomial of α.*

2.6. Let Q be the quadric over E given by

$$Q = \{\omega \in \mathbb{A}_E^m \mid \alpha q(\omega) = 1\}.$$

Since the element v is an E-point of Q, the variety Q is E-rational. Set $Y = R_{E/F}(Q)$ to be the Weil restriction of Q (see [2]). The variety Y is a closed subvariety of dimension $(m-1)n$ of the affine space $R_{E/F}(\mathbb{A}_E^m) = \mathbb{A}_F^{nm}$ and we have the bijection $Y(F) = Q(E)$ between the sets of F-points of Y and E-points of Q. Since Q is rational over E, Y is rational over F.

2.7. In order to define the next variety U we identify $R_{E/F}(\mathbb{A}_E^m)$ with the affine space $M_{n,m}$ of $n \times m$-matrices over F by choosing $\{1, \alpha, \ldots, \alpha^{n-1}\}$ as a basis of the vector space E over F. Thus, a vector $\omega = (\omega_0, \ldots, \omega_{m-1}) \in R_{E/F}(\mathbb{A}_E^m)(F)$ corresponds to the matrix $(\omega_{i,j})_{i,j=0}^{n-1,m-1}$, where the entries $\omega_{i,j} \in F$ are defined by $\omega_j = \sum_{i=0}^{n-1} \omega_{i,j}\alpha^i$. For any $\omega = (\omega_=, \ldots, \omega_{n-1})$ we define $\omega(t) = (\omega_0(t), \ldots, \omega_{m-1}(t))$, where $\omega_j(t) = \sum_{i=0}^{n-1} \omega_{i,j} t^i$. Note that each $\omega_j(t)$ is of degree at most $n-1$. We define U to be the open subset of the affine space $R_{E/F}(\mathbb{A}_E^m)$ defined by

$$U = \{\omega \in M_{n,m} \mid \Phi_\omega(t) = tq(\omega(t)) - 1 \text{ is separable of degree } 2n-1\}.$$

Clearly, the coefficients of the polynomial $\Phi_\omega(t) \in F[t]$ depend on the choice of the isomorphism $R_{E/F}(\mathbb{A}_E^m) \cong M_{n,m}$, i.e., they depend on the choice of α.

2.8 Lemma. *The open subset $U \cap Y$ of Y contains an F-point.*

Proof. Since Y is F-rational and $U \cap Y$ is open in Y, by Lemma 2.4 it is enough to show that $U \cap Y$ contains a point ρ over the algebraic closure $\bar{F}$ of the field F. Let $g(t)$ be a polynomial over F such that

1. $\deg g(t) = n - 1$
2. $g(t)$ is coprime with the polynomial $f_\alpha(t)$
3. $-g(0)f_\alpha(0) = 1$
4. $g(t)$ is separable

Choose a hyperbolic plane $\mathbb{H}$ in the quadratic space $(V_{\bar F}, q_{\bar F})$ over $\bar F$. Choose a basis $\{e_1, e_2\}$ of $\mathbb{H}$ such that $q(e_1) = q(e_2) = 0$ and $q(e_1 + e_2) = 1$. Let $g_1(t)$, $g_2(t)$ be polynomials over $\bar F$ of degree $n - 1$ such that

$$tg_1(t)g_2(t) = g(t)f_\alpha(t) + 1.$$

Set $\rho(t) = g_1(t)e_1 + g_2(t)e_2$ to be a vector of polynomials over $\bar F$ which can be identified with an $\bar F$-point of $R_{E/F}(\mathbb{A}^m_E)$ following 2.7. Then we have

$$tq(\rho(t)) = t(q(e_1)g_1(t)^2 + q(e_1 + e_2)g_1(t)g_2(t) + q(e_2)g_2(t)^2) =$$

$$= tg_1(t)g_2(t) = g(t)f_\alpha(t) + 1$$

and

- $\alpha q(\rho(\alpha)) = g(\alpha)f_\alpha(\alpha) + 1 = 1$
- $\Phi_\rho(t) = tq(\rho(t)) - 1 = g(t)f_\alpha(t)$ is separable of degree $2n - 1$.

Hence $\rho \in (U \cap Y)(\bar F)$ is the desired point. □

2.9. Define one more open subset of Y. For that consider a closed subset $Z \subset \mathbb{A}^m_E$ defined by

$$Z = \{\omega \in \mathbb{A}^m_E \mid \langle v, \omega\rangle - 1 \in \{0\}_E\},$$

where $\langle\, ,\, \rangle : V_E \times V_E \to E$ is the bilinear form associated with the quadratic form αq_E and $\{0\}_E$ the image of the zero section $\operatorname{Spec} E \to \mathbb{A}^m_E$ of $\mathbb{A}^m_E$. Set $W = R_{E/F}(Q \setminus Z)$. Passing to the algebraic closure $\bar F$ we see that W is a non-empty open subset of $Y = R_{E/F}(Q)$. The set $W(F)$ of F-points of W consists of all $w \in Q(E)$ satisfying the condition $\langle v, \omega\rangle - 1 \in E^*$.

2.10 Lemma. *There exists $\omega' \in V_E$ such that*

(i) $\alpha q(\omega') = 1$

(ii) $\langle v, \omega' \rangle - 1 \in E^*$

(iii) *the polynomial* $\Phi_{\omega'}(t)$ *is separable of degree* $2n-1$.

Proof. By Lemma 2.8 the set $U \cap Y$ is non-empty open in Y. The set W defined in 2.9 is also non-empty open in Y. Since the variety Y is irreducible, the set $W \cap U \cap Y$ is non-empty open in Y. Since Y is F-rational, the set $W \cap U \cap Y$ contains an F-point. Recall that $Y(F) = Q(E) \subset V_E$. Let $\omega' \in (W \cap U \cap Y)(F) \subset V_E$. We claim that ω' satisfies (i) to (iii). In fact, property (i) holds because $\omega' \in Q(E)$, property (ii) holds because $\omega' \in W(F) = (Q \setminus Z)(E)$ and property (iii) holds because $\omega' \in U(F)$. $\square$

3 The Norm Principle

3.1. Let R be a semi-local Noetherian domain with infinite residue fields of characteristic different from 2 (in this case $\frac{1}{2} \in R$). Let S/R be a finite étale R-algebra (not necessarily a domain). Let (V, q) be a quadratic space of rank m over R. Let (V_S, q_S) be the base change of (V, q) via the extension S/R. Let $D_q(R)$ (resp. $D_q(S)$) be the group generated by the invertible elements of R (resp. S) represented by the form q.

The goal of the present section is to prove the following

3.2 Theorem. *There is an inclusion of the subgroups of* R^*

$$N_R^S(D_q(S)) \subset D_q(R),$$

where $N_R^S : S^* \to R^*$ *is the norm map for the finite étale extension* S/R.

3.3. For simplicity we will consider only the case of local R. By a variety over R we will mean a reduced separated scheme of finite type over $\operatorname{Spec} R$. From this point onwards, by "bar" we mean the reduction modulo the maximal ideal $\mathfrak{m}$ of R. So that $\overline{S} = S/\mathfrak{m}S$. We will write F for $\overline{R}$ and E for $\overline{S}$. So E/F is a finite étale algebra.

To prove Theorem 3.2 we need the following auxiliary results.

3.4 Lemma. *Let* (S^m, ϕ) *be a quadratic space over* S *and let* $\langle\, ,\, \rangle : S^m \times S^m \to S$ *be the associated bilinear form. Let* $v \in S^m$ *be such that* $\phi(v) = 1$. *Let* $\omega' \in E^m$ *be such that* $\overline{\phi}(\omega') = \bar{1}$ *and* $\langle \overline{v}, \omega' \rangle - \bar{1} \in E^*$ *(a unit). Then there exists* $\omega \in S^m$ *satisfying the conditions*

(i) $\phi(\omega) = 1$

(ii) $\overline{\omega} = \omega'$ *in* E^m.

Proof. If $\tilde{\omega}$ is a lift of ω' we have $\phi(\tilde{\omega}) = 1 + h$ and $\langle v, \tilde{\omega} \rangle - 1 = u$ with $h \in \mathfrak{m}$ and $u \in R^*$. Putting

$$\omega = \frac{\lambda v + \tilde{\omega}}{\lambda + 1}$$

we find

$$\phi(\omega) = \frac{\lambda^2 + 2\lambda(1 + u) + 1 + h}{(\lambda + 1)^2} .$$

Thus, for $\lambda = -h/2u$ we have $\phi(\omega) = 1$ and since $h \in \mathfrak{m}$, ω is a lift of ω'. □

3.5. Recall that a polynomial $f(t) \in R[t]$ is said to be separable if the quotient ring $R[t]/(f(t))$ is a finite étale extension of R. Since R is local, a polynomial f is separable iff its reduction $\overline{f}$ modulo the maximal ideal $\mathfrak{m}$ is a separable polynomial over $\overline{R}$.

3.6. Similar to 2.2, since, S being étale over R, there exists an element $\alpha \in S^*$ such that the powers $1, \alpha, \ldots, \alpha^{n-1}$ form a basis of the free R-module S. As in the case of fields such an element is called *primitive*. In other words, S can be written as a quotient $R[t]/(f_\alpha(t))$ of the polynomial ring $R[t]$, where $f_\alpha(t)$ is a monic separable polynomial called the *minimal polynomial* for α. In this case α is identified with the image of t by means of the quotient map $R[t] \to R[t]/(f_\alpha(t))$.

3.7. As in 2.3 consider a primitive element α of the extension S/R. An element $\beta \in S^*$ can be written as $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ in S^* with $b_0, \ldots, b_{n-1} \in R$. Then, for every integer i with $0 \leq i \leq n - 1$,

$$\beta^i = b_0^{(i)} + b_1^{(i)}\alpha + \cdots + b_{n-1}^{(i)}\alpha^{n-1} \text{ with } b_j^{(i)} \in R.$$

Clearly, each $b_j^{(i)}$ is a polynomial in $b_0, \ldots, b_{n-1}$. The condition that β be primitive is the non-vanishing of the determinant of $\left(b_j^{(i)}\right)$ and can thus be expressed by the non-vanishing of a polynomial $d(b_0, \ldots, b_{n-1})$. We define an open subset P of $R_{S/R}(\mathbb{G}_{m,S})$ by

$$P = \{(b_0, \ldots, b_{n-1}) \mid d(b_0, \ldots, b_{n-1}) \in R^*\} .$$

Observe that $P(R)$ is the set of primitive invertible elements of S.

3.8. Following 2.7, for a given primitive element α and any vector $\omega \in V_S$ we define the polynomial $\Phi_\omega(t) \in R[t]$ as follows. We identify the free S-module V_S with the set of matrices $M_{n,m}(R)$ using $\{1, \alpha, \dots, \alpha^{n-1}\}$ as a basis of S over R. Thus, a vector $\omega = (\omega_0, \dots, \omega_{m-1}) \in V_S$ corresponds to the matrix $(\omega_{i,j})_{i,j=0}^{n-1,m-1}$, where the entries $\omega_{i,j} \in R$ are defined by $\omega_j = \sum_{i=0}^{n-1} \omega_{i,j}\alpha^i$. We set

$$\Phi_\omega(t) = tq(\omega(t)) - 1 \in R[t],$$

where $\omega(t) = (\omega_0(t), \dots, \omega_{m-1}(t))$ is the vector of m polynomials $\omega_j(t) = \sum_{i=0}^{n-1} \omega_{i,j}t^i$ of degree at most $n-1$. Clearly, the coefficients of the polynomial $\Phi_\omega(t)$ depend on the choice of α.

3.9 Lemma. *Let $\alpha \in S$ be a primitive invertible element of the finite étale extension S/R. Consider the quadratic space $(V_S, \alpha q_S)$ over S. Assume $\alpha q(v) = 1$ for a vector $v \in V_S$. Then there exists an $\omega \in V_S$ such that*

(i) $\alpha q(\omega) = 1$;

(ii) *the polynomial $\Phi_\omega(t)$ (defined in 3.8) is separable of degree $2n - 1$.*

Proof. According to our notation we write V_F for $V/\mathfrak{m}V$ and V_E for $V_S/\mathfrak{m}V_S$. The element $\overline{\alpha} \in E$ is a primitive element of E/F. It satisfies the relation $\overline{\alpha q}(\overline{v}) = \bar{1}$ for the vector $\overline{v} \in V_E$. By Lemma 2.10 applied to $\overline{\alpha}$ and $\overline{v}$ there exists $\omega' \in V_E$ satisfying the conditions $\overline{\alpha q}(\omega') = \bar{1}$ and $\langle \overline{v}, \omega' \rangle - \bar{1} \in E^*$, where $\langle \, , \rangle : V_E \times V_E \to E$ is the bilinear form associated with $\overline{\alpha q}$.

Now apply Lemma 3.4 to the quadratic space $(V_S, \alpha q_S)$ and the vectors $v \in V_S$, $\omega' \in V_E$. We find a vector $\omega \in V_S$ such that

(i) $\alpha q(\omega) = 1$ in S;

(ii) $\overline{\omega} = \omega'$ in V_E.

Property (ii) implies that the reduction modulo $\mathfrak{m}$ of the polynomial $\Phi_\omega(t) \in R[t]$ coincides with the polynomial $\Phi_{\omega'}(t) \in F[t]$. The polynomial $\Phi_{\omega'}(t)$ is separable of degree $2n-1$ by property (iii) of 2.10. Hence, $\Phi_\omega(t)$ is separable of degree $2n - 1$ (see 3.5). □

3.10 Lemma. *Let (V, q) be a quadratic space over R. Then the group of squares $(R^*)^2$ is contained in $D_q(R)$. In particular, $a \in D_q(R)$ if and only if $a^{-1} \in D_q(R)$.*

Proof. For any $b \in S^*$ and $q(u) \in R^*$ we have $b^2 = q(ub)/q(u) \in D_q(R)$. □

3.11 Proposition. *Let $\alpha \in S$ be a primitive invertible element of the finite étale extension S/R. In particular, the ring S can be written as $S = R[t]/(f_\alpha(t))$, where $f_\alpha(t)$ is the minimal polynomial of α. Assume $\alpha q(v) = 1$ for a vector $v \in V_S$. Then $N_R^S(q(v)) \in D_q(R)$.*

Proof. By Lemma 3.9 there exists $\omega \in V_S$ such that

(i) $\alpha q(\omega) = 1$;

(ii) the polynomial $\Phi_\omega(t)$ is separable of degree $2n-1$.

We have $\Phi_\omega(\alpha) = \alpha q(\omega) - 1 = 0$. This implies $\Phi_\omega(t) = c \cdot h(t) f_\alpha(t)$, where $c \in R^*$ and $h(t)$ is some monic polynomial of degree $n-1$. The polynomial $h(t)$ is separable, since $\Phi_\omega(t)$ is separable. Clearly, we have the relation

$$1 + c \cdot h(t) f_\alpha(t) = tq(\omega(t)). \tag{1}$$

The proof proceeds by the induction on degree of the extension S/R. The case $n = 1$ is obvious. Assume that the proposition holds for all finite étale extensions of degree strictly less than n.

Consider the finite étale extension $T = R[t]/(h(t))$ over R, where $h(t)$ is the polynomial appearing in (1). Observe that the degree of T/R is $n-1$. Let β be the image of t under the quotient map $R[t] \to R[t]/(h(t))$. Observe that β is a primitive element of the R-algebra T with the minimal polynomial $h(t)$.

Consider the reduction modulo the ideal $(h(t))$ of the relation (1). We get $1 = \beta q(u)$ in T for some $u \in V_T$. By Lemma 3.10 we get $\beta \in D_q(T)$. Substituting $t = 0$ in (1) we get $f_\alpha(0) = -1/(c \cdot h(0))$. Together with the fact that for the extension $S = R[t]/(f_\alpha(t))$ over R, $N_R^S(\alpha) = (-1)^{\deg(S/R)} f_\alpha(0)$, this implies the following chain of relations in R:

$$N_R^S(q(v)) = 1/N_R^S(\alpha) = (-1)^n/f_\alpha(0) = c \cdot (-1)^{n-1} h(0) = c \cdot N_R^T(\beta).$$

Since c is the leading coefficient of the polynomial $tq(\omega(t))$ of degree $2n-1$, it is represented by the form q. Namely, $c = q(\omega_{n-1,0}, \ldots, \omega_{n-1,m-1})$, where $\omega_{n-1,j} \in R$ are the leading coefficients of polynomials $\omega_j(t)$. By the induction hypothesis the norm $N_R^T(\beta)$ lies in $D_q(R)$. Hence $N_R^S(q(v)) \in D_q(R)$. This completes the proof of Proposition 3.11 □

3.12 Lemma. *Consider the multiplicative group $\mathbb{G}_{m,S}$ over the semi-local scheme* $\operatorname{Spec} S$. *Let W be an open subset of $\mathbb{G}_{m,S}$ such that for each closed point $x \in \operatorname{Spec} S$ the fiber W_x over x is non-empty. Then there exists $b \in S^*$ such that $b^2 \in W(S)$.*

Proof. For each closed point x of $\operatorname{Spec} S$ there is an element a_x in the residue field of x such that $a_x^2 \in W_x$. Since S is semi-local there is an element $b \in S^*$ such that $b_x = a_x$ in the residue field of x, for each x. Clearly, $b^2 \in W(S)$. □

Proof of Theorem 3.2. Let $a = q(u) \in S^*$ for certain $u \in V_S$. Consider the non-empty open subset P of $R_{S/R}(\mathbb{G}_{m,S})$ defined in 3.7. Clearly, each closed fiber of aP over $\operatorname{Spec} S$ is non-empty. By Lemma 3.12 there exists an element $b \in S^*$ such that $b^2 \in aP(S)$. It means that $\alpha = a^{-1}b^2$ is in $P(S)$, i.e., primitive. Replacing a by α and u by $v = u \cdot b^{-1}$, we get $\alpha q(v) = 1$. Then, by Lemma 3.10 and Proposition 3.11, we get the desired inclusion $N_R^S(a) = N_R^S(q(v)) \cdot N_R^S(b)^2 \in D_q(R)$. □

3.13. As before let R be a semi-local Noetherian domain with infinite residue fields of characteristic different from 2. Let S/R be a finite étale R-algebra of degree n. Let (V, q) be a quadratic space over R of rank m. By $D_q^0(S)$ (resp. $D_q^1(S)$) we denote the set of all even (resp. odd) products of invertible elements of S represented by q_S, i.e.,

$$D_q^i(S) = \{\prod_{j=0}^{l} q(v_j) \mid v_j \in S^m,\ q(v_j) \in S^*,\ l \equiv i \bmod 2\}, \quad i = 0, 1.$$

Observe that $D_q^0(S)$ is a subgroup of the group $D_q(S)$ and $(S^*)^2 \subset D_q^0(S)$. Clearly, if $c \in D_q^i(S)$, $i = 0, 1$, and $b \in D_q^0(S)$, then $cb \in D_q^i(S)$. The following result is an obvious consequence of the proof of Theorem 3.2.

3.14 Theorem. *Let $N_R^S : S^* \to R^*$ be the norm map. Then*

$$N_R^S(D_q^0(S)) \subset D_q^0(R),$$

Proof. For a positive integer n we set $D_q^n(S) = D_q^0(S)$ if n is even and $D_q^n(S) = D_q^1(S)$ if n is odd. By the proof of Proposition 3.11 and Theorem 3.2 it follows that $N_R^S(a) \in D_q^n(R)$, where a is an element represented by q_S and S/R is an extension of degree n. □

4 Grothendieck's conjecture for the spinor group

Let R be a local domain with residue field of characteristic different from 2 and q be a quadratic space over R. Following [6, IV.6] we define the spinor group (scheme) $Spin_q$ to be $Spin_q(R) = \{x \in S\Gamma_q(R) \mid x\sigma(x) = 1\}$, where σ is the canonical involution, $S\Gamma_q(R) = \{c \in C_0(V,q)^* \mid cVc^{-1} \subset V\}$ is the special Clifford group and $C_0(V,q)$ is the even part of the Clifford algebra of the respective quadratic space (V,q) over R. The present section is devoted to the proof of the following result:

4.1 Theorem. *Let R be a local regular ring containing an infinite field of characteristic different from 2. Let K be its quotient field. Let q be a quadratic space over R. Then the induced map on the sets of principal homogeneous spaces*

$$H^1_{et}(R, Spin_q) \to H^1_{et}(K, Spin_q)$$

has trivial kernel, where $Spin_q$ is the spinor group for the quadratic space q.

4.2. Observe that the theorem is a particular case of Grothendieck's conjecture on principal homogeneous spaces [3], which states that, for a smooth reductive group scheme G over R, the induced map $H^1_{et}(R,G) \to H^1_{et}(K,G)$ has trivial kernel.

Proof. The proof is based on the results of [7], [10] and [11].

Assume R is a local regular ring containing a field of characteristic different from 2. Let K be its quotient field. We have the following commutative diagram (see [6, IV.8.2.7]):

$$\begin{array}{ccccccc} SO_q(R) & \xrightarrow{SN} & R^*/(R^*)^2 & \longrightarrow & H^1_{et}(R, Spin_q) & \longrightarrow & H^1_{et}(R, SO_q) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ SO_q(K) & \xrightarrow{SN} & K^*/(K^*)^2 & \longrightarrow & H^1_{et}(K, Spin_q) & \longrightarrow & H^1_{et}(K, SO_q), \end{array}$$

where $SN : SO_q(R) \to H^1_{et}(R, \mu_2) = R^*/(R^*)^2$ is the spinor norm. The main result of [7] says that the vertical arrow on the right hand side has trivial kernel (see also [10, 3.4]). Thus, in order to show that the middle one has trivial kernel, it is enough to check that the induced map on the cokernels $coker(SN)(R) \to coker(SN)(K)$ is injective. First, we prove the geometric case. To do that we use the following slight modification of the main result of section 2 of [10].

4.3 Proposition. *Let R be a local regular ring of geometric type over an infinite field. Let F be a presheaf from the category of affine schemes over R to abelian groups. Assume F satisfies the axioms* C, E *of [10] and the weak versions of the axioms* TE, TA, TB *of [10] (see 4.4). Then the canonical map $F(R) \to F(K)$ is injective.*

4.4. The weak versions of the axioms TE, TA and TB state

- For a finite étale R-algebra T (instead of finitely generated projective considered in [10]) there is given a transfer map $Tr_R^T : F(T) \to F(R)$.
- This transfer map is additive in the sense of TA of [10].
- For a finitely generated projective $R[t]$-algebra S such that the algebras $S/(t)$ and $S/(t-1)$ are finite étale over R there is the commutative diagram of the axiom TB of [10]

$$\begin{array}{ccc} F(S) & \longrightarrow & F(S/(t)) \\ \downarrow & & \downarrow{\scriptstyle Tr} \\ F(S/(t-1)) & \xrightarrow{Tr} & F(R) \end{array}$$

The proof of 4.3 follows immediately after one replaces the Geometric Presentation Lemma [8, 10.1] used in section 1.1 of [10] by its stronger (étale) version

4.5 Lemma (Étale Geometric Presentation Lemma). *Let R be a local essentially smooth algebra over an infinite field k, m its maximal ideal and S an essentially smooth k-algebra which is an integral domain and finite over the polynomial algebra $R[t']$. Suppose that $e : S \to R$ is an R-augmentation and let $I = \ker e$. Assume that S/mS is smooth over the residue field R/m at the maximal ideal $e^{-1}(m)/mS$. Then, given a regular function $f \in S$ such that $S/(f)$ is finite over R, we can find a $t \in I$ such that*

- *S is finite over $R[t]$;*
- *There is an ideal J comaximal with I and such that $I \cap J = (t)$;*
- *(f) and J are comaximal; (f) and $(t-1)$ are comaximal;*
- *$S/(t)$ is étale over R; $S/(t-1)$ is étale over R.*

Proof. See [11, 6.1] □

Consider the presheaf of abelian groups $F : T \mapsto coker(SN)(T)$. According to 4.3 to prove the mentioned injectivity we have to show that the functor F satisfies axioms C, E and the weak versions of axioms TE, TA, TB of [10] (see 4.4). Axioms C, E, TA and TB hold by the same arguments as in sections 3.2 and 3.4 of [10].

Consider, for instance, the proof of axiom E. First, following the proof of E.(a) and E.(b) of [10, 3.2] for a given quadratic space q over R we construct the R-algebra $\tilde{S}$, two quadratic spaces $q_1 = q \otimes_A \tilde{S}$ and $q_2 = q \otimes_R \tilde{S}$ over $\tilde{S}$ and the isomorphism Ψ between them such that the restrictions $q_1|_R$ and $q_2|_R$ coincide with q and the restriction $\Psi|_R$ is the identity. Then following the proof of E.(c) the isomorphism Ψ induces a commutative diagram

$$\begin{array}{ccc} SO_{q_1}(T) & \xrightarrow{\Psi} & SO_{q_2}(T) \\ \downarrow{\scriptstyle SN} & & \downarrow{\scriptstyle SN} \\ T^*/(T^*)^2 & \xrightarrow{\Psi} & T^*/(T^*)^2 \end{array}$$

for any $\tilde{S}$-algebra T. Taking the cokernels of the vertical arrows we obtain the desired functor transformation $\Phi : F_1(T) \to F_2(T)$ of E.(c).

Hence, in order to prove the injectivity, it remains to produce a well-defined transfer map $Tr_R^S : F(S) \to F(R)$ for any finite étale extension S/R of a local regular ring of geometric type over an infinite field.

To produce such a map it suffices to take the norm map $N_R^S : S^* \to R^*$ and to check the inclusion

$$N_R^S(SN(SO_q(S))) \subset SN(SO_q(R)).$$

Since in the semi-local case $SN(SO_q(S)) = D_q^0(S)$ and $SN(SO_q(R)) = D_q^0(R)$ (see [6, IV.6], [1, III.3.21]) it remains to check the inclusion

$$N_R^S(D_q^0(S)) \subset D_q^0(R).$$

This inclusion holds by Theorem 3.14. Hence, the norm map $N_R^S : S^* \to R^*$ induces the desired transfer map $Tr_R^S : F(S) \to F(R)$. This completes the proof of Theorem 4.1 in the geometric case.

Finally, to extend our result to the case of a local regular ring R containing an infinite field of characteristic different from 2 we use Popescu's approximation theorem [11, 7.5]. We refer to the item 1 of section 5 of [10] for the precise arguments. □

References

[1] R. Baeza: *Quadratic forms over semi-local rings*, Lecture Notes in Mathematics, Vol. 655, Springer-Verlag, 1978.

[2] M. Demazure and P. Gabriel: *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, North-Holland, 1970.

[3] A. Grothendieck, Le groupe de Brauer. II. Théorie cohomologique. (French) Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam; Masson, Paris, 1968, pp.67-87.

[4] T.Y. Lam: *The algebraic theory of quadratic forms*, W.A. Benjamin, 1973.

[5] M. Knebusch, Ein Satz über die Werte von quadratischen Formen über Körpern, Invent. Math. 12 (1971), 300–303.

[6] M.-A. Knus: *Quadratic and Hermitian Forms over Rings*, Grund. Math. Wiss. 294, Springer-Verlag, 1991.

[7] M. Ojanguren, Quadratic forms over regular rings, *J. Indian Math. Soc.* 44: 109–116 (1980).

[8] M. Ojanguren, I. Panin, Rationally trivial hermitian spaces are locally trivial, *Math. Z.* 237: 181–198, 2001.

[9] K. Zainoulline: On Knebusch's Norm Principle for quadratic forms over semi-local rings, Preprints of Max-Planck-Institute für Mathematik 40, 2003.

[10] K. Zainoulline, On Grothendieck's conjecture on principal homogeneous spaces for some classical algebraic groups, *St. Petersburg Math. J.* 12(1): 117–143, 2001.

[11] K. Zainoulline, The Purity Problem for Functors with Transfers, *K-Theory* 22(4): 303–333, 2001.

Manuel Ojanguren
Ecole Polytechnique Fédérale de Lausanne
Institut de Géométrie, Algèbre et Topologie
Bâtiment BCH
1015 Lausanne
Switzerland
e-mail: manuel.ojanguren@epfl.ch

Ivan Panin
St. Petersburg Department of
V.A. Steklov Institute of Mathematics
27, Fontanka
St. Petersburg 191023
Russia
e-mail: panin@pdmi.ras.ru

Kirill Zainoulline
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld
Germany
e-mail: kirill@mathematik.uni-bielefeld.de