



HAL
open science

SPRINGER'S ODD DEGREE EXTENSION THEOREM FOR QUADRATIC FORMS OVER SEMILOCAL RINGS

Philippe Gille, Erhard Neher

► **To cite this version:**

Philippe Gille, Erhard Neher. SPRINGER'S ODD DEGREE EXTENSION THEOREM FOR QUADRATIC FORMS OVER SEMILOCAL RINGS. 2021. hal-03124810v1

HAL Id: hal-03124810

<https://cnrs.hal.science/hal-03124810v1>

Preprint submitted on 29 Jan 2021 (v1), last revised 18 Jun 2021 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SPRINGER'S ODD DEGREE EXTENSION THEOREM FOR QUADRATIC FORMS OVER SEMILOCAL RINGS

PHILIPPE GILLE AND ERHARD NEHER

Abstract: A fundamental result of Springer says that a quadratic form over a field of characteristic $\neq 2$ is isotropic if it is so after an odd degree extension. In this paper we generalize Springer's theorem as follows. Let R be an arbitrary semilocal ring, let S be a finite R -algebra of odd degree, which is étale or generated by one element, and let q be a nonsingular R -quadratic form whose base ring extension q_S is isotropic. We show that then q is already isotropic.

Keywords: Quadratic forms, semilocal rings, Springer Odd Degree Extension Theorem.

MSC 2000: 11E08, 11E81.

INTRODUCTION

A celebrated result of Springer [Sp] says that a quadratic form over a field F of characteristic $\neq 2$ that becomes isotropic over an odd degree field extension is already isotropic over F . The result was conjectured by Witt and was also proven, but not published by E. Artin. An account of Springer's result is given in [Lam, VII, Thm. 2.7] or [Sch, II, Thm. 5.3]. It is proven for arbitrary fields in [EKM, 18.5].

Springer's Theorem has many important consequences, for example for Witt groups. It is therefore not surprising that it has been generalized by replacing odd degree extensions by more general field extensions, see for example, [Ho1, Prop. 5.3], [Ho2, Cor. 4.2] or [Lag, Lem. 2.8], or by replacing the base field F by more general rings. The main result of this paper goes in the latter direction:

Odd Degree Extension Theorem. (Theorem 2.1) *Let R be a semilocal ring, M a finite projective R -module, $q: M \rightarrow R$ a nonsingular quadratic form, and S a finite R -algebra of odd degree, which is étale or one-generated. If the base ring extension q_S is isotropic, then already q is isotropic.*

Since the terminology regarding quadratic forms over rings is not standard, see the comparison in 1.2(a), let us explain what we mean with a nonsingular quadratic form. Recall that the radical of (M, q) with polar

Date: January 29, 2021.

P. Gille was supported by the ANR project *Geolie* ANR-15-CE40-0012.

E. Neher acknowledges partial support from NSERC through a Discovery grant.

form b_q is $\text{rad}(M, q) = \{m \in M : q(m) = 0 = b_q(m, M)\}$. We call q *nonsingular*, if $\text{rad}((M, q)_F) = \{0\}$ for all R -fields F . An example of such a form is a *regular* quadratic form, defined by the condition that its polar form induces an isomorphism between M and its dual space. Nonsingular and regular quadratic forms are the same in case $2 \in R^\times = \{u \in R : uR = R\}$, the units of R , or in case the projective R -module M has constant even rank, but not in general. For example, for $u \in R^\times$ the quadratic form $R \rightarrow R$, $x \mapsto ux^2$ is always nonsingular, but regular only if $2 \in R^\times$. We call a finite projective R -algebra S of constant degree d *one-generated* if it is generated by one element, equivalently, $S \cong R[X]/f$ for a monic polynomial of degree d .

Special cases of the Odd Degree Extension Theorem have been proven before; all of them assumed $2 \in R^\times$, so that nonsingular = regular. Specifically, it was proven by Panin and Rehmman [PR] under the assumption that R is a noetherian local integral domain, which has an infinite residue field, and that S is étale (necessarily one-generated in this case). It was extended in [PP] by Panin-Pimenov to R a semi-local noetherian integral domain whose residue fields are all infinite. It was stated in [Scu] for R semilocal, $2 \in R^\times$, with a proof that we could not understand.

For proving the Odd Degree Extension Theorem one can easily reduce to M of constant rank $r \geq 2$. The case $r = 2$ (Lemma 2.2) holds for any finite R -algebra; our proof uses a consequence of Deligne's trace homomorphism for the flat cohomology of abelian affine group schemes (Lemma B.3). For $r \geq 3$ we follow an approach inspired by the paper [PR] of Panin and Rehmman and first deal with one-generated algebras. A crucial step here is proving that isotropic elements can be lifted from $M \otimes_R (S/\text{Jac}(R)S)$ to $M \rightarrow_R S$ (Corollary A.6). We obtain this as an application of Demazure's Conjugacy Theorem for reductive R -group schemes. We should point out, that in this part we use the classical version (R a field, [EKM]) of the Odd Degree Extension Theorem. Once the case of one-generated algebras has been settled, the case of étale algebras easily follows by applying a recent result of Bayer-Fluckiger, First and Parimals [BFP] on embeddings of finite étale R -algebras into one-generated R -algebras.

Structure of the paper. Section 1 presents a review of nonsingular quadratic forms and proves some results, needed for our proof of the Odd Degree Extension Theorem in the first part of section 2. In the second part of that section we prove some consequences of the theorem, well-known in case of base fields. The paper closes with two appendices, A and B. Their results are used in our proof of the Odd Degree Extension Theorem, but they are of interest beyond that Theorem.

Basic notation. Throughout, R is a commutative associative unital ring. We do not assume that $2 \in R^\times$, unless this is explicitly stated so. Also, modules, quadratic forms and algebras will be defined over R . We use $R\text{-alg}$ to denote the category of commutative associative unital R -algebras.

Objects of $R\text{-alg}$ are sometimes also referred to as R -rings. If M is an R -module and $S \in R\text{-alg}$, we put $M_S = M \otimes_R S$.

We say an R -module M is finite projective if it is finitely generated projective (= locally free of finite rank). A finite R -algebra is an algebra $S \in R\text{-alg}$ whose underlying R -module is finitely generated, but not necessarily projective. A finite projective R -algebra is an R -ring S whose underlying R -module is finite projective. The norm of such an R -algebra S is denoted $N_{S/R}$. A finite projective R -algebra S is called finite étale if it is separable, see for example [Fo] or [Knu] for other equivalent definitions. We call $S \in R\text{-alg}$ an étale R -algebra of degree $d \in \mathbb{N}$ if S is a finite étale algebra whose underlying R -module is projective of constant rank d .

1. QUADRATIC FORMS

This section starts with a review of known facts on bilinear and quadratic forms over arbitrary rings, thereby also establishing our notation and terminology, 1.1–1.3. We study quadratic forms over semilocal rings in the second part of this section.

1.1. Quadratic and symmetric bilinear forms (terminology, basic facts). (a) A (*symmetric*) *bilinear module* is a pair (M, b) consisting of a finite projective R -module and a symmetric R -bilinear map $b: M \times M \rightarrow R$. We will only consider symmetric bilinear forms, and hence simply speak of bilinear modules. We use the symbol $(M, b) \cong (M', b')$ to denote isometric bilinear modules. When M is clear from the context or unimportant, we will sometimes write b for (M, b) . Given a bilinear module (M, b) , its *adjoint* is the R -linear map $b^*: M \rightarrow M^* = \text{Hom}_R(M, R)$, $m \mapsto b(m, \cdot)$. We call (M, b) *regular* if b^* is an isomorphism.

(b) A *quadratic module* is a pair (M, q) where M is a finite projective R -module and $q: M \rightarrow R$ is an R -quadratic form. We use b_q to denote the polar form of q . We call q or (M, q) *regular* if b_q is regular. As for bilinear modules, $(M, q) \cong (M', q')$ indicates isometric quadratic modules. We sometimes write q instead of (M, q) , if M is unimportant or clear from the context.

(c) (*Base change*) Let $S \in R\text{-alg}$, and let (M, b) be an R -bilinear module. There exists a unique S -bilinear form $b_S: M_S \times M_S \rightarrow S$ satisfying $b_S(s_1 \otimes m_1, m_2 \otimes s_2) = s_1 b(m_1, m_2) s_2$ for $m_i \in M$ and $s_i \in S$. Given an R -quadratic module (N, q) , there exists a unique S -quadratic form $q_S: N_S \rightarrow S$ satisfying $q_S(s \otimes n) = s^2 q(n)$ for $s \in S$ and $n \in N$. The polar of q_S is the base change of the polar of q . If (M, b) (or (N, q)) is regular, then so is (M_S, b_S) (respectively (N_S, q_S)).

(d) (*Tensor products*) Let (M_i, b_i) , $i = 1, 2$, be bilinear modules. There exists a unique symmetric bilinear form $b_1 \otimes b_2$ on $M_1 \otimes_R M_2$ satisfying $(b_1 \otimes b_2)(m_1 \otimes m_2, m'_1 \otimes m'_2) = b_1(m_1, m'_1) b_2(m_2, m'_2)$ for $m_i, m'_i \in M_i$. Given an R -bilinear module (M, b) and an R -quadratic form (N, q) , there

exists a unique R -quadratic form $b \otimes q: M \otimes_R N \rightarrow R$ satisfying

$$(1.1.1) \quad \begin{aligned} (b \otimes q)(m \otimes n) &= b(m, m)q(n), \text{ and} \\ b_{b \otimes q}(m \otimes n, m' \otimes n') &= b(m, m')b_q(n, n') \end{aligned}$$

for all $m, m' \in M$ and $n, n' \in N$, where b_q is the polar form of q . It is called the *tensor product of (M, b) and (N, q)* , [Sa, Thm. 1]. The polar form of $b \otimes q$ is the tensor product of the symmetric bilinear forms $b \otimes b_q$. If (M, b) and (N, q) are regular, then so is $(M, b) \otimes (N, q)$. The tensor product is compatible with base change: for $S \in R\text{-alg}$ we have

$$(M, b)_S \otimes_S (N, q)_S \xrightarrow{\sim} ((M, b) \otimes_R (N, q))_S$$

with respect to $m \otimes s_1 \otimes n \otimes s_2 \mapsto m \otimes m \otimes s_1 s_2$.

(e) Given a bilinear module (M, b) , the *orthogonal module* of a submodule $U \subset M$ is $U^\perp = \{m \in M : b(m, U) = 0\}$. We call U *totally isotropic* if $U \subset U^\perp$. A submodule U of a quadratic module (M, q) is *totally isotropic* if $q(U) = 0$, in which case U is also a totally isotropic submodule of (M, b_q) . If (M, b) is a bilinear module and $U \subset M$ is a submodule such that $(U, b|_U)$ is regular, then $M = U \oplus U^\perp$.

1.2. Nonsingular quadratic forms. Recall that the *radical* of a quadratic module (M, q) is $\text{rad}(M, q) = \{m \in M : q(m) = 0 = b_q(m, M)\}$. It is a submodule of M and satisfies $(\text{rad}(M, q))_S \subset \text{rad}((M, q)_S)$, $S \in R\text{-alg}$. We call (M, q) or simply q *nonsingular* if $\text{rad}((M, q)_F) = \{0\}$ for all fields $F \in R\text{-alg}$. A *quadratic space* is a quadratic module (M, q) with a nonsingular q . We will use the following properties of nonsingular forms (for details see the references in (a)).

(a) (*Comparison of terminology*) Our terminology of a regular bilinear form or regular quadratic form follows [Knu] and [Sch] (except that in these references “regular” and “nonsingular” are used interchangeably), but a regular bilinear form as defined here is called “non singular” in [Ba] and “nondegenerate” in [EKM]. A nonsingular quadratic form is called “nondegenerate” in [Co1], “nondegenerate” in [EKM], “semiregular” in [Knu] in case of odd rank, cf. (e), and “separable” in [Pe].

(b) A regular quadratic form is nonsingular, since $\text{rad}((M, q)_S) = 0$ for a regular form and any $S \in R\text{-alg}$ by (c).

(c) If $2 \in R^\times$, a nonsingular form is regular. Indeed, if $2 \in R^\times$, then $\text{rad}(q_S) = \{m \in M_S : b_{q_S}(m, M_S) = 0\}$, $S \in R\text{-alg}$, and so the adjoint of b_q is an isomorphism by Nakayama.

(d) If q is nonsingular, then so is q_S for any $S \in R\text{-alg}$.

(e) Let (M, q) be a quadratic module with M of constant even rank. Then q is nonsingular if and only if q is regular, cf. (h) below.

(f) A quadratic R -space (M, q) with M faithfully projective is *primitive* in the sense that $q(M)$ generates R as ideal. If R is semilocal, then $q(m) \in R^\times$ for some $m \in M$ (which is unimodular in the sense of 1.8).

(g) Let $(M, q) = (M_1, q_1) \perp (M_2, q_2)$ be a direct sum of quadratic modules. If q is nonsingular, then so are q_1 and q_2 . Conversely, if q_1 is regular, then q is nonsingular if and only if q_2 is nonsingular. If q_1 and q_2 are nonsingular, then q need not be nonsingular, see the example in 1.7.

(h) (*1-dimensional forms*) Let $u \in R^\times$. We define $\langle u \rangle_b: R \times R \rightarrow R$, $(r_1, r_2) \mapsto ur_1r_2$ and $\langle u \rangle_q: R \rightarrow R$, $r \mapsto ur^2$. Then $\langle u \rangle_b$ is a regular bilinear form. The polar of the quadratic form $\langle u \rangle_q$ is $2\langle u \rangle$, whence $\langle u \rangle_q$ is regular if and only if $2 \in R^\times$, but $\langle u \rangle_q$ is always nonsingular. We abbreviate $\langle u \rangle = \langle u \rangle_b$ if the meaning of $\langle u \rangle$ is clear from the context.

If (M, b) and (N, q) are bilinear and quadratic modules respectively, then

$$\langle 1 \rangle_b \otimes b \cong b, \quad \langle 1 \rangle_b \otimes q \cong q$$

under the standard isomorphism $R \otimes_R M \xrightarrow{\sim} M$. However, $b \otimes \langle 1 \rangle_q = b_q$, where $b_q: M \rightarrow R$, $m \mapsto b(m, m)$, is the quadratic form associated with b . Its polar is $b_{q_b} = 2b$.

(i) (*Reduction to constant rank*) Let $R = R_0 \times \cdots \times R_n$ be a direct product of rings. A quadratic module (M, q) over R uniquely decomposes as an orthogonal sum

$$(1.2.1) \quad (M, q) = (M_0, q_0) \perp \cdots \perp (M_n, q_n)$$

where each (M_i, q_i) is a quadratic module over R_i . Conversely, given quadratic R_i -modules (M_i, q_i) , the formula (1.2.1) defines a quadratic R -module. The quadratic module (M, q) is regular (nonsingular) if and only if all quadratic R_i -modules (M_i, q_i) are regular (nonsingular respectively).

For arbitrary R , a finite projective R -module M gives rise to a decomposition $R = R_0 \times \cdots \times R_n$ and hence to $M = M_0 \times \cdots \times M_n$ such that M_i is a projective R_i -module of constant rank i . The discussion above then describes the reduction of quadratic modules to quadratic modules of constant rank.

(j) (*Witt cancellation*) Let R be a semilocal ring, let q_1, q_2, q'_1 and q'_2 be quadratic forms where q_1 is regular and q_2 is nonsingular and of positive rank. If $q_1 \cong q'_1$ and $q_1 \perp q_2 \cong q'_1 \perp q'_2$, then $q_2 \cong q'_2$. Indeed, since the nonsingular form q_2 is primitive by (f), this follows from [Kne, Kürzungssatz]. Witt cancellation with all forms q_i and q'_i being regular, is proven in [Ba, III, (4.3)].

1.3. Metabolic and hyperbolic spaces. Let (U, b) be a bilinear module. The *metabolic space* associated with (U, b) is the bilinear module $\mathbb{M}(U, b) = (U \oplus U^*, b_{\mathbb{M}(U, b)})$ whose bilinear form $b_{\mathbb{M}(U, b)}$ is defined by

$$b_{\mathbb{M}(U, b)}(u + \varphi, v + \psi) = b(u, v) + \varphi(v) + \psi(u).$$

It is a regular bilinear form, justifying the terminology “space”. By definition, the *hyperbolic bilinear space* is $\mathbb{H}_b(U) = \mathbb{M}(U, 0)$ where 0 is the null form.

Given a finite projective R -module U , the associated *hyperbolic space* $\mathbb{H}(U)$ is the quadratic module $(U^* \oplus U, \text{hyp})$ with $\text{hyp}(\varphi \oplus u) = \varphi(u)$. The polar form of the hyperbolic quadratic form hyp is the bilinear form $b_{\mathbb{H}_b(U,0)}$, in particular, hyp is nonsingular. We call $\mathbb{H}(R)$ the *hyperbolic plane*.

We say a bilinear module (M, b) *metabolic* if there exists a bilinear module (U, b_U) such that $(M, b) \cong \mathbb{M}(U, b_U)$. The same terminology will be applied to hyperbolic quadratic spaces. The following facts are for example proven in [Ba, I, §3 and §4].

(a) Let (M, b) be a regular bilinear module and let $U \subset M$ be a totally isotropic complemented submodule. Then there exists a submodule $V \subset M$ such that $U \cap V = 0$, $(U \oplus V, b|_{U \oplus V})$ is metabolic and hence $M = (U \oplus V) \perp (U \oplus V)^\perp$. If $b(m_1, m_2) = b_0(m_1, m_2) + b_0(m_2, m_1)$ for some bilinear form $b_0: M \times M \rightarrow R$, one can choose V such that $(U \oplus V, b_{U \oplus V})$ is a hyperbolic bilinear space

(b) (*Characterization of metabolic spaces*) A regular bilinear module (M, b) is metabolic if and only if one of the following conditions holds:

- (i) M contains a totally isotropic complemented submodule V with $V = V^\perp$, a so-called *Lagrangian*,
- (ii) M contains a totally isotropic and complemented submodule U satisfying $\text{rank}_{\mathfrak{p}} M = 2 \text{rank}_{\mathfrak{p}} U$ for all $\mathfrak{p} \in \text{Spec}(R)$.

In this case $(M, b) \cong \mathbb{M}(U)$ for $U \cong V^*$. In particular, $\mathbb{M}(U)$ is free whenever V is free, and any decomposition $V = V_1 \oplus \cdots \oplus V_n$ gives rise to an decomposition $\mathbb{M}(U) = \mathbb{M}(U_1) \perp \cdots \perp \mathbb{M}(U_n)$ with $U_i \cong V_i^*$.

To see that M is metabolic in case (ii), apply (a) to get $M = (U \oplus V) \perp (U \oplus V)^\perp$ where $U \oplus V$ is metabolic and $\text{rank}_{\mathfrak{p}} = 2 \text{rank}_{\mathfrak{p}} U = \text{rank}_{\mathfrak{p}} M$, whence $(U \oplus V)^\perp = 0$. The last claim follows from $V^* = V_1^* \oplus \cdots \oplus V_n^*$.

In the remainder of this section we consider quadratic spaces (M, q) over R in two settings: (a) q is regular, and (b) R is semilocal. The results in case (a) are proven in [Ba, §3 and §4]. Since our techniques in case (b) easily also lead to proofs in the setting of (a), we prove (a) and (b) at the same time. We first recall a folklore result about lifting of subspaces in the semilocal setting. It is straightforward to prove or can be obtained by specializing the Reduction Theorem [Knu, II, (4.6.1)].

1.4. Lemma. *Let R be a semilocal ring, let M be a finite projective R -module and let $U \subset M$ be a complemented submodule. For a maximal ideal $\mathfrak{m} \triangleleft R$ we put $\kappa(\mathfrak{m}) = R/\mathfrak{m}$, $M(\mathfrak{m}) = M \otimes_R \kappa(\mathfrak{m}) = M/\mathfrak{m}M$, and analogously for $U(\mathfrak{m})$. We further assume that $r \in \mathbb{N}_+$ and that for every $\mathfrak{m} \in \text{Specmax}(R)$ there exists an r -dimensional subspace $W[\mathfrak{m}] \subset M(\mathfrak{m})$ with $U(\mathfrak{m}) \cap W[\mathfrak{m}] = \{0\}$.*

Then there exists a free submodule $W \subset M$ of rank r which satisfies $W(\mathfrak{m}) = W[\mathfrak{m}]$, $U \cap W = \{0\}$ and which has the property that $U \oplus W$ is complemented in M .

1.5. Proposition. *Let (M, q) be a quadratic space over R , let $U \subset M$ be a complemented totally isotropic submodule, and assume one of the following.*

- (a) q is regular, or
- (b) R is semilocal.

Then there exists a totally isotropic submodule $V \subset M$ such that $U \cap V = \{0\}$, $(U \oplus V, q_{U \oplus V}) \cong \mathbb{H}(U)$ and hence $M = (U \oplus V) \oplus (U \oplus V)^\perp$.

Proof. (I) (*Intermediate step*) Suppose there exists a submodule $W \subset M$ satisfying

$$(1.5.1) \quad \begin{aligned} &U \cap W = \{0\}, \text{ and for which the canonical map} \\ &\beta: U \xrightarrow{\sim} W^*, \quad u \mapsto (w \mapsto b_q(u, w)) \end{aligned}$$

is an isomorphism of R -modules. By [Ba, I, (1.7)], we can choose a not necessarily symmetric bilinear form b_0 satisfying $b_0(m, m) = q(m)$ for all $m \in M$. By (1.5.1), for every $w \in W$ there exists a unique $u_w \in U$ such that $b_q(u_w, w') = b_0(w, w')$ holds for all $w' \in W$. Because of uniqueness of the u_w , the map $U \rightarrow W$, $w \mapsto u_w$, is R -linear. Then $V = \{w - u_w : w \in W\} \cong W$ is a totally isotropic submodule: since $q(u_w) = 0$ we have

$$q(w - u_w) = q(w) - b_q(w, u_w) = b_0(w, w) - b_q(u_w, w) = 0.$$

Moreover, $U \cap V = 0$ and the canonical map $U \xrightarrow{\sim} V^*$, $u \mapsto (v \mapsto b_q(u, v))$ is an isomorphism. Hence $(U \oplus V, q|_{U \oplus V}) \cong \mathbb{H}(U)$. Since $\mathbb{H}(U)$ is a regular quadratic module, 1.1(e) applies and yields $M = (U \oplus V) \oplus (U \oplus V)^\perp$.

In the remainder of the proof we will establish the existence of a submodule W satisfying (1.5.1). We point out that (I) applies to the two cases (a) and (b).

(II) (*Case (a) in general and case (b) with R a field*) Let $U^\perp = \{m \in M : b_q(m, U) = 0\}$. We have a well-defined pairing

$$\alpha: U \times M/(U^\perp) \rightarrow R, \quad (u, \bar{m}) \mapsto b_q(u, m)$$

which is regular: if $\alpha(u, \bar{m}) = b_q(u, m) = 0$ for all $m \in M$, then $u \in \text{rad}(b_q)$. Hence $u = 0$ in case (a), while in case (b) we get $u \in \text{rad}(q)$ because $q(u) = 0$, so that again $u = 0$ follows, using that $\text{rad}(q) = 0$ if R is a field. Also, if $\alpha(U, \bar{m}) = b_q(U, m) = 0$, then $m \in U^\perp$, and therefore $\bar{m} = 0$ follows. We now get that α induces an isomorphism $\alpha^*: U \xrightarrow{\sim} (M/U^\perp)^*$. We claim that there exists a submodule $W \subset M$ such that $M = U^\perp \oplus W$, and therefore $\text{can}: W \xrightarrow{\sim} M/U^\perp$ under the canonical map. The existence of W follows in case (a) from [Ba, I, (3.2)(a)], saying that U^\perp is complemented in M . It is obvious in case (b) with R a field. Denoting by $\text{can}^*: (M/U^\perp)^* \xrightarrow{\sim} W^*$ the dual of the isomorphism can , we have $((\text{can}^* \circ \alpha^*)(u))(w) = \alpha^*(u)(\text{can}(w)) = \alpha^*(u)(\bar{w}) = b_q(u, w) = (\beta(u))(w)$, i.e., W satisfies (1.5.1). Now (I) finishes the proof in case (a), and in case (b) with R a field. Before we can deal with a semilocal R in case (b) we make a further reduction.

(III) (*Reduction to constant rank*) Since U is complemented, it is finitely generated projective. By 1.1(i), we can therefore decompose $R = R_1 \times \cdots \times R_n$ and correspondingly

$$(M, q) = (M_1, q_1) \perp \cdots \perp (M_n, q_n), \quad U = U_1 \times \cdots \times U_n$$

such that each $U_i \subset M_i$ is a complemented submodule of constant rank and a totally isotropic submodule of the R_i -quadratic space (M_i, q_i) . If $V_i \subset M_i$, $1 \leq i \leq n$, are submodules as in the claim of the lemma, then $V = V_1 \times \cdots \times V_n$ satisfies the conditions for (M, q) . Without loss of generality we can therefore assume that U has constant rank, say rank r . It is then free of rank r .

(IV) (*Case (b) in general*) By (III) we can assume that U is free of rank r . Using the notation of Lemma 1.4, we know that $q_{\kappa(\mathfrak{m})}$ is nonsingular by 1.2(d). Thus, by (II), the lemma holds for $\kappa(\mathfrak{m})$. We can therefore choose an r -dimensional subspace $W[\mathfrak{m}]$ such that $U(\mathfrak{m}) \cap W[\mathfrak{m}] = \{0\}$ and $U(\mathfrak{m}) \xrightarrow{\sim} W[\mathfrak{m}]^*$ via $b_{\kappa(\mathfrak{m})}$. By Lemma 1.4, the $W[\mathfrak{m}]$ lift to a submodule W satisfying $U \cap W = \{0\}$ and $W(\mathfrak{m}) = W[\mathfrak{m}]$. Moreover, the map $U \rightarrow W^*$, induced by b_q , is an isomorphism by Nakayama, since it is an isomorphism after passing to each $\kappa(\mathfrak{m})$. Again (I) finishes the proof. \square

1.6. Corollary (Characterization of hyperbolic spaces). *Let (M, q) be a quadratic R -space and assume that q is regular or that R is semilocal. Then the following are equivalent:*

- (i) (M, q) is hyperbolic;
- (ii) M admits a direct summand U satisfying $q(U) = 0$ and $2 \operatorname{rank}_{\mathfrak{p}} U = \operatorname{rank}_{\mathfrak{p}} M$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$;
- (iii) M admits a direct summand U satisfying $q(U) = 0$ and $U = U^\perp$.

In this case $(M, q) \cong \mathbb{H}(U)$.

Proof. (i) \implies (ii) being obvious because $\operatorname{rank}_{\mathfrak{p}} U = \operatorname{rank}_{\mathfrak{p}} U^*$, let us assume (ii) and prove (iii). By Proposition 1.5, there exists a submodule $V \subset M$ such that $(U \oplus V, q|_{U \oplus V}) \cong \mathbb{H}(U)$ is hyperbolic and $M = (U \oplus V) \oplus (U \oplus V)^\perp$. Since $V \cong U^*$ as R -modules, $\operatorname{rank}_{\mathfrak{p}}(U \oplus V) = \operatorname{rank}_{\mathfrak{p}} M$, whence $U \oplus V = M$ and $U^\perp = U \oplus (U^\perp \cap V)$ with $U^\perp \cap V \cong \{\varphi \in U^* : \varphi(U) = 0\} = \{0\}$. The proof of (iii) \implies (i) follows the same pattern. \square

1.7. Corollary. *Let (M, q) and (M', q') be regular quadratic modules.*

(a) [Ba, I, (4.7.i)] *If (M, q) and (M', q') are isometric, then the quadratic module $(M, q) \perp (M', -q')$ is hyperbolic: $(M, q) \perp (M', -q') \cong \mathbb{H}(M)$.*

(b) *Conversely, if R is semilocal and if $(M, q) \perp (M', -q') \cong \mathbb{H}(M)$, then $(M, q) \cong (M', q')$.*

Proof. (a) Let $f: (M, q) \rightarrow (M', q')$ be an isometry. The quadratic form $q \perp (-q')$ is regular. The diagonal submodule $U = \{(m, f(m)) : m \in M\} \subset M \oplus M'$ is complemented by $\{(m, 0) : m \in M\}$ and satisfies 1.6(ii). Hence $(M, q) \perp (M', -q') \cong \mathbb{H}(M)$.

(b) By (a), $(M, q) \perp (M, -q) \cong \mathbb{H}(M) \cong (M, q) \perp (M', -q')$. Hence $(M, -q) \cong (M' - q')$ by Witt cancellation 1.2(j), which implies our claim. \square

Corollary 1.7(a) is not true for nonsingular quadratic forms, even over fields. For example, let $(M, q) = (F, \langle u \rangle_q) = (M', q')$ with F a field of characteristic 2 and $u \in F^\times$. Then (M, q) is nonsingular by 1.2(h), but $0 \neq (1_F, 1_F) \in \text{rad}(q \perp (-q))$, so that $q \perp (-q)$ is singular, hence in particular not hyperbolic.

1.8. Unimodular and isotropic vectors. Let M be a finite projective R -module. For $x \in M$ and $\mathfrak{p} \in \text{Spec}(R)$ we put $x(\mathfrak{p}) = x \otimes_R 1_{\kappa(\mathfrak{p})}$. Recall that $u \in M$ is called *unimodular* if u satisfies one of the following equivalent conditions, see e.g. [Lo, 0.3]:

- (i) Ru is complemented and free of rank 1,
- (ii) there exists $\varphi \in M^*$ satisfying $\varphi(u) = 1$,
- (iii) $u(\mathfrak{p}) \neq 0$ for all $\mathfrak{p} \in \text{Spec}(R)$,
- (iv) $u(\mathfrak{m}) \neq 0$ for all maximal $\mathfrak{m} \in \text{Spec}(R)$.

Let (M, q) be a quadratic module. We call $m \in M$ *isotropic* if m is unimodular and $q(m) = 0$. We say (M, q) is *isotropic* if M contains an isotropic vector. We note some useful facts.

(a) If m is a unimodular (isotropic) vector of (M, q) , then $m \otimes 1_S$ is a unimodular (isotropic respectively) vector of $(M, q)_S$ for any $S \in R\text{-alg}$.

(b) Let $R[X]$ the polynomial ring over R in the variable X and let (M, q) be a quadratic module. For $v = v(X) \in M \otimes_R R[X]$ define the affine R -scheme

$$Z_v = \{x \in \mathbb{G}_{a,R} : v(x) = 0\},$$

whose T -points, $T \in R\text{-alg}$, is the set $Z_v(T) = \{t \in T : v(t) = 0\}$ where $v(t) \in M \otimes_R T$ is obtained by substituting t for X . Then

$$(1.8.1) \quad Z_v \text{ empty} \implies v \text{ unimodular.}$$

Indeed, if $\mathfrak{p} \in \text{Spec}(R[X])$, then $v(\mathfrak{p}) = v(X \otimes 1_{\kappa(\mathfrak{p})}) \neq 0$ since otherwise $X \otimes 1_{\kappa(\mathfrak{p})} \in Z_v(\kappa(\mathfrak{p}))$.

(c) Let (M, q) be a quadratic space over R and assume that q is regular or that R is semilocal. By Proposition 1.5, any isotropic vector embeds into a hyperbolic plane $\mathbb{H} = \mathbb{H}(R)$ and $(M, q) = \mathbb{H} \perp (M_1, q_1)$. In particular, $\text{rank}_{\mathfrak{p}} M \geq 2$ holds for every $\mathfrak{p} \in \text{Spec}(R)$.

(d) Let M be a projective R -module of constant rank 2 and let $q: M \rightarrow R$ be a nonsingular quadratic form. By 1.2(e), q is nonsingular if and only if q is regular. Hence, by (c), we have the implication “ \implies ” of

$$(1.8.2) \quad (M, q) \text{ isotropic} \iff (M, q) \cong \mathbb{H}(R).$$

Thus, in this case M is free of rank 2. The other direction in (1.8.2) holds because in $\mathbb{H}(R) = R \oplus R$ with the hyperbolic form hyp , given by $\text{hyp}(r_1, r_2) = r_1 r_2$, the vector $(1, 0)$ is isotropic.

2. SPRINGER'S ODD EXTENSION THEOREM

Let (M, q) be a quadratic module. To simplify notation, we will often abbreviate $q(x) = q_S(x)$ for $x \in M_S$ if S is clear from the context. We will also say that q is S -isotropic if q_S is isotropic, cf. 1.8. We recall that a quadratic space (M, q) is a quadratic module with a nonsingular q .

2.1. Theorem (Springer's Theorem). *Let R be a semilocal ring and let (M, q) be a quadratic space. Let S be a finite R -algebra of odd degree, which is étale or one-generated. If q is S -isotropic, then q is R -isotropic.*

The proof of this theorem will be given in 2.5. Lemma 2.2 proves Springer's Theorem in the case of rank $M = 2$. It involves a much weaker condition than R being semilocal or that S is one-generated or étale. By 1.2(e), a quadratic form on such an R -module M is nonsingular if and only if it is regular.

2.2. Lemma (Rank 2). *Let $S \in R\text{-alg}$ be a finite R -algebra of odd degree and let (M, q) be a quadratic space of constant rank 2, representing a unit in R . Then (M, q) is isotropic if and only if $(M, q)_S$ is isotropic.*

Proof. It is clear that (M, q) isotropic $\implies (M, q)_S$ isotropic. Let us therefore assume that $(M, q)_S$ is isotropic. Since q is isotropic if and only if uq is isotropic for some $u \in R^\times$, we may assume that q represents 1. It then follows from [Knu, V, (2.2.1)] that there exists a quadratic étale R -algebra A with norm n_A such that $(M, q) \cong (A, n_A)$ (in fact A is the even Clifford algebra of (M, q)). Without loss of generality, let $(M, q) = (A, n_A)$. By assumption, $(A, n_A)_S$ is isotropic, equivalently, $(n_A)_S = n_{A_S}$ is hyperbolic. Now recall [Knu, V, (2.2.4)]: a quadratic étale S -algebra has a hyperbolic norm if and only if A_S is split, i.e., $A_S \cong S \times S$ as S -algebra. It follows that A_S is split. By [Knu, III, (4.1.2)], the automorphism group scheme of the R -algebra A is the abelian constant group scheme $\mathbb{Z}/2\mathbb{Z}$. Since S has odd degree, we are in the setting of the Example in B.4. Thus (A, n_A) is split, i.e., n_A is isotropic. \square

We recall (1.8.2): under the assumption of Lemma 2.2, (M, q) is isotropic $\iff (M, q) \cong \mathbb{H}(R)$. The assumption that (M, q) represent a unit is always fulfilled if R is semilocal, see for example [Ba, Prop. I.3.4]. Our proof of Springer's Theorem also uses the following Lemma 2.3, a variation of [PR, Prop. 1.1].

2.3. Lemma. *Let k be a field, let (V, q) be an isotropic quadratic k -space of dimension $r \geq 3$, and let $P = P(X) \in k[X]$ be a monic polynomial of degree $d \geq 1$. Then there exists $v = v(X) \in V \otimes_k k[X]$ satisfying the following conditions:*

- (i) $q(v(X)) \in k[X]$ is a polynomial of degree $2d - 2$, which is divisible by P ;
- (ii) the k -scheme $Z_{v(X)} = \{x \in \mathbb{G}_a : v(x) = 0\}$ is empty.

In particular, $v(X)$ is unimodular.

Proof. Since q is isotropic, (V, q) contains a hyperbolic plane \mathbb{H} and $(V, q) = \mathbb{H} \perp (W, q|_W)$ for $(W, q|_W) = \mathbb{H}^\perp$, see 1.8(c) or [EKM, 7.13]. The quadratic module $(W, q|_W)$ contains $w \in W$ with $q(w) = a \in k^\times$. In view of our claims, it is then no harm to replace V by $\mathbb{H} \oplus ka$. Thus q is given by $q(x, y, z) = xy + az^2$, which is nonsingular by 1.2(g) and 1.2(h) (but not regular in characteristic 2).

By the Euclidean division algorithm there exist unique polynomials $Q(X) \in k[X]$ of degree $d - 2$ and $R(X)$ of degree $\leq d - 1$ such that $X^{2d-2} = P(X)Q(X) + R(X)$. We define $v(X) = (-a, R(X), X^{d-1}) \in V \otimes k[X]$. Then $q(v(X)) = -aR(X) + aX^{2d-2} = aP(X)Q(X)$. Thus, the condition (i) is fulfilled with $q(v(X)) = aP(X)Q(X)$. Since the first component of $v(X)$ is $-a$, the condition (ii) is satisfied too. It implies unimodularity of $v(X)$ by (1.8.1). \square

2.4. Consequences of Lemma 2.3. As motivation for step (III) in the proof of Theorem 2.1 below, we discuss some consequences of Lemma 2.3. Step (III) will be more technical, but uses the same ideas. Let us put

$$S = k[X]/(P), \quad \theta = X + (P) \in S.$$

Then S is one-generated with θ as primitive element. The element $v(\theta) \in (V \otimes_k k[X]) \otimes_{k[X]} S = V \otimes_k S$ is unimodular since it is obtained from the unimodular $v(X)$ by base change, see 1.8(a), and it satisfies $q(v(\theta)) = 0$ by condition (i) of 2.3, i.e., $v(\theta)$ is an isotropic vector in $V \otimes_k S$.

Again by condition (i) of 2.3, there exists $u \in k^\times$ and $Q(X) \in k[X]$ of degree $d - 2$ such that $q(v(X)) = uP(X)Q(X) \in k[X]$. Let

$$T = k[X]/(Q), \quad \vartheta = X + (Q) \in T.$$

Then T is one-generated of degree $d - 2$ with primitive element ϑ . The same arguments showing that $v(\theta)$ is an isotropic vector proves that $v(\vartheta) \in V \otimes_k T$ is isotropic.

In step (III) of the proof of Theorem 2.1 we will know that $V \otimes_k S$ is isotropic and use a refinement of the argument above to conclude that $V \otimes_k T$ is isotropic, the point being that $\deg T = \deg S - 2$.

2.5. Proof of Theorem 2.1. (I) *Reduction to M free of rank $r \geq 3$.* Let $R = R_0 \times \cdots \times R_n$ and $(M, q) = (M_0, q_0) \perp \cdots \perp (M_n, q_n)$ be the rank decomposition of (M, q) as in 1.1(i). Thus, M_i is a projective R_i -module of rank i and each $q_i: M_i \rightarrow R_i$ is a nonsingular quadratic form. The R -algebra S decomposes correspondingly, $S = S_0 \times \cdots \times S_n$ where each S_i is a finite R_i -algebra of degree $d = \deg S$. We have

$$M \otimes_R S \cong (M_0 \otimes_{R_0} S_0) \times \cdots \times (M_n \otimes_{R_n} S_n)$$

with each $M_i \otimes_{R_i} S_i$ being projective of rank i as S_i -module. Since $q_{M \otimes_R S}$ is isotropic, so is every $q_{M_i \otimes_{R_i} S_i}$. By 1.8(c), $M_i \otimes_{R_i} S_i = 0$ for $i = 0, 1$. Since

in both cases (S one-generated or S étale) the R_i -modules S_i are faithfully flat, we get $M_0 = 0 = M_1$ and $R_0 = 0 = R_1$.

In the decomposition $R = R_2 \times \cdots \times R_n$, each R_i is a semilocal ring. We have already observed that $(M, q)_S$ is isotropic if and only if every $M_i \otimes_{R_i} S_i$ is isotropic. Since the analogous fact holds for (M, q) , it suffices to prove that every (M_i, q_i) is isotropic. Thus, without loss of generality, we can assume that M has constant rank $r \geq 2$. The case $r = 2$ has been dealt with in Lemma 2.2. We can therefore assume that M has rank $r \geq 3$. Since R is semilocal, this implies that M is free of rank r .

(II) $R = k$ is a field and S is one-generated. In this case $S \cong k[X]/P$ for some monic $P \in k[X]$. Let $P = P_1^{e_1} \cdots P_n^{e_n}$ be the prime factor decomposition of P in $k[X]$, and put $L_i = k[X]/P_i$. Since $d = \dim_k S = \sum_i e_i [L_i : k]$ is odd, one of the $[L_i : k]$ is odd. Then $L = L_i \in S\text{-alg}$ and thus $q_L = (q_S) \otimes_S L$ is isotropic. Since L/k has odd degree, the classical Springer Odd Degree Extension Theorem [EKM, Cor. 18.5] says that q is isotropic.

(III) R semilocal and S is one-generated. As before, let $S = R[X]/(P)$ where $P \in R[X]$ is a monic polynomial of degree d . We denote by $\kappa_1, \dots, \kappa_c$ the residue fields of R . For each i , $1 \leq i \leq c$, the κ_i -algebra $S_{\kappa_i} = S \otimes_R \kappa_i$ is one-generated, namely $S_{\kappa_i} = \kappa_i[X]/P_{\kappa_i}$ for $P_{\kappa_i} = P \otimes_R 1_{\kappa_i}$, and of odd degree d . Since q is S -isotropic, it is also $S \otimes_R \kappa_i$ -isotropic. The case (II) then shows that q_{κ_i} is isotropic. Now Lemma 2.3 provides unimodular elements $v_i(X) \in (M \otimes_R \kappa_i) \otimes_{\kappa_i} \kappa_i[X] = M \otimes_R \kappa_i[X]$ such that $q(v_i(X))$ is the product of a unit in κ_i^\times and a monic polynomial of degree $2d - 2$ which is divisible by P_{κ_i} and has the property that the κ_i -scheme

$$Z_{v_i} = \{x \in \mathbb{G}_{a, \kappa_i} : v_i(x) = 0\} \text{ is empty.}$$

Let $\theta = X + (P) \in S$ and denote by θ_i its image in S_{κ_i} . Then $v_i(\theta_i)$ is obtained from the unimodular $v_i(X)$ by base change and is therefore unimodular. It also satisfies $q(v_i(\theta_i)) = 0$ since $q(v_i(X))$ is divisible by P_{κ_i} . In other words, $v_i(\theta_i)$ is an S_{κ_i} -isotropic vector.

According to Corollary A.6 of the appendix, the $v_i(\theta_i)'s \in M \otimes_R S_{\kappa_i}$ lift to an isotropic $v \in M \otimes_R S$. We decompose $v = m_0 + m_1\theta + \cdots + m_{d-1}\theta^{d-1}$ where the m_j 's belong to M , and define $v(X) = m_0 + m_1X + \cdots + m_{d-1}X^{d-1} \in M \otimes_R R[X]$. By construction $q(v(X)) \in P(X)R[X]$ is a polynomial of degree $\leq 2d - 2$. Since the specialization to each $\kappa_i[X]$ is of degree $2d - 2$, it follows that $q(v(X))$ is the product of a unit $u \in R^\times$ and a monic polynomial of degree $2d - 2$. Summarizing, we have that $q(v(X)) = u P(X) Q(X)$ with $Q(X)$ monic of degree $d - 2$ and $u \in R^\times$.

Since $Z_{v_i} = \{t \in \mathbb{G}_{a, \kappa_i} : v_i(t) = 0\}$ is empty for each i , it follows that $Z_v = \{x \in \mathbb{G}_{a, R} : v(x) = 0\}$ is empty too. We define $T = R[X]/Q(X)$. Then $w = v(X)$ modulo Q is an isotropic vector of M_T . Thus, q is T -isotropic with T one-generated of degree $d - 2$. We continue the induction until we reach $d - 2 = 1$ and can conclude that M is isotropic.

(IV) S is étale. According to [BFP, Prop. 7.3] there exists a finite étale R -algebra T of odd degree such that $S \otimes_R T$ is one-generated as R -algebra. The paper [BFP] assumes throughout that $2 \in R^\times$, but the proof of the quoted proposition works for arbitrary R .

Since q is S -isotropic, it is a fortiori $S \otimes_R T$ -isotropic. Since $S \otimes_R T$ has odd degree, the preceding case (III) shows that q is isotropic. \square

As in the case of fields, see e.g. [Sch, II], Theorem 2.1 has a number of consequences worth stating. First, by 1.8(c), Springer's Theorem says: if $(M, q)_S$ contains a hyperbolic plane \mathbb{H} , then so does (M, q) . Corollary 2.6 says that this is true for arbitrary hyperbolic spaces. We say a quadratic module (M, q) contains a quadratic module (M_1, q_1) if there exists a complemented submodule $N \subset M$ such that $(M_1, q_1) \cong (N, q|_N)$. In this case, we usually identify $(M_1, q_1) = (N, q|_N)$. We recall that if (M_1, q_1) is regular, e.g., a hyperbolic space, then $(M, q) = (M_1, q_1) \perp (M_1, q_1)^\perp$ by 1.1(e).

2.6. Corollary. *Let R, S and (M, q) be as in Theorem 2.1. If $(M, q)_S$ contains a hyperbolic space $\mathbb{H}(N')$ with N' projective of constant rank r , then (M, q) contains a hyperbolic space $\mathbb{H}(N)$ with N projective of rank r .*

Proof. Recall ([Kmu, V, (1.1.1)]) that S is semilocal and that a projective module of constant rank over a semilocal ring is free. We can of course assume that $r > 0$ and that M has constant rank, cf. 1.2(i). It follows that $(M, q)_S$ is isotropic. Hence, by Springer's Theorem 2.1, the quadratic module (M, q) contains an isotropic vector e . By 1.8(c) we then have a decomposition $(M, q) = \mathbb{H}(Re) \perp (M_1, q_1)$ where (M_1, q_1) is a quadratic space by 1.2(g). If $(M_1, q_1) = 0$, we are done. Otherwise, M_1 has positive rank. Also, $\mathbb{H}(Se) \perp (M_1, q_1)_S = (M, q)_S \cong \mathbb{H}(N') \perp \mathbb{H}(N')^\perp$. Since N' is free, it decomposes as $N' \cong Re' \oplus N'_1$ where e' is isotropic and N'_1 is a totally isotropic submodule of rank $r - 1$. Therefore

$$\mathbb{H}(Se) \perp (M_1, q_1)_S = (M, q)_S \cong \mathbb{H}(Se') \perp (\mathbb{H}(N'_1) \perp \mathbb{H}(N')^\perp).$$

Since $\mathbb{H}(Se)$ is regular and $(M_1, q_1)_S$ is nonsingular and of positive rank, we can cancel $\mathbb{H}(Se) \cong \mathbb{H}(Se')$ using 1.2(j). We find that the nonsingular quadratic module (M_1, q_1) satisfies the assumption of the corollary with r replaced by $r - 1$. We then continue by induction on r . \square

2.7. Corollary. *Let R, S and (M, q) be as in Theorem 2.1, let (M_1, q_1) be a regular quadratic R -module such that $(M_1, q_1)_S$ is contained in $(M, q)_S$. Then (M_1, q_1) is contained in (M, q) .*

Proof. We apply the rank decomposition 1.2(i) to (M_1, q_1) and can then without loss of generality assume that (M_1, q_1) has constant rank. Since $(M_1, q_1)_S$ is regular, the nonsingular quadratic S -space $(M, q)_S$ decomposes,

$$(M, q)_S \cong (M_1, q_1)_S \perp (M'_2, q'_2)$$

where (M'_2, q'_2) is a nonsingular S -space by 1.2(g). By Corollary 1.7, the quadratic S -module $q_S \perp (-q_1)_S$ contains a hyperbolic S -space isometric

to $\mathbb{H}(M_{1,S})$. Hence by Corollary 2.6, there exists a nonsingular quadratic R -module (M_2, q_2) such that

$$q \perp (-q_1) \cong \mathbb{H}(M_1) \perp q_2 \cong q_1 \perp (-q_1) \perp q_2.$$

Canceling $-q_1$ by Witt cancellation 1.2(j), yields the result. \square

For easier reference, we explicitly state the case $(M_1, q)_S \cong (M_1, q_1)_S$ in the following Corollary 2.8. The case (iii) is obtained by writing S/R as a finite tower of odd one-generated (= simple) field extensions.

2.8. Corollary. *Let R be a semilocal ring, let q and q' be regular R -quadratic forms, and let $S \in R\text{-alg}$ be a finite R -algebra of odd degree which satisfies one of the following conditions,*

- (i) S is a one-generated R -algebra, or
- (ii) S is an étale R -algebra, or
- (iii) R is a field and S/R is a field extension.

Then

$$q_S \cong q'_S \iff q \cong q'.$$

In Corollary 2.9, $\widehat{W}_q(R)$ and $W_q(R)$ denote the Witt-Grothendieck ring and Witt ring of regular quadratic R -modules respectively, as for example defined in [Ba, I, §2, §4]. These are commutative associative rings without a multiplicative identity if $2 \notin R^\times$. The proof of 2.9 is standard, using Corollary 2.7.

2.9. Corollary. *Let R be a semilocal ring and let $S \in R\text{-alg}$ be a finite R -algebra of odd degree, which is one-generated or étale. Then the maps*

$$(2.9.1) \quad \widehat{W}_q(R) \longrightarrow \widehat{W}_q(S) \quad \text{and} \quad W_q(R) \longrightarrow W_q(S),$$

induced by $[q] \mapsto [q_S]$, are monomorphisms.

Corollary 2.9 was established in [Ba, V, Thm.6.9] for Frobenius extensions, based on a detailed study of torsion in the kernels of the maps in (2.9.1) and in this way avoiding Springer's Theorem, which is not proven in [Ba].

2.10. Set of values. By definition, the *set of values* $D(q)$ of a quadratic module (M, q) is

$$D(q) = q(M) \cap R^\times.$$

We will use the following elementary facts.

(a) The set of values is stable under base change: if $S \in R\text{-alg}$, then $D(q) \otimes 1_S \subset D(q_S)$.

(b) If q contains a hyperbolic plane, then $D(q) = R^\times$. Recall from 1.8(c) that q contains a hyperbolic plane whenever (M, q) is an isotropic quadratic space and R is semilocal or q is regular.

(c) (*Direct products*) Let $R = R_1 \times R_2$ be a direct product. By 1.2(i), the quadratic module (M, q) uniquely decomposes as $(M, q) = (M_1, q_1) \times$

(M_2, q_2) where (M_i, q_i) , $i = 1, 2$, is a quadratic R_i -module, which is nonsingular if (M, q) is so. We have $D(q) = D(q_1) \times D(q_2)$. An $S \in R\text{-alg}$ which is projective of rank $d \in \mathbb{N}_+$ uniquely decomposes as $S = S_1 \times S_2$ where each S_i is a projective R_i -module of rank d . In view of 1.2(i), this shows that the determination of $D(q)$ can often be reduced to that of $D(q)$ where (M, q) has constant rank.

(d) Let $(M, q) = (R, \langle u \rangle)$ with $u \in R^\times$. Then $D(q) = uR^{\times 2}$. For any $S \in R\text{-alg}$ which is projective of odd rank d we have

$$(2.10.1) \quad a \otimes 1_S \in D(q_S) \iff a \in D(q).$$

By (a) we only need to prove “ \implies ”. We have $D(q_S) = (u \otimes 1_S) S^{\times 2}$, and if $a \otimes 1_S = (u \otimes 1_S) s^2$ for some $s \in S$, then $a^d = N_{S/R}(a \otimes 1_S) = u^d N_{S/R}(s)^2$. Since $a^d \in aR^{\times 2}$ and $u^d \in uR^{\times 2}$, we get $a \in uR^{\times 2} = D(q)$.

In the following Corollary 2.11 we will prove (2.10.1) for more general nonsingular forms.

2.11. Corollary. *Let R be a semilocal ring, let $a \in R^\times$ and let (M, q) be a quadratic space for which $q' = q \perp \langle -a \rangle$ is nonsingular, cf. 1.2(g). Furthermore, let $S \in R\text{-alg}$ be a finite R -algebra of odd degree which is étale or one-generated. Then*

$$(2.11.1) \quad a \otimes 1_S \in D(q_S) \iff a \in D(q).$$

This is a well-known result in case R is a field of characteristic $\neq 2$ and S/R is an extension field, see for example [Lam, VII, Cor. 2.9]. In this case, no assumption on q' is necessary.

Proof. We will of course only prove “ \implies ”. By 2.10(c) and 2.10(d) we can assume that M has constant rank ≥ 2 . The assumption implies that q'_S contains an isotropic vector $(x, 1)$ for some $x \in M_S$. Hence, by Theorem 2.1 for q' , we get that q' is R -isotropic, i.e., there exists $m \in M$ and $r \in R$ such that $(m, r) \in M \oplus R$ is unimodular and satisfies $q(m) = ar^2$. At this point, two cases are clear:

- (i) $r = 0$: Then $m \in M$ is an isotropic vector of q . Hence, by 1.8(c), (M, q) contains a hyperbolic plane and then we are done by 2.10(b).
- (ii) $r \in R^\times$: Then $a = q(r^{-1}m)$ and we are again done.

In particular, (2.11.1) holds in case R is a field. For general R we will choose an isotropic vector of q' more carefully.

Let $\mathfrak{m} \triangleleft R$ be a maximal ideal of R with residue field $\kappa = R/\mathfrak{m}$, and put $S \otimes_R \kappa = S/\mathfrak{m}S$. We thus have extensions

$$\begin{array}{ccc} S & \longrightarrow & S \otimes_R \kappa \\ \uparrow & & \uparrow \\ R & \longrightarrow & \kappa \end{array} .$$

Since nonsingularity is inherited by extensions and since $(S \otimes_R \kappa)/\kappa$ has odd degree and is étale or one-generated, the field case applies and yields the

existence of $m_\kappa \in M \otimes_R \kappa$ satisfying $q_\kappa(m_\kappa) = a \otimes 1_\kappa$. In this way we obtain a family $(v_{\mathfrak{m}})_{\mathfrak{m} \in \text{Specmax}(R)}$ of isotropic vectors $v_{\mathfrak{m}} = (m_\kappa, 1_\kappa) \in (M \oplus R)_\kappa$. By Corollary A.6, we then get an isotropic element $v = (x, r) \in M \oplus R$ that lifts the $v_{\mathfrak{m}}$'s. In particular, $r_\kappa = 1_\kappa$ for every residue field κ of R . This implies $r \in R^\times$. So we are done by (ii) above. \square

APPENDIX A. LIFTING ISOTROPIC ELEMENTS

The goal of this appendix is Corollary A.6, which gives a criterion for lifting isotropic elements from localisations. We obtain this as a consequence of a surjectivity result for localizations of quadrics (Proposition A.5), which in turn is a special case of Demazure's fundamental Conjugacy Theorem, proven in [SGA3, XXVI] and re-stated below.

If $C \in R\text{-alg}$ and $\mathfrak{m} \triangleleft R$ is a maximal ideal of R we abbreviate $C/\mathfrak{m} := C/\mathfrak{m}C$. We use the terms *reductive (semisimple) group scheme* and *parabolic subgroup scheme* as defined in [SGA3, Tome III], but refer to a group scheme over $\text{Spec}(R)$ as an R -group scheme. We furthermore use the setting and the results of [SGA3, XXVI.3] for schemes of parabolic subgroup schemes.

A.1. Theorem (Demazure's Conjugacy Theorem). *Let R be a semilocal ring and let \mathbf{G} be a reductive R -group scheme. Denote by $\text{Dyn}(\mathbf{G})$ its Dynkin R -scheme (which is finite étale) and by $\text{Of}(\text{Dyn}(\mathbf{G}))$ the R -scheme of clopen subsets of $\text{Dyn}(\mathbf{G})$. Let $t \in \text{Of}(\text{Dyn}(\mathbf{G}))(R)$ be a type of parabolic subgroups and denote by $\mathbf{X} = \text{Par}(\mathbf{G})_t$ the R -scheme of parabolic subgroups of type t . Then the following hold.*

- (a) $\mathbf{G}(R)$ acts transitively on $\mathbf{X}(R)$.
- (b) If S is a finite R -algebra such that $\mathbf{X}(S) \neq \emptyset$, the map

$$\mathbf{X}(S) \longrightarrow \prod_{\mathfrak{m} \in \text{Specmax}(S)} \mathbf{X}(S/\mathfrak{m})$$

is onto.

Proof. (a) If $\mathbf{X}(R) = \emptyset$, the statement is obvious. We can thus assume that $\mathbf{X}(R) \neq \emptyset$ and pick a point $x \in \mathbf{X}(R)$; this corresponds to an R -parabolic subgroup \mathbf{P} of \mathbf{G} of type t . According to [SGA3, XXVI.4.3.5], \mathbf{G} admits a parabolic subgroup \mathbf{P}' opposite to \mathbf{P} . Corollary 5.2. of *loc. cit.* then says in particular that $\mathbf{X}(R) = \mathbf{G}(R)/\mathbf{P}(R)$. Thus $\mathbf{G}(R)$ acts transitively on $\mathbf{X}(R)$.

(b) Recall that S is semilocal, for example by [Knu, VI, (1.1.1)]. Our assumption is that \mathbf{G}_S admits an S -parabolic subgroup scheme \mathbf{Q} of type t . As noted in (a), it admits an opposite parabolic S -subgroup \mathbf{Q}' . According to [SGA3, XXVI.5.2], the product $\text{rad}_u(\mathbf{Q})(S) \times \text{rad}_u(\mathbf{Q}')(S) \rightarrow \mathbf{X}(S)$ is surjective (here $\text{rad}_u(\cdot)$ denotes the unipotent radical). Applying this for the semilocal ring S as well as for the semilocal ring S/\mathfrak{m} , $\mathfrak{m} \in \text{Specmax}(R)$,

shows that the horizontal maps in the commutative diagram below are surjective:

$$\begin{array}{ccc} \mathrm{rad}_u(\mathbf{Q})(S) \times \mathrm{rad}_u(\mathbf{Q}')(S) & \longrightarrow & \mathbf{X}(S) \\ \downarrow & & \downarrow \\ \prod_{\mathfrak{m}} \mathrm{rad}_u(\mathbf{Q})(S/\mathfrak{m}) \times \mathrm{rad}_u(\mathbf{Q}')(S/\mathfrak{m}) & \longrightarrow & \prod_{\mathfrak{m}} \mathbf{X}(S/\mathfrak{m}) \end{array}$$

Since $\prod_{\mathfrak{m}} S/\mathfrak{m} \cong \prod_{\mathfrak{m}} S \otimes_R (R/\mathfrak{m}) \cong S \otimes_R (R/\mathrm{Jac}(R)) \cong S/\mathrm{Jac}(R)S$, where $\mathrm{Jac}(R)$ denotes the Jacobson radical of R , the map $S \rightarrow \prod_{\mathfrak{m}} S/\mathfrak{m}$ is onto. On the other hand, the S -scheme $\mathrm{rad}_u(\mathbf{Q})$ (respectively $\mathrm{rad}_u(\mathbf{Q}')$) is isomorphic to a vector S -group scheme [SGA3, XXVI.2.5], so that the left vertical map is onto. Hence, by a simple diagram chase the right vertical map is onto too. \square

A.2. Corollary. *We use the notation of A.1, except that R need not be semilocal, but can be arbitrary. In particular, \mathbf{G} is a reductive R -group scheme and x, y are parabolic subgroups in $\mathbf{X}(R)$.*

Then there exist $f_1, \dots, f_n \in R$ satisfying $f_1 + \dots + f_n = 1$ and $y_{R_{f_i}} \in \mathbf{G}(R_{f_i}) \cdot x_{R_{f_i}}$ for $i = 1, \dots, n$. In other words, x and y are locally \mathbf{G} -conjugated for the Zariski topology on R .

Proof. The group \mathbf{G} is an R -group of type (RR) by [SGA3, XXII.5.1.3] and the points x, y of $\mathbf{X}(R)$ are parabolic subgroups, hence subgroups of type (R) by 5.2.3 of *loc. cit.*. It then follows from Theorem 5.3.9 of *loc. cit.* that the strict transporter \mathbf{T} , defined by

$$\mathbf{T}(S) = \{g \in \mathbf{G}(S) : g \cdot x_S = y_S\} \quad (S \in R\text{-alg}),$$

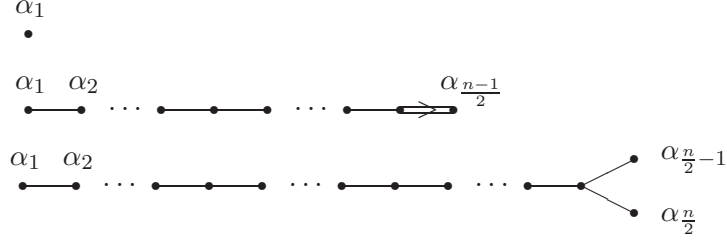
is a finitely presented affine R -scheme (among other properties). Since $\mathbf{T}(R_{\mathfrak{m}}) \neq \emptyset$ for any maximal $\mathfrak{m} \in \mathrm{Spec}(R)$ by A.1(a), the claim follows from Lemma A.3 below. \square

A.3. Lemma. *Let R be arbitrary and let \mathbf{T} be an R -scheme which is locally of finite presentation. If $\mathbf{T}(R_{\mathfrak{m}}) \neq \emptyset$ for all maximal $\mathfrak{m} \in \mathrm{Spec}(R)$, then there exists a Zariski cover (f_1, \dots, f_n) of R for which $\mathbf{T}(R_{f_i}) \neq \emptyset$ for all i , $1 \leq i \leq n$.*

Proof. Fix a maximal $\mathfrak{m} \in \mathrm{Spec}(R)$. Then $R_{\mathfrak{m}} = \varinjlim_{f \notin \mathfrak{m}} R_f$, hence $\mathrm{Spec}(R) = \varprojlim_{f \notin \mathfrak{m}} \mathrm{Spec}(R_f)$ and so $\mathbf{T}(R_{\mathfrak{m}}) = \varinjlim_{f \notin \mathfrak{m}} \mathbf{T}(R_f)$, according to [St, Tag 01ZC]. It follows that there exists $f_{\mathfrak{m}} \in R \setminus \mathfrak{m}$ such that $\mathbf{T}(R_{f_{\mathfrak{m}}}) \neq \emptyset$. The $f_{\mathfrak{m}}$'s for \mathfrak{m} running over the maximal ideals of R generate R as ideal. Hence, there exists finitely many maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ such that $R = R_{f_{\mathfrak{m}_1}} + \dots + R_{f_{\mathfrak{m}_n}}$. \square

A.4. An important special case of Theorem A.1 and Corollary A.2 is that of quadrics elaborated below. Let us explain some notation. We let (M, q) be a quadratic space with M of constant rank n . The associated special

orthogonal group scheme $\mathbf{G} = \mathbf{SO}(q)$ is defined in [Co1, C.2.10]. It is a semisimple R -group scheme of type A_1 for $n = 3$, of type $B_{(n-1)/2}$ for odd $n \geq 5$ and of type $D_{n/2}$ for even $n \geq 4$. We use Bourbaki's enumeration of the corresponding Dynkin diagrams:



We also use the projective space $\mathbb{P}(M^\vee)$ with Grothendieck's convention, i.e., $\mathbb{P}(M^\vee)(S)$, $S \in R\text{-alg}$, corresponds to the direct summands D of M_S which are locally free of rank 1. The quadric \mathbf{Q} defined by $q = 0$ consists of those D in $\mathbb{P}(M^\vee)(S)$ with $q(D) = 0$. For $D \in \mathbf{Q}(R)$ we let \mathbf{P} be the R -subgroup scheme of \mathbf{G} which stabilizes D . Finally, we remind the reader of our abbreviation $S/\mathfrak{m} = S/\mathfrak{m}S$ for $S \in R\text{-alg}$ and $\mathfrak{m} \in \text{Specmax}(R)$.

A.5. Proposition. *We use the notation of A.4. Then the following hold.*

- (a) (i) \mathbf{P} is a parabolic R -subgroup of \mathbf{G} .
 - (ii) The orbit map $\mathbf{G} \rightarrow \mathbb{P}(M^\vee)$, $g \rightarrow g.[D]$, induces an isomorphism $\mathbf{G}/\mathbf{P} \xrightarrow{\sim} \mathbf{Q}$ of R -schemes.
 - (iii) \mathbf{Q} is \mathbf{G} -isomorphic to $\text{Par}(\mathbf{G})_{t_1}$ where the type t_1 is constant and of value $\text{Dyn}(G)(R) \setminus \{\alpha_1\}_R$ with the enumeration of the respective Dynkin diagrams displayed above.
- (b) Let R be semilocal. Then
- (i) $\mathbf{G}(R)$ acts transitively on $\mathbf{Q}(R)$, and
 - (ii) if S is a finite R -algebra such that $\mathbf{Q}(S) \neq \emptyset$, then

$$(A.5.1) \quad \mathbf{Q}(S) \longrightarrow \prod_{\mathfrak{m} \in \text{Specmax}(R)} \mathbf{Q}(S/\mathfrak{m})$$

is onto.

Proof. We prove only the even rank case, the odd case being analogous.

(a) We observe that the claims hold over a field [Co2, Th. 3.9.(i)] and also that they are local for the flat topology. According to [Co1, Lemma C.2.1] or [Knu, IV, (3.2.1)], we may assume that (M, q) is the standard hyperbolic quadratic R -form over R^{2n} ($n \geq 2$), defined by $q(x_1, \dots, x_n, y_1, \dots, y_n) = x_1y_1 + \dots + x_ny_n$.

We first consider the case $D = Rp$ where $p = (1, 0, \dots, 0, 0, \dots, 0)$, and denote by \mathbf{P}_p the corresponding subgroup scheme. This permits us to assume $R = \mathbb{Z}$. Then \mathbf{P}_p is an affine finitely presented \mathbb{Z} -group scheme whose algebraically closed fibers are smooth connected and of dimension $2n - 2$. By

[AG, Lemma B.1], \mathbf{P}_p is smooth. Since the geometric fibers of \mathbf{P}_p are parabolic subgroups, \mathbf{P}_p is parabolic too. The induced orbit map $f : \mathbf{G}/\mathbf{P}_p \rightarrow \mathbf{Q}$ is a monomorphism. The field case ensures that this is a fiberwise isomorphism. Since \mathbf{G}/\mathbf{P}_p is flat and of finite presentation, the fiberwise isomorphism criterion [EGA, IV₄, 17.9.5] enables us to conclude that f is an isomorphism. It follows that \mathbf{Q} is homogeneous under \mathbf{G} . Thus (i) and (ii) hold for the special p .

Let us now deal with the general case. Since \mathbf{G} -homogeneity is a local property with respect to the flat topology, \mathbf{Q} is homogeneous under \mathbf{G} . The case of a general D then follows from the observation that D is locally \mathbf{G} -conjugated to $R\rho$ in the Zariski topology by applying Corollary A.2 to \mathbf{Q} . This proves (i) and (ii) in general.

(iii) We first deal with the special p above. We have an isomorphism $\mathbf{G}/\mathbf{P} \cong \mathbf{Q}$. On the other hand, according to [SGA3, XXVI.3.6], we have a \mathbf{G} -isomorphism $\mathbf{G}/\mathbf{P} \xrightarrow{\sim} \text{Par}(\mathbf{G})_{t(\mathbf{P})}$, hence an \mathbf{G} -isomorphism $\mathbf{Q} \xrightarrow{\sim} \text{Par}(\mathbf{G})_{t(\mathbf{P})}$. This isomorphism applies a point $x \in \mathbf{Q}(R)$ to the stabilizer \mathbf{G}_x , so is a canonical isomorphism. Here $t(\mathbf{P}) \in \text{Of}(\text{Dyn}(\mathbf{G}))(R)$ is the type of \mathbf{P} . Checking that it is t_1 , reduces to the field case which is [Co2, Lemma 3.12].

For the general case, let S be a flat cover of R such that $\mathbf{Q}(S) \neq \emptyset$. We have an isomorphism $\mathbf{Q}_S \xrightarrow{\sim} \text{Par}(G)_{t_1, S}$ which is canonical and \mathbf{G}_S -equivariant. By faithfully flat descent, it descends to a \mathbf{G} -equivariant isomorphism $\mathbf{Q} \xrightarrow{\sim} \text{Par}(\mathbf{G})_{t_1}$.

(b) follows from Theorem A.1 applied to $\mathbf{Q} \cong \text{Par}(\mathbf{G})_{t_1}$. □

A.6. Corollary. *We assume that R is a semilocal ring. Let (M, q) be a quadratic space of constant rank ≥ 3 , let S be a finite R -algebra such that q_S is isotropic, and let $(v_{\mathfrak{m}})_{\mathfrak{m} \in \text{Specmax}(R)}$ be a family of isotropic elements $v_{\mathfrak{m}} \in M \otimes_R S/\mathfrak{m}$. Then there exists an isotropic $v \in M \otimes_R S$ that lifts the $v_{\mathfrak{m}}$'s.*

Proof. Let $\mathbf{Q} \subset \mathbb{P}(M^\vee)$ be the projective quadric associated with q in Proposition A.5. Our assumption is that $\mathbf{Q}(S) \neq \emptyset$.

Each S/\mathfrak{m} -module $(S/\mathfrak{m}).v_{\mathfrak{m}}$ is a direct summand of $M \otimes_R S/\mathfrak{m}$ which is free of rank one, so defines a point $x_{\mathfrak{m}} \in \mathbf{Q}(S/\mathfrak{m})$. Proposition A.5(b)(ii) provides an element $x \in \mathbf{Q}(S)$ which lifts the $x_{\mathfrak{m}}$'s. Since S is semilocal, x is represented by an S -module D which is a direct summand of rank one of $M \otimes_R S$ and satisfies $q(D) = 0$. We write $D = Sv$ where v is an S -unimodular element of $M \otimes_R S$ satisfying $q(v) = 0$. Since $S^\times \rightarrow \prod_{\mathfrak{m}} (S/\mathfrak{m})^\times$ is onto, we can modify v by an unit of S to ensure that v lifts the $v_{\mathfrak{m}}$'s. □

APPENDIX B. TRACE FOR TORSORS

B.1. Weil restriction ([BLR, 7.6], [CGP, A.5], [DG, I, §1, 6.6]). Let $S \in R\text{-alg}$. Given an S -functor Y' , the *Weil restriction* of Y' is the R -functor

$\mathbf{R}_{S/R}(Y')$ defined by

$$\mathbf{R}_{S/R}(Y')(A) = Y'(A \otimes_R S), \quad (A \in R\text{-}\mathbf{alg}).$$

It is uniquely determined by the following universal property: for every R -functor X there exists a bijection

$$(B.1.1) \quad \xi = \xi_{X,Y'}: \text{Mor}_{S\text{-}\mathbf{alg}}(X_S, Y') \xrightarrow{\sim} \text{Mor}_{R\text{-}\mathbf{alg}}(X, \mathbf{R}_{S/R}(Y'))$$

where X_S is the S -functor obtained from X by base change, thus satisfying $X_S(B) = X({}_R B)$ for $B \in S\text{-}\mathbf{alg}$. Here and sometimes in the following we write ${}_R B$ to denote the R -algebra obtained from the S -algebra B by restriction of scalars. The bijection ξ is functorial in X and Y' . It maps $g \in \text{Mor}_{S\text{-}\mathbf{alg}}(X_S, Y')$ to the composition

$$X(A) \xrightarrow{X(\text{inc}_1)} X({}_R(A \otimes_R S)) \xrightarrow{g({}_R(A \otimes_R S))} Y'({}_R(A \otimes_R S))$$

where $A \in R\text{-}\mathbf{alg}$ and inc_1 is the R -algebra homomorphism

$$\text{inc}_1 = \text{inc}_{1,A}: A \longrightarrow {}_R(A \otimes_R S), \quad a \mapsto a \otimes 1_S.$$

We consider two special cases of (B.1.1). First, for $Y' = X_S$ and $g = \text{Id}_{X_S}$ we get the morphism

$$j = j_X = \xi(\text{Id}_{X_S}): X \longrightarrow \mathbf{R}_{S/R}(X_S)$$

of R -functors, determined by $j_X(A) = X(\text{inc}_{1,A})$, $A \in R\text{-}\mathbf{alg}$. Second, putting $X = \mathbf{R}_{S/R}(Y')$ in (B.1.1), there exists a unique morphism

$$q = q_{Y'}: \mathbf{R}_{S/R}(Y')_S \longrightarrow Y'$$

of S -functors satisfying $\xi(q_{Y'}) = \text{Id}_{\mathbf{R}_{S/R}(Y')}$. For $B \in S\text{-}\mathbf{alg}$ we have $\mathbf{R}_{S/R}(Y')_S(B) = \mathbf{R}_{S/R}(Y')({}_R B) = Y'({}_R B \otimes_R S)$ and so

$$q_{Y'}(B): Y'({}_R B \otimes_R S) \longrightarrow Y'(B).$$

In fact, $q_{Y'}(B) = Y'(m_B)$ where m_B is the S -algebra homomorphism

$$m_B: ({}_R B) \otimes_R S \longrightarrow B, \quad b \otimes s \mapsto bs$$

([CGP, A.5.7]). For $Y' = X_S$ we now have constructed morphisms

$$X_S \xrightarrow{j_{X,S}} \mathbf{R}_{S/R}(X_S)_S \xrightarrow{q_{X_S}} X_S$$

between S -functors. Untangling the constructions above, we find

$$(B.1.2) \quad q_{X_S} \circ j_{X,S} = \text{Id}_{X_S}$$

because $B \xrightarrow{\text{inc}_{1,B}} {}_R B \otimes_R S \xrightarrow{m_B} B$ equals Id_B .

B.2. Cohomology and restriction. Let G be a flat R -group sheaf. We denote by

$$H^1(R, G) = H_{\text{fppf}}^1(R, G)$$

the pointed set of isomorphism classes of G -torsors over $\text{Spec}(R)$ in the flat topology. Let $S \in R\text{-alg}$. The base change $X_S = X \times_{\text{Spec}(R)} \text{Spec}(S)$ of a G -torsor X is a G_S -torsor, giving rise to the *restriction map*

$$\text{res} = \text{res}_{S/R, G}: H^1(R, G) \rightarrow H^1(S, G_S), \quad [X] \mapsto [X_S].$$

A homomorphism $f: G \rightarrow H$ of flat R -group sheaves induces a map in cohomology

$$f_*: H^1(R, G) \rightarrow H^1(R, H), \quad [X] \mapsto [X \wedge^G H]$$

where $X \wedge^G H = (X \times_{\text{Spec}(R)} H)/G$ is the contracted product with respect to the G -action on H via f . Contracted products are special cases of fppf quotients and as such allow base change [GM, (4.30)]. Hence $(X \wedge^G H)_S$ and $X_S \wedge^{G_S} H_S$ are isomorphic H_S -torsors, giving rise to a commutative diagram

$$(B.2.1) \quad \begin{array}{ccc} H^1(R, G) & \xrightarrow{f_*} & H^1(R, H) \\ \text{res} \downarrow & & \downarrow \text{res} \\ H^1(S, G_S) & \xrightarrow{f_{S,*}} & H^1(S, H_S) \end{array}$$

of pointed sets. It is known that $H = \mathbb{R}_{S/R}(G_S)$ is again a flat R -group sheaf if G is so and that the maps

$$j: G \rightarrow \mathbb{R}_{S/R}(G_S) \quad \text{and} \quad q: \mathbb{R}_{S/R}(G_S)_S \rightarrow G_S$$

of B.1 are homomorphisms of R -group sheaves.

Hence, passing to cohomology, the maps in the diagram are well-defined:

$$(B.2.2) \quad \begin{array}{ccc} H^1(R, G) & \xrightarrow{j_*} & H^1(R, \mathbb{R}_{S/R}(G_S)) \\ \text{res}_G \downarrow & \swarrow i & \downarrow \text{res}_{\mathbb{R}(G_S)} \\ H^1(S, G_S) & \xleftarrow{q_*} & H^1(S, \mathbb{R}_{S/R}(G_S)_S) \end{array}$$

We claim that (B.2.2) is a commutative diagram. Indeed, since $q \circ j_S = \text{Id}_{G_S}$ by (B.1.2), this follows from commutativity of (B.2.1):

$$(B.2.3) \quad \text{res}_G = q_* \circ (j_S)_* \circ \text{res}_{S/R, G} = q_* \circ \text{res}_{\mathbb{R}_{S/R}(G_S)} \circ j_* = i \circ j_*.$$

The map $i = q_* \circ \text{res}_{\mathbb{R}_{S/R}(G_S)}$ is injective by [SGA3, XXIV.8.2].

In particular, *assume that G is an abelian affine R -group scheme*. Then so are G_S , $\mathbb{R}_{S/R}(G_S)$ and $\mathbb{R}_{S/R}(G_S)_S$. Moreover, the cohomology sets and maps used in (B.2.2) are abelian groups and group homomorphisms respectively. Since i is injective, we get from (B.2.3) that

$$(B.2.4) \quad \text{Ker}(\text{res}_G) = \text{Ker}(i \circ j_*) = \text{Ker}(j_*).$$

B.3. Deligne trace homomorphism. Let $S \in R\text{-alg}$ be locally free of finite rank $d \in \mathbb{N}_+$, i.e., the R -module S is projective of constant rank d , and let G be an abelian affine R -group scheme. We then have Deligne's trace homomorphism

$$(B.3.1) \quad \text{tr}: R_{S/R}(G) \rightarrow G, \quad \text{satisfying } \text{tr} \circ j = \times d,$$

where $\times d: G \rightarrow G$ is the group homomorphism given on T -points, $T \in R\text{-alg}$, by $g \mapsto g^d$ [SGA4₃, XVII, 6.3.13–6.3.15]. It induces an endomorphism

$$(\times d)_*: H^1(R, G) \longrightarrow H^1(R, G)$$

given by the analogous formula. Since $(\times d)_* = \text{tr}_* \circ j_*$ by (B.3.1), we obtain from (B.2.4) that

$$(B.3.2) \quad \text{Ker}(\text{res}_{S/R, G}) = \text{Ker}(j_*) \subset \text{Ker}((\times d)_*).$$

In particular, this implies the following.

B.4. Lemma. *In the setting of B.3 assume that $\times d: G \rightarrow G$ is an isomorphism. Then the restriction homomorphism $\text{res}_{S/R, G}: H_{\text{fppf}}^1(R, G) \rightarrow H_{\text{fppf}}^1(S, G)$ is injective.*

Example. Let G be the constant R -group scheme $\mathbb{Z}/2\mathbb{Z}$, which is the automorphism group scheme of a quadratic étale R -algebra A , and let d be odd. Then Lemma B.4 applies and in particular shows that A is split, i.e., $A = R \times R$, if and only if A_S is split.

REFERENCES

- [AG] S. Alsaody, P. Gille, *Isotopes of octonion algebras, G_2 -Torsors and triality*, Adv. Math. **343** (2019), 864–909.
- [Ba] R. Baeza, *Quadratic Forms over Semilocal Rings*, Lecture Notes in Mathematics **655** (1978).
- [BFP] E. Bayer-Fluckiger, U. A. First, and R. Parimala, *On the Grothendieck-Serre Conjecture for Classical Groups*, [arXiv:1911.07666](https://arxiv.org/abs/1911.07666)
- [BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band **21**, Springer-Verlag 1990.
- [Co1] B. Conrad, *Reductive group schemes*, in *Autour des schémas en groupes, vol. I*, Panoramas et Synthèses **42-43**, Soc. Math. France 2014.
- [Co2] ———, *Standard parabolics subgroups. Theory and Examples*, <http://math.stanford.edu/~conrad/249BW16Page/handouts/stdpar.pdf>
- [CGP] B. Conrad, O. Gabber, and G. Prasad, *Pseudo-reductive groups*, second edition. New Mathematical Monographs **26**, Cambridge University Press, Cambridge 2015.
- [DG] M. Demazure and P. Gabriel, *Groupes algébriques*, North-Holland (1970).
- [EGA] A. Grothendieck (avec la collaboration de J. Dieudonné), *Eléments de Géométrie Algébrique*, Publications mathématiques de l'I.H.É.S. no. 4, 8, 11, 17, 20, 24, 28, 32, 1960–1967.
- [EKM] R. Elman, N. Karpenko, and A. Merkurjev, *The algebraic and geometric theory of quadratic forms*, Amer. Math. Soc. Colloq. Publ. **56**, Amer. Math. Soc., Providence, RI, 2008.
- [Fo] T. J. Ford, *Separable Algebras*, Graduate Studies in Mathematics **183**, Amer. Math. Soc, Provident, RI, (2017).

- [GM] G. van der Geer and B. Moonen, preliminary version of a book on *Abelian Varieties*, <https://www.math.ru.nl/~bmoonen/research.html#lecturenotes>
- [Ho1] D. W. Hoffmann, *Diagonal forms of degree p in characteristic p* , Algebraic and arithmetic theory of quadratic forms, 135–183, *Contemp. Math.*, **344**, Amer. Math. Soc., Providence, RI, 2004.
- [Ho2] ———, *Similarity of quadratic and symmetric bilinear forms in characteristic 2*, *Indagationes Mathematicae* (2020), <https://doi.org/10.1016/j.indag.2020.08.008>.
- [Kne] M. Knebusch, *Isometrien über semilokalen Ringen*, *Math. Z.* **108** (1969), 255–268.
- [Knu] M.-A. Knus, *Quadratic and Hermitian Forms over Rings*, *Grundlehren der mathematischen Wissenschaften* **294** (1991), Springer.
- [Lag] A. Laghribi, *The norm theorem for totally singular quadratic forms*, *Rocky Mountain J. Math.* **36** (2006), 575–592.
- [Lam] T. Y. Lam, *An Introduction to Quadratic Forms over Fields*, *Graduate Studies in Mathematics* **67**, Amer. Math. Soc., Providence, RI, 2005.
- [Lo] O. Loos, *Generically algebraic Jordan algebras over commutative rings*, *J. Algebra* **297** (2006), 474–529.
- [PR] I. Panin and U. Rehman, *A variant of a theorem by Springer*, *St. Petersburg Math. J.* **19** (2008), 953–959.
- [PP] I. Panin and K. Pimenov, *Rationally isotropic quadratic spaces are locally isotropic: II*, *Doc. Math.* 2010, Extra vol.: Andrei A. Suslin sixtieth birthday, 515–523.
- [Pe] H. P. Petersson, *A survey on Albert algebras*, *Transform. Groups* **24** (2019), 219–278.
- [Sa] C. H. Sah, *Symmetric bilinear forms and quadratic forms*, *J. Algebra* **20** (1972), 144–160.
- [Sch] W. Scharlau, *Quadratic and Hermitian Forms*, *Grundlehren der Mathematischen Wissenschaften* **270**, Springer-Verlag Berlin 1985.
- [Scu] S. Scully, *The Artin-Springer Theorem for quadratic forms over semi-local rings with finite residue fields*, *Proc. Amer. Math. Soc.* **146** (2018), 1–13.
- [SGA3] *Séminaire de Géométrie algébrique de l’I.H.E.S., 1963-1964, schémas en groupes, dirigé par M. Demazure et A. Grothendieck*, *Lecture Notes in Math.* 151-153. Springer (1970).
- [SGA4₃] *Théorie des topos et cohomologie étale des schémas, Tome 3 (French), Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4). Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat.* *Lecture Notes in Mathematics* **305**, Springer-Verlag, Berlin-New York, 1973.
- [Sp] T. A. Springer, *Sur les formes quadratiques d’indice zéro*, *C. R. Acad. Sci. Paris* **234** (1952), 1517–1519.
- [St] The Stacks Project Authors, *Stacks project*, <http://stacks.math.columbia.edu/>

UMR 5208 DU CNRS - INSTITUT CAMILLE JORDAN - UNIVERSITÉ CLAUDE BERNARD
 LYON 1, 43 BOULEVARD DU 11 NOVEMBRE 1918, 69622 VILLEURBANNE CEDEX - FRANCE
Email address: gille@math.univ-lyon1.fr

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF OTTAWA, OTTAWA,
 ONTARIO, CANADA, K1N 6N5
Email address: neher@uottawa.ca