On Knebusch's Norm Principle for quadratic forms over semi-local rings

K. Zainoulline

kirill@mathematik.uni-bielefeld.de

Abstract

We prove Knebusch's Norm Principle for finite extensions of semi-local regular rings containing a field of characteristic 0. As an application we prove the version of Grothendieck-Serre's conjecture on principal homogeneous spaces for the split case of the spinor group.

MSC2000: 13H05, 11E08, 14M17

Key Words: local regular ring, quadratic form, norm principle

1 Introduction

Let L/K be a finite field extension and q be a regular quadratic form over K. Let $D(q_L) \subset L^*$ be the subgroup generated by the set of non-zero elements of the field L represented by the form q. The well-known Knebusch's Norm Principle for quadratic forms over fields [4], [3, VII.5.1] says there is an inclusion $N_K^L(D(q_L)) \subset D(q_K)$ between the subgroups of K^*, where N_K^L is the norm map.

The present paper is devoted to the proof of Knebusch's Norm Principle for quadratic forms over semi-local regular rings. Namely, we want to prove the following

1.1 Theorem. *Let S/R be a finite extension of semi-local regular rings containing a field k of characteristic 0. Let q be a regular quadratic form over R of rank m and $q_S = q \otimes_R S$ be it's base change. Then we have the following inclusion between the subgroups of the group of invertible elements R^**

$$N_R^S(D^0(q_S)) \subset D^0(q_R),$$

where $N_R^S : S^* \to R^*$ is the norm map and the subgroup $D^0(q_S) \subset S^*$ is generated by all products of two elements represented by q_S, i.e., $D^0(q_S) = \langle q_S(x_1)q_S(x_2) \mid x_1,\, x_2 \in S^m\rangle$. In particular, the following inclusion holds

$$N_R^S(D(q_S)) \subset D(q_R),$$

where the subgroup $D(q_S) \subset S^*$ is generated by all invertible elements of S that are represented by the quadratic form q_S, i.e., $D(q_S) = \langle q_S(x),\, x \in S^m\rangle$.

In order to prove 1.1, first, we prove Norm Principle for simple extensions of semi-local domains (Theorem 4.2). Briefly speaking, a finite extension S/R is called simple, where R is a semi-local domain, if $S = R[t]/(p(t))$ is the quotient of the polynomial ring $R[t]$ by some monic polynomial p. A finite etale extension (or separable in the case of fields) is an example of a simple extension (see section 2). The proof of 4.2 proceeds by induction on degree of extension. In order to make the induction step we use general position arguments of section 3 (Theorem 3.11). Then, using 4.2 we prove the version of Grothendieck-Serre's conjecture on principal homogeneous spaces [2] for the case of the spinor group (Theorem 5.2). The conjecture states the canonical map

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

has trivial kernel, where R is a semi-local regular ring and K is it's quotient field. We prove the map i_R has the trivial kernel if R is a semi-local regular ring containing a field of characteristic 0. The main tool of the proof is the injectivity theorem of section 2 of [7] together with the etale version of Geometric Presentation Lemma [8, 6.1]. We finish the proof of 1.1 by some diagram chase, where Knebusch's Norm Principle over fields and Grothendieck-Serre's conjecture over rings play the crucial role.

Agreements and Notations All rings are assumed to be commutative with units. By R and S we denote semi-local domains. k means the residue field (sections 2, 3 and 4) or the base field (section 5). By "bar" we mean the reduction modulo the maximal ideal (radical) of a (semi-)local ring. By a ring extension S/R we mean a ring S together with a ring monomorphism $R \to S$. By S^* we denote the group of invertible elements of S.

For simplicity all the proofs and definitions of sections 2, 3 and 4 are given for local rings only. In order to pass from the local case to the semi-local case, one has to replace the words "maximal ideal" by the words "radical ideal".

Let S/R be a ring extension such that S is free as the R-module. Then there is the norm map denoted by N^S_R that is given as follows. For any $c \in S$ let $l_c : S \to S$ be the endomorphism of the free R-module S given by the left multiplication by c. Then we set $N^S_R(c) = \det(l_c)$, where l_c is the respective matrix.

We say a quadratic form q over R is regular if the determinant of the respective symmetric matrix is invertible in R. Observe that any regular quadratic form over a semi-local ring of characteristic different from 2 is diagonalizable, i.e., q can be represented as a sum of squares with coefficients from R^*.

The author is grateful to Max-Planck-Institute für Mathematik in Bonn and European Post-Doctoral Institute for hospitality and financial support. The author is also grateful to the RTN-Network HPRN-CT-2002-00287 and INTAS-Project 99-00817 for the travel support during the work.

2 Simple extensions of local rings

2.1. We say a ring extension S/R is a simple extension of degree n if there exists an element $c \in S^*$ such that S is free as the R-module with the basis $\{1, c, \ldots, c^{n-1}\}$ denoted by $\mathcal{B}(c)$. The element c is called a primitive element. Let $c^n = a_0 + a_1 c + \ldots + a_{n-1} c^{n-1}$ be the unique presentation of the element c^n in the basis $\mathcal{B}(c)$. The polynomial $p_c(t) = t^n - a_{n-1} t^{n-1} - \ldots - a_0$ is called a minimal polynomial for the primitive element c. It has the property $p_c(c) = 0$. Observe that S can be identified with the quotient $R[t]/p_c(t)$ of the polynomial ring $R[t]$ modulo the principal ideal generated by $p_c(t)$. Since c is invertible, it's norm $N_R^S(c) = (-1)^n p_c(0) = (-1)^{n-1} a_0$ is invertible as well.

To the opposite direction, for a given monic polynomial $p(t) \in R[t]$ such that $p(0) \in R^*$ the ring extension $S = R[t]/p(t)$ over R is a simple extension of degree $n = \deg p$. The image of t by means of the canonical map $R[t] \to R[t]/p(t)$ gives the respective primitive element of the extension S/R.

2.2. Clearly, if $c \in S^*$ is a primitive element of a simple extension S/R, then it's inverse c^{-1} is primitive and $r_1 c + r_0$ is primitive for any $r_1 \in R^*$ and $r_0 \in R$ such that $p_c(-r_0/r_1) \in R^*$.

2.3. Let S/R be a simple extension with the primitive element c, then $\bar{S}/\bar{R}$ is a simple extension of the same degree with the primitive element $\bar{c}$. Moreover, if b is a primitive element of $\bar{S}$, then by Nakayama's lemma the preimage $c \in \rho^{-1}(b)$ is primitive as well, where $\rho : S \to \bar{S}$ is the reduction map. In other words, if S^*_{prim} denotes the subset of primitive elements of S and $\bar{S}^*_{prim}$ denotes the subset of primitive elements of $\bar{S}$, then we have $S^*_{prim} = \rho^{-1}(\bar{S}^*_{prim})$.

2.4 Remark. Let S/R be a simple extension. In the case $R = k$ is a field the algebra S can be viewed as the product of local Artinian algebras over k. For instance, if k is algebraically closed, the algebra S is isomorphic to the product of algebras of the kind $k[t]/t^m$, $m \geq 1$. In the case S is a field we get a simple field extension S/k. Recall (by the Primitive Element Theorem) that any finite separable field extension is simple but not in the other direction. There are examples of finite field extensions which are not simple.

3 Some general position arguments

In the present section S will be a simple extension of an infinite field k.

3.1. Let S be a simple extension of k of degree n. The k-algebra S can be viewed as the k-vector space of dimension n and, thus, can be identified with the set of rational points of the affine space $\mathbb{A}^n$ over k. From this point on we assume $S = \mathbb{A}^n(k)$ is the topological space by means of Zariski topology structure.

For example, any map $S \to S$ given by $b \mapsto f(b)$ is continuous, where $f(t) \in S[t]$ is a polynomial with coefficients in S. And the set S^* of invertible elements is open in S, since it is given by the equation $N_k^S(x) \neq 0$, where N_k^S is the norm map.

In the case of an infinite field k this topology has the important property – the intersection of any two open subsets is non-empty.

3.2 Lemma. *Let S be a simple extension of a field k. Then the subset of primitive elements S^*_{prim} is non-empty and open in S^*.*

Proof. We fix some primitive element c of S. An element $b \in S^*$ is primitive iff the matrix $(b_{i,j})_{i,j=0}^{n-1}$ has non-zero determinant, where $b_{i,j}$ is the i-th coefficient in the presentation of the j-th power b^j of the element b in the basis $\mathcal{B}(c)$. Observe that $b_{i,1} = b_i$ are the coefficients of the presentation of the element b in the basis $\mathcal{B}(c)$, i.e, $b = b_0 + b_1 c + \ldots + b_{n-1}c^{n-1}$. Clearly, the determinant $\det(b_{i,j})$ can be viewed as the polynomial in n variables $b_0, \ldots, b_{n-1}$ and, thus, the subset

$$S^*_{prim} = \{b = (b_0, \ldots, b_{n-1}) \in S^* \mid \det(b_{i,j}) \neq 0\}$$

is open in S^*. $\square$

3.3 Lemma. *Let S be a simple extension of an infinite field k of characteristic different from 2 and let $c \in S^*$ be an invertible element. Then the subset $V_c = \{b \in S^* \mid cb^2$ is primitive$\}$ is non-empty and open in S^*.*

Proof. Since the map $S^* \to S^*$ given by $b \mapsto cb^2$ is continuous, it is enough to show that the image of the map $f : S^* \to S^*$ given by $b \mapsto b^2$ is dense. (observe that the multiplication by c is the homeomorphism). The algebra S splits as the product of local Artinian algebras and the image of f is dense if the image of the restriction of f to the each component of this product is dense. Thus, we may assume S is a local Artinian algebra over k and, hence, it is irreducible.

Assume the image of f is not dense. Then the closure of the image of f in S must have the dimension strictly less than the dimension of S (considered as the affine space over k). It means that f induces the regular map between two affine spaces such that the dimension of the target space is strictly less than the dimension of the origin space S. In particular, there exists an element $u \in S^*$ such that the equation $b^2 = u$ has infinite number of solutions (the dimension of the fiber of f over u is ≥ 1 and k is infinite). Hence, we get contradiction by Lemma 3.4. $\square$

3.4 Lemma. *Let S be a simple extension over an infinite field k of characteristic different from 2. Let u be an invertible element of S. Then the number of solution of the equation $b^2 = u$ is finite (or empty).*

Proof. Let k' be the algebraic closure of the field k. Let $S' = S \otimes_k k'$ be the base change of S. Clearly, S' is the simple extension of k' of the same degree. The number of solutions of $b^2 = u$ over S is finite if it is finite over S'.

Since the algebra S' splits as the finite product of algebras of the kind $A_m = k'[t]/t^m$, $m \geq 1$, it is enough to show that the number of solutions of $b^2 = u$ is finite in A_m for any m.

The case $m = 1$ is trivial, since $A_1 = k'$ is a field. Let $m > 1$. In the basis $\mathcal{B}(t)$ of A_m our equation can be written as:

$$(b_0 + b_1 t + \ldots + b_{m-1} t^{m-1})^2 = u_0 + u_1 t + \ldots + u_{m-1} t^{m-1}.$$

Hence, we get the system of m quadratic equations over k'

$$b_0^2 = u_0,\ 2b_0 b_1 = u_1,\ 2(b_0 b_2 + b_1^2) = u_2,\ 2(b_3 b_0 + b_2 b_1) = u_3, \ldots \qquad (*)$$

which has the property that any element b_j is the solution of the quadratic or linear equation over k' (precisely the $j+1$-th equation) with coefficients b_i, $i < j$, and u_i, $i \leq j$. Then it follows immediately that the number of solutions of (*) is finite. $\square$

3.5 Remark. The assumption that the characteristic of k is different from 2 is essential. Take k to be the algebraic closure of the finite field $\mathbb{F}_2$ then the algebra $S = k[t]/t^2$ is the simple extension of k. But it easy to see that the image of the map $b \to b^2$ coincides with the subspace $k \cdot 1$ in $S = k \cdot 1 \oplus k \cdot t$ which consists of all non-primitive elements of S..

3.6. Let $c \in S^*$ be a primitive element of a simple extension S/k of degree n. Let x be an element of S. By the symbol $\{x, c\}$ we denote the n-th coefficient of the presentation of x in the basis $\mathcal{B}(c)$, i.e., $\{x, c\} = x_{n-1}$, where $\sum_{i=0}^{n-1} x_i c^i = x$.

3.7 Lemma. *Let S be a simple extension of degree n of a field k of characteristic 0. Let $c \in S^*_{prim}$ be a primitive element and let x be a non-zero element of S. Then the subset $W_{c,x} = \{b \in V_c \mid \{xb^{-1}, cb^2\} \neq 0\}$ is non-empty and open in S^*, where V_c is the non-empty open subset from Lemma 3.3.*

3.8 Remark. The assumption that k has characteristic 0 is essential. Take k to be the algebraic closure of the finite field $\mathbb{F}_3$. Consider the algebra $S = k[t]/t^3 - 1$. Take $x = c = t$. It is easy to see that $\{xb^{-1}, cb^2\} = 0$ for all $b \in S^*$.

Proof. Let $xb^{-1} = v_0 + v_1(cb^2) + \ldots + v_{n-1}(cb^2)^{n-1}$ be the presentation of the element xb^{-1} in the basis $\mathcal{B}(cb^2)$. Our goal is to show that the subset of the elements $b \in V_c$ with $v_{n-1} \neq 0$ is non-empty and open in S^*.

Multiplying the presentation of xb^{-1} by b we get the following equation:

$$x = v_0 b + v_1(cb^3) + \ldots + v_{n-1} c^{n-1} b^{2n-1}. \qquad (*)$$

Now consider the primitive element c of S. Let $x = x_0 + x_1 c + \ldots + x_{n-1} c^{n-1}$ and $b = b_0 + b_1 c + \ldots + b_{n-1} c^{n-1}$ be the presentations of the elements x and b in the basis $\mathcal{B}(c)$. Consider the equation (*) in terms of the basis $\mathcal{B}(c)$. We get the system of n linear equations in n variables $v_0, \ldots, v_{n-1}$:

$$\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} = v_0 \cdot \begin{pmatrix} h_{0,0}(b_0, \ldots, b_{n-1}) \\ h_{1,0}(b_0, \ldots, b_{n-1}) \\ \vdots \\ h_{n-1,0}(b_0, \ldots, b_{n-1}) \end{pmatrix} + \ldots v_{n-1} \cdot \begin{pmatrix} h_{0,n-1}(b_0, \ldots, b_{n-1}) \\ h_{1,n-1}(b_0, \ldots, b_{n-1}) \\ \vdots \\ h_{n-1,n-1}(b_0, \ldots, b_{n-1}) \end{pmatrix},$$

where $h_{i,j}$ are polynomials in n variables $b_0, \dots, b_{n-1}$ with coefficients from k. In particular, the first column is the vector of monomials $(b_0, \dots, b_{n-1})$, i.e., $h_{i,0} = b_i$ for all $i = 0 \dots n-1$. The second column consists of the coefficient of the presentation of cb^3 in the basis $\mathcal{B}(c)$ and so on. Solving this linear system we get

$$v_{n-1} = \det(A_{(n-1)}) / \det(A),$$

where A is the matrix of the system and the matrix $A_{(n-1)}$ is got by replacing the last column of A by the vector x (of free terms). Observe that both $\det(A_{(n-1)})$ and $\det(A)$ are homogeneous polynomials (in n variables $b_0, b_1, \dots, b_{n-1}$) of degrees $1 + 3 + \dots + (2n-3) = (n-1)^2$ and $1 + 3 + \dots + (2n-1) = n^2$ respectively. Hence, the map $V_c \to k$ given by $b = (b_0, \dots, b_{n-1}) \mapsto v_{n-1}$ is the regular map (observe that the determinant $\det(A)$ is non-zero for all $b \in V_c$, since cb^2 is primitive). Thus, the subset W_c is open in S^*. The fact that W_c is non-empty follows from Sublemma 3.9 below. $\square$

3.9 Sublemma. *If $x \neq 0$, then the polynomial $\det(A_{n-1})$ is non-trivial.*

Proof. We may assume the field k is algebraically closed. We have the presentation of the determinant

$$\det(A_{(n-1)}) = \Delta_0 x_{n-1} - \Delta_1 x_{n-2} + \dots + (-1)^{n-1} \Delta_{n-1} x_0,$$

where Δ_i, $i = 0, \dots, n-1$, is the determinant of the $(n-1-i, n-1)$-minor of $A_{(n-1)}$. For each monomial $b_0^{m_0} b_1^{m_1} \dots b_{n-1}^{m_{n-1}}$ we define the weight to be the sum $\sum_{i=0}^{n-1} i \cdot m_i$. Observe that each polynomial Δ_i consists of monomials of weight $\geq i$. Indeed, it is enough to consider the simple extension $S = k[t]/t^n$ over k (see 2.4). In this case the element $h_{i,j}(b_0, \dots, b_{n-1})$ of the respective matrix A is the zero polynomial if $i < j$ and consists of monomials of the weight $i - j$ otherwise, i.e., we have the following matrix of weights

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 2 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ n-1 & n-2 & n-3 & \dots & 0 \end{pmatrix}.$$

where the first column corresponds to the vector of monomials $(b_0, \dots, b_{n-1})$.

Now it is easy to see that the polynomial Δ_i consists of monomials of the weight that is greater or equal than the weight of the product of diagonal elements of the $(n-1-i, n-1)$-minor of $A_{(n-1)}$, i.e., precisely i.

Now each minor can be viewed as the sum $\Delta_i = h_i + h_{>i}$ of two homogeneous polynomials (in n-variables $b_0, b_1, \dots, b_{n-1}$) of degree $(n-1)^2$, where h_i is the sum of monomials of weight i and $h_{>i}$ is the sum of monomials of weight strictly bigger than i.

We claim that $h_i \neq 0$. Indeed, for $i = 0$ we have $h_0 = b_0^{(n-1)^2}$, i.e., $h_0 \neq 0$. For $i = 1$ we have $h_1 = -C^1_{2n-3} b_0^{n(n-2)} b_1 = -(2n-3) b_0^{n(n-2)} b_1$ which is non-zero if the characteristic of k doesn't divide $2n-3$. For $i > 1$ the polynomial

h_i contains the unique monomial (the monomial with the maximal power of b_0) $(-1)^i(2(n-i)-1)b_0^{n(n-2)}b_i$ which is non-zero if the characteristic of k doesn't divide $2(n-i)-1$.

Now it follows immediately that the polynomials Δ_i, $i=0,\dots,n-1$, are linearly independent. And we are done. $\square$

We will need one more fact concerning the polynomials Δ_i:

3.10 Sublemma. . *For any integers $0 \le i,j \le n-1$ The polynomials $\Delta_i\Delta_j$, where $i \le j$, are linearly independent.*

Proof. The product $\Delta_i\Delta_j$ is the homogeneous polynomial of degree $2(n-1)^2$ and can be represented as follows $\Delta_i\Delta_j = h_ih_j + g_{>i+j}$, where h_ih_j is the sum of monomials of weight $i+j$ and $g_{>i+j}$ consists of monomials of weight strictly bigger than $i+j$. Observe now that h_ih_j contains the unique monomial (the monomial with the maximal power of b_0) $(-1)^{i+j}(2(n-i)-1)(2(n-j)-1)b_0^{2n(n-2)}b_ib_j$ (see the proof of the previous Sublemma). $\square$

Now we are ready to prove the main result of this section:

3.11 Theorem. *Let S be a simple extension of degree n of a field k of characteristic 0. Let c be a primitive element of S/k. Let q be a regular quadratic form over k of rank m. and $x=(x^{(1)},\dots,x^{(m)})$ be a vector in S^m such that $q(x)\neq 0$. By $\{x,c\}=(x^{(1)}_{n-1},\dots,x^{(m)}_{n-1})$ we denote the vector of the $(n-1)$-th coordinates of x in the basis $\mathcal{B}(c)$, i.e., $\{x,c\}_j=\{x^{(j)},c\}$. Then the subset*

$$U_{c,x,q}=\{b\in V_c \mid q(\{xb^{-1},cb^2\})\neq 0\}$$

is non-empty and open in S^*.

3.12 Remark. According to 3.8 the Theorem is not true if the characteristic of the residue field k is non-zero. Take $k=\bar{\mathbb{F}}_3$, $S=k[t]/(t^3-1)$, $q(x)=x^2$ and $c=x=t$.

Proof. The proof is a little modification of the proof of 3.7. We use the notation introduced in the proof of Lemma 3.7.

Clearly, $U_{c,x,q}$ is open (by the same arguments as in 3.7). The main problem is to show that $U_{c,x,q}$ is non-empty. Hence, we have to prove that the polynomial $q(\det(A^{(1)}_{(n-1)}),\dots,\det(A^{(m)}_{(n-1)}))$ is non-trivial, where $A^{(j)}_{(n-1)}$ denotes the matrix corresponding to the element $x^{(j)}$. Let

$$\det(A^{(j)}_{(n-1)})=\Delta_0x^{(j)}_{n-1}-\Delta_1x^{(j)}_{n-2}+\ldots+(-1)^{n-1}\Delta_{n-1}x^{(j)}_0$$

be the representation as in the proof of 3.9, where $x^{(j)}=\sum_{i=0}^{n-1}x_i^{(j)}c^i$ is the presentation of $x^{(j)}$ in the basis $\mathcal{B}(c)$. Let $q(x)=\sum_j a_j(x^{(j)})^2$ be our quadratic form.

Then, we have

$$(\det A)^2 \cdot q(\{xb^{-1}, cb^2\}) = \sum_j a_j (\det A^{(j)}_{(n-1)})^2 =$$

$$= \sum_j a_j (\sum_i (-1)^i x^{(j)}_{n-1-i} \Delta_i)^2$$

Now if we replace Δ_i by $(-1)^i t^{n-1-i}$ we get precisely

$$\sum_j a_j (\sum_i (-1)^i x^{(j)}_{n-1-i} \Delta_i)^2 = q(x^{(1)}(t), \ldots, x^{(m)}(t)) \tag{*}$$

as the polynomial in $R[t]$, where $x^{(j)}(t) = \sum_i x_i^{(j)} t^i$.

Assume that the polynomial $q(\{xb^{-1}, cb^2\})$ is trivial. Since the polynomials $\Delta_i \Delta_j$ are linearly independent (by Sublemma 3.10), this implies that the polynomials $\Delta_i \Delta_j$ in the sum (*) have zero coefficients. In particular, the t^i have trivial coefficients as well, i.e., the polynomial $q(x^{(1)}(t), \ldots, x^{(m)}(t))$ is trivial. This contradicts with the hypothesis of the Theorem that the image of $q(x^{(1)}(t), \ldots, x^{(m)}(t))$ by means of the canonical map $R[t] \to R[t]/p_c(t) = S$, i.e., precisely $q(x)$, is non-trivial. $\square$

4 The Knebusch's Norm Principle

4.1. Let q_S be a quadratic form of rank m over a ring S. By $D^0(q_S)$ ($D^1(q_S)$) we denote the set of all even (odd) products of invertible elements of S represented by q_S, i.e.,

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

Observe that $D^0(q_S)$ forms the subgroup of the group $D(q_S)$ generated by all invertible elements represented by q_S. And $D^1(q_S)$ is just a subset of $D(q_S)$. Clearly, if $c \in D^i(q_S)$, $i = 0, 1$, and $b \in D^0(q_S)$, then $cb \in D^i(q_S)$.

Let n be a positive integer, then we set $D^n(q_S) = D^0(q_S)$ if n is even and $D^n(q_S) = D^1(q_S)$ if n is odd.

The goal of the present section is to prove the following

4.2 Theorem. *Let R be a semi-local domain with residue fields of characteristic 0. Let S/R be a simple extension of degree n. Let q be a regular quadratic form over R of rank m. Let $c \in S^*$ be an element represented by the form q_S, i.e., $c = q_S(x)$ for some vector $x \in S^m$. Then $N_R^S(c) \in D^n(q_R)$, where N_R^S is the norm map. In particular, there is an inclusion between the subgroups of R^**

$$N_R^S(D^0(q_S)) \subset D^0(q_R),$$

where $D^0(q_S)$ is the subgroup generated by all products of two elements of S^* represented by q_S.

4.3 Lemma. *In the hypothesis of Theorem 4.2 we have $(S^*)^2 \subset D^0(q_S)$.*

Proof. Let $r \in R^*$ be a value of the quadratic form q, i.e., $r = q(y)$ for some $y \in R^m$. Then for any $b \in S^*$ we have $b^2 = q(yb)q(y/r) \in D^0(q_S)$. $\square$

The Proof of Theorem 4.2. We prove by induction on the degree n of the simple extension S/R. The case $n = 1$ is trivial. Assume $n > 1$.

In order to make the induction step we use the following idea: Since any square can be viewed as the product of two elements represented by the quadratic form q, the multiplication by a square doesn't change a lot, hence, it gives some freedom in the choice of elements. As a consequence, by applying general position arguments (Theorem 3.11) we may control the leading coefficient of the polynomial h (see the equation (**)) and make it invertible. Since it is invertible, we may apply the induction hypothesis and we are done.

More precisely, let $c = q_S(x)$ for some $x \in S^m$. We want to show $N_R^S(c) \in D^n(q)$. By 2.3 and Lemma 3.3 the element c can be written as the product $c = cb^2 \cdot (1/b)^2$, where $cb^2 = q_S(xb) \in D^n(q_S)$ is primitive. Hence, by multiplicativity of the norm map and Lemma 4.3 we may assume c (replaced by cb^2) is primitive.

Now we mimic the proof of [4] (see also [3, VII.5.1]). Replace c by it's inverse c^{-1}. We get the equation $1 = cq_S(x)$, where c is primitive. More precisely, we have

$$1 = cq_S(x^{(1)}(c), \ldots, x^{(m)}(c)), \tag{*}$$

where $x^{(j)}(c) \in S$ is the j-th coordinate of the vector x written in the basis $\mathcal{B}(c)$. According to Theorem 3.11 we may assume that the value of the quadratic form q_S on the last coefficients of the vectors $x^{(j)}$, i.e., $q(x^{(1)}_{n-1}, \ldots, x^{(m)}_{n-1})$, is invertible in R. In fact, it is enough to consider the quotient modulo the maximal ideal of R (see 2.3), i.e., the simple extension $\bar{S}/k$. The open subset $U_{c,x,q}$ from 3.11 is non-empty and open. Take any element b from $U_{c,x,q}$ and replace c by cb^2 and x by x/b.

Consider the pull-back of the equation (*) by means of the canonical map $R[t] \to R[t]/p_c(t) = S$. Since $tq(x(t)) - 1$ lies in the principal ideal $(p_c(t))$ of the polynomial ring $R[t]$ there is a polynomial $h(t)$ such that

$$1 + p(t)h(t) = tq_S(x^{(1)}(t), \ldots, x^{(m)}(t)). \tag{**}$$

Since R is a domain the leading coefficient of the left hand side of (**) coincides with the leading coefficient of h, denoted by r, and coincides with the leading coefficient of the right hand side that is $r = q(x^{(1)}_{n-1}, \ldots, x^{(m)}_{n-1})$, where r is invertible in R. Clearly, we have $n + \deg h = 2(n-1) + 1$. So that $\deg h = n - 1$.

As in [4] we have $N_R^S(c) = (-1)^n p_c(0)$ and $1 + p_c(0)h(0) = 0$. Hence, we have

$$N_R^S(c)^{-1} = (-1)^{n-1} g(0) r,$$

where $g(t) = h(t)/r$ is the monic polynomial of degree $\deg h = n - 1$. Observe that the norm of the primitive element $u = t$ of the respective simple extension $T = R[t]/g(t)$ over R is precisely $N_R^T(u) = (-1)^{n-1}g(0)$. Hence, in order to show that $N_R^S(c) \in D^n(q)$ it is enough to show that $N_R^T(u) \in D^{n-1}(q)$. But this follows by the induction hypothesis, since u is represented by the quadratic form q_T. Indeed, taking (**) modulo the principal ideal (g(t)) we get similar to (*) the equation $1 = uq_T(x(u))$, i.e., $u = q_T(x(u)/u)$. $\square$

5 Grothendieck-Serre's conjecture for the case of the spinor group

5.1. Let R be a semi-local domain with the residue fields of characteristic different from 2 and q be a regular quadratic form over R. Following [5, 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. Recall that $S\Gamma_q(R) = \{c \in C_0(V,q)^* \mid cVc^{-1} \subset V\}$, where $C_0(V,q)$ is the even part of the Clifford algebra of the respective quadratic space (V,q) over R.

The goal of the present section is:

5.2 Theorem. *Let R be a semi-local regular ring containing a field of characteristic 0. Let K be it's quotient field. Let q be a regular quadratic form 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 form q.

5.3 Remark. Observe that the theorem is the particular case $G = Spin_q$ of Grothendieck-Serre's conjecture on principal homogeneous spaces [2], which states for a flat 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 papers [7] and [8].

Assume R is a semi-local regular ring of geometric type over a field of characteristic 0. Let K be it's quotient field. We have the following commutative diagram (see [5, IV.8.2.7]):

$$\begin{tikzcd}
SO_q(R) \arrow[r, "SN"] \arrow[d] & R^*/(R^*)^2 \arrow[r] \arrow[d] & H^1_{et}(R, Spin_q) \arrow[r] \arrow[d] & H^1_{et}(R, SO_q) \arrow[d] \\
SO_q(K) \arrow[r, "SN"] & K^*/(K^*)^2 \arrow[r] & H^1_{et}(K, Spin_q) \arrow[r] & H^1_{et}(K, SO_q),
\end{tikzcd}$$

where $SN : SO_q(R) \to H^1_{et}(R, \mu_2) = R^*/(R^*)^2$ is the spinor norm. The main result of paper [6] says that the vertical arrow on the right hand side has trivial kernel (see also [7, 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.

Consider the group scheme $F : S \mapsto coker(SN)(S)$. According to the theorem of section 2 of [7] to prove the mentioned injectivity we have to show that the functor F satisfies all the axioms C,TE,TA,TB, E of sections 1 and 2 of [7]. In fact, all the axioms, excluding the existence of transfer map, i.e., TE, holds by the same arguments as in sections 3.2 and 3.4 of [7]. Hence, in order to prove the injectivity we have to produce a well-defined transfer map $Tr^S_R : F(S) \to F(R)$ for any finite surjective extension of semi-local rings S/R (see the axiom TE of [7]).

Observe that for any finite surjective extension S/R of semi-local rings there is already a well-defined norm map $N^S_R : S^*/(S^*)^2 \to R^*/(R^*)^2$. Hence, if we show that the norm map N^S_R is compatible with the spinor norm, i.e.,

$$N^S_R(SN(SO_q(S))) \subset SN(SO_q(R)),$$

then taking $Tr^S_R = N^S_R$ on the quotients modulo the images of SN we get the desired transfer map.

In fact, instead of finite surjective extensions we may consider only finite etale extensions S/R of semi-local rings. Indeed, if we replace the Geometric Presentation Lemma [6, 10.1] used in the section 1.1 of [7] by it's stronger (etale) version from [8, 6.1], then nothing will be changed in the proof of the injectivity theorem of section 2 of [7].

According to the definition of the spinor norm [5, IV.6], [1, III.3.21] to show the norm map commutes with the spinor norm is equivalent to show the norm map commutes with the functor $D : S \mapsto D^0(q_S)$ (that sends any R-algebra S to the subgroup $D^0(q_S)$), i.e., $N^S_R(D^0(q_S)) \subset D^0(q_R)$. Hence, we have to prove the analog of Knebusch's Norm Principle for quadratic forms in the case of finite etale extensions of semi-local rings. But this is done by Theorem 4.2.

Finally, to extend our result to the case of a semi-local regular ring containing a field of characteristic 0 we use Popesky's approximation theorem [8, 7.5]. We refer to the item 1 of section 5 of [7] for the precise arguments. □

Now we are ready to prove the main theorem of this paper

The Proof of Theorem 1.1. We use the notations of the proof of Theorem 5.2. Let K and L be the quotient fields of the semi-local rings R and S respectively. Observe that L/K is a finite field extension. We have the commutative diagram of abelian groups

$$\begin{tikzcd} S^*/(S^*)^2 \arrow[r, "can"] \arrow[d, "N^S_R"'] & coker(SN)(S) \arrow[r, "i_S"] & coker(SN)(L) \arrow[d, "N^L_K"] \\ R^*/(R^*)^2 \arrow[r, "can"] & coker(SN)(R) \arrow[r, "i_R"] & coker(SN)(K) \end{tikzcd}$$

where can is the quotient map, the maps i_R and i_S are injective according to the proof of 5.2 and N^L_K is the norm map for the finite field extension L/K taken modulo the images of the spinor norms. Observe that N^L_K is well-defined since the Norm Principle holds in the case of finite field extensions [4].

The diagram immediately implies that the norm map N_R^S is well-defined on the quotients, i.e., $N_R^S(SN(SO_q(S))) \subset SN(SO_q(R))$ or, equivalently,

$$N_R^S(D^0(q_S)) \subset D^0(q_R).$$

$\square$

5.4 Remark. Observe that under some restrictions the proofs of 5.2 and 1.1 imply that the Grothendieck-Serre's conjecture for the spinor group is equivalent to the Knebusch's Norm Principle.

References

[1] R. Baeza, Quadratic forms over semilocal rings, Lect. Notes in Math. 655, 1978.

[2] 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.

[3] T.Y. Lam, The algebraic theory of quadratic forms, Math. Lect. Notes Ser., W.A.Benjamin, Inc., 1973.

[4] M. Knebusch, Ein Satz über die Werte von quadratischen Formen über Körpern. (German) *Invent. Math.* 12: 300-303, 1971.

[5] M.-A. Knus, Quadratic and Hermitian Forms over Rings, Grund. der Math Wiss. 294, Springer-Verlag, Berlin, 1991.

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

[7] K. Zainoulline, On Grothendieck's conjecture on principal homogeneous spaces for some classical algebraic groups, *Algebra i Analiz* 12(1): 150-184, 2000 (Russian); transl. in *St.Petersburg Math. J.* 12(1): 117-143, 2001. (the draft version is available on http://www.math.uiuc.edu/K-theory/0332/)

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

Current address (till 31/08/2003): Fakultät für Mathematik, Universität Bielefeld, Postfach 100131, D-33501 Bielefeld, Germany

Permanent address: Laboratory of Algebra and Number Theory, Steklov Mathematical Institute at St.Petersburg, Fontanka 27, 191011 St.Petersburg, Russia