Jean-Louis Colliot-Thélène · Skip Garibaldi
R. Sujatha · Venapally Suresh *Editors*

DEVELOPMENTS IN MATHEMATICS 18

Quadratic Forms, Linear Algebraic Groups, and Cohomology

Springer

QUADRATIC FORMS, LINEAR ALGEBRAIC GROUPS, AND COHOMOLOGY

Developments in Mathematics

VOLUME 18

Series Editor:
Krishnaswami Alladi, *University of Florida, U.S.A.*

QUADRATIC FORMS, LINEAR ALGEBRAIC GROUPS, AND COHOMOLOGY

Edited by

JEAN-LOUIS COLLIOT-THÉLÈNE
CNRS, Université Paris-Sud, Orsay, France

SKIP GARIBALDI
Emory University, Atlanta, GA, USA

R. SUJATHA
Tata Institute of Fundamental Research, Mumbai, India

VENAPALLY SURESH
University of Hyderabad, Hyderabad, India

Springer

Editors
Prof. Jean-Louis Colliot-Thélène
CNRS
Université Paris-Sud
Labo. Mathematiques
91405 Orsay CX
France
jlct@math.u-psud.fr

Prof. Skip Garibaldi
Emory University
Dept. Mathematics &
Computer Science
Dowman Dr. 400
30322 Atlanta Georgia
MSC W421
USA
skip@mathcs.emory.edu

Prof. R. Sujatha
Tata Institute of Fundamental Research
School of Mathematics
Homi Bhabha Rd.
400005 Mumbai
Colaba
India
sujatha@math.tifr.res.in

Venapally Suresh
University of Hyderabad
Dept. Mathematics & Statistics
500046 Hyderabad
P.O. Central University
India
suresh.venapally@gmail.com

ISSN 1389-2177
ISBN 978-1-4419-6210-2 e-ISBN 978-1-4419-6211-9
DOI 10.1007/978-1-4419-6211-9
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2010930046

Mathematics Subject Classification (2010): 11Exx, 11Fxx, 19Gxx, 20Gxx

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

We dedicate this volume to Professor Parimala on the occasion of her 60th birthday. It contains a variety of papers related to the themes of her research. Parimala's first striking result was a counterexample to a quadratic analogue of Serre's conjecture (*Bulletin of the American Mathematical Society*, 1976). Her influence has continued through her tenure at the Tata Institute of Fundamental Research in Mumbai (1976–2006), and now her time at Emory University in Atlanta (2005–present).

A conference was held from 30 December 2008 to 4 January 2009, at the University of Hyderabad, India, to celebrate Parimala's 60th birthday (see the conference's Web site at http://mathstat.uohyd.ernet.in/conf/quadforms2008). The organizing committee consisted of J.-L. Colliot-Thélène, Skip Garibaldi, R. Sujatha, and V. Suresh. The present volume is an outcome of this event.

We would like to thank all the participants of the conference, the authors who have contributed to this volume, and the referees who carefully examined the submitted papers. We would also like to thank Springer-Verlag for readily accepting to publish the volume. In addition, the other three editors of the volume would like to place on record their deep appreciation of Skip Garibaldi's untiring efforts toward the final publication.

We are grateful for the support and the hospitality of the University of Hyderabad, especially the members of the Department of Mathematics and Statistics. We would like to thank the office staff of the Department of Mathematics and Statistics and the other staff of the University responsible for providing administrative and logistical support.

We are also extremely grateful to the University Grants Commission, India and the National Board for Higher Mathematics for financial support.

Paris, France	*J.-L. Colliot-Thélène*
Atlanta, USA	*Skip Garibaldi*
Mumbai, India	*R. Sujatha*
Hyderabad, India	*V. Suresh*
December 2009	

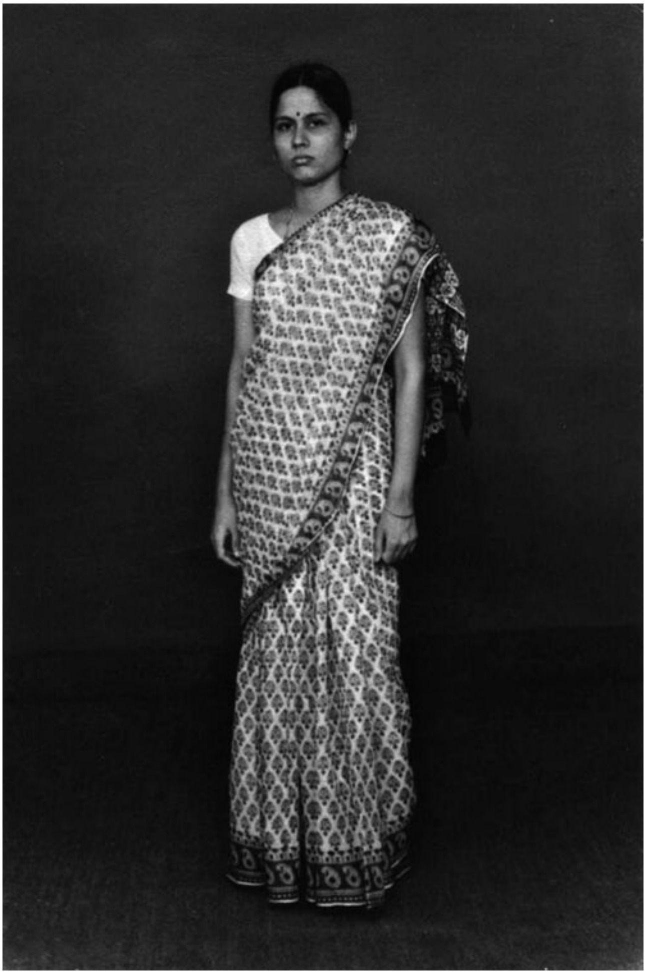


Fig. 1 Parimala during her high school years

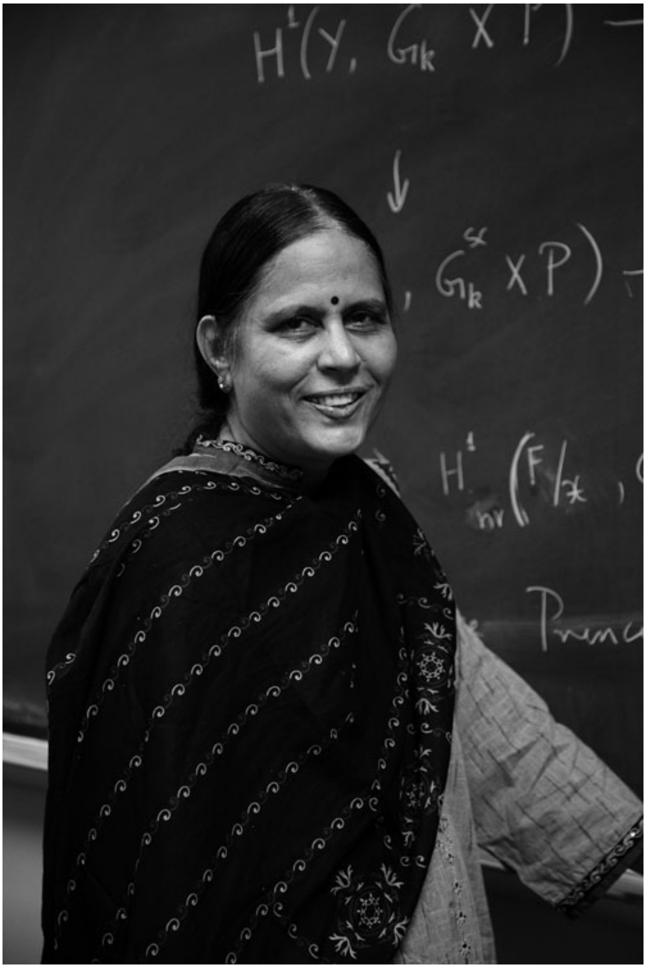


Fig. 2 Parimala at Emory in 2009

Contents

Part II Invited Articles

Part I
Surveys

Multiples of forms

Eva Bayer-Fluckiger

To my friend Parimala

Summary The aim of this paper is to survey and extend some results concerning multiples of (quadratic, hermitian, bilinear...) forms.

Introduction

Let k be a field of characteristic $\neq 2$. Let k_s be a separable closure of k, and set $\Gamma_k = \mathrm{Gal}(k_s/k)$. Let $\mathrm{cd}_2(\Gamma_k)$ be the 2-cohomological dimension of Γ_k. It is a classical question whether it is possible to characterize quadratic forms over k up to isomorphism via some cohomological invariants. For instance, it is well-known that if $\mathrm{cd}_2(\Gamma_k) = 1$, then two quadratic forms are isomorphic if and only if they have the same dimension and discriminant.

The same problem is relevant for hermitian forms over division algebras, G-forms (where G is a finite group), systems of quadratic or hermitian forms, etc.

Such a direct comparison does not seem to be possible for fields of arbitrary cohomological dimension. For this reason, the following weaker question was proposed in [2, 8.5] (in the context of trace forms of Galois algebras). Let I be the fundamental ideal of the Witt ring of k, let d be a positive integer, and let $\phi \in I^d$. Can we compare $\phi \otimes q$ and $\phi \otimes q'$ in terms of some cohomological invariants ?

This question was mostly studied for hermitian forms over division rings with involution and for trace forms of Galois algebras (see for instance [2–4, 7]). This paper will survey and slightly extend these results. For instance, we will show the following

E. Bayer-Fluckiger
Ecole Polytechnique Fédérale de Lausanne, Mathématiques, EPFL–FSB–IMB–CSAG,
Station 8, 1015 Lausanne, Switzerland, e-mail: eva.bayer@epfl.ch

2010 Mathematics subject classification. Primary: 12G05. Secondary: 12F99.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_1,

Theorem. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \le d$*, and let G be a finite group that has no quotient of order* 2*. Let q and* q' *be two G-quadratic forms defined on the same* $k[G]$*-module, and let* $\phi \in I^{d-1}$*. Then*

$$\phi \otimes q \simeq \phi \otimes q'.$$

1 Multiples of Quadratic Forms

1.1 Galois Cohomology

Let k_s be a separable closure of k, and set $\Gamma_k = \mathrm{Gal}(k_s/k)$. For any discrete Γ_k-module C, set $H^i(k,C) = H^i(\Gamma_k,C)$. We say that the *2-cohomological dimension* of Γ_k is at most d, denoted by $\mathrm{cd}_2(\Gamma_k) \le d$, if $H^i(k,C) = 0$ for all $i > d$ and for every finite 2-primary Γ_k-module C.

Set $H^i(k) = H^i(k,\mathbf{Z}/2\mathbf{Z})$, and recall that $H^1(k) \simeq k^*/k^{*2}$. For all $a \in k^*$, let us denote by $(a) \in H^1(k)$ the corresponding cohomology class. We use the additive notation for $H^1(k)$. If $a_1,\dots,a_n \in k^*$, we denote by $(a_1)\cup\cdots\cup(a_n) \in H^n(k)$ their cup product.

If U is a linear algebraic group defined over k, let $H^1(k,U)$ be the pointed set $H^1(\Gamma_k,U(k_s))$ (cf. [11], [12, Chap. 10]).

1.2 Quadratic Forms

All quadratic forms are supposed to be nondegenerate. We denote by $W(k)$ the Witt ring of k, and by $I = I(k)$ the fundamental ideal of $W(k)$. For all $a_1,\dots,a_n \in k^*$, let us denote by $\langle\langle a_1,\dots,a_n\rangle\rangle = \langle 1,-a_1\rangle \otimes\cdots\otimes \langle 1,-a_n\rangle$ the associated n-fold Pfister form. It is well known that I^n is generated by the n-fold Pfister forms. The following has been conjectured by Milnor

Theorem 1.2.1 (cf. Orlov–Vishik–Voevodsky [8]). *For every positive integer n, there exists an isomorphism*

$$e_n : I^n/I^{n+1} \to H^n(k)$$

such that

$$e_n(\langle\langle a_1,\dots,a_n\rangle\rangle) = (a_1)\cup\cdots\cup(a_n)$$

for all $a_1,\dots,a_n \in k^*$.

It is easy to see that the above theorem has the following consequences (cf. [3]):

Corollary 1.2.2. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \le d$*. Let q and* q' *be two quadratic forms with* $\dim(q) = \dim(q')$*, and let* $\phi \in I^d$*. Then* $\phi \otimes q \simeq \phi \otimes q'$*.*

For every quadratic form q, let us denote by $\mathrm{disc}(q) \in H^1(k)$ its discriminant. Recall that if $n = \dim(q)$, then $\mathrm{disc}(q) = (-1)^{n(n-1)/2}\det(q)$.

Corollary 1.2.3. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$*. Let* q *and* q' *be two quadratic forms with* $\dim(q) = \dim(q')$*, and let* $\phi \in I^{d-1}$*. Then*

$$\phi \otimes q \simeq \phi \otimes q' \textit{ if and only if } e_{d-1}(\phi) \cup (\mathrm{disc}(q)) = e_{d-1}(\phi) \cup (\mathrm{disc}(q')) \in H^d(k).$$

For any quadratic form q, let us denote by $w_2(q) \in Br_2(k)$ the Hasse–Witt invariant of q. Recall that if $q \simeq \langle a_1, \dots, a_n \rangle$, then $w_2(q) = \prod_{i<j}(a_i, a_j)$, where (a_i, a_j) is the quaternion algebra over k determined by a_i and a_j. We can extend the previous results as follows:

Corollary 1.2.4. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$*. Let* q *and* q' *be two quadratic forms. Suppose that* $\dim(q) = \dim(q')$ *and* $\det(q) = \det(q')$*. Let* $\phi \in I^{d-2}$*. Then*

$$\phi \otimes q \simeq \phi \otimes q' \textit{ if and only if } e_{d-2}(\phi) \cup w_2(q) = e_{d-2}(\phi) \cup w_2(q') \in H^d(k).$$

Proof. Let $Q = q \oplus (-q')$, and let $\dim(q) = \dim(q') = m$, $\det(q) = \det(q') = d$, Then $\det(Q) = (-1)^m d^2 = (-1)^m$ in k^*/k^{*2}, hence $\mathrm{disc}(Q) = (-1)^m(-1)^m = 1$. This implies that $Q \in I^2$.

As $Q \in I^2$, $e_2(Q)$ is defined. We have $e_2(Q) = w_2(q) + w_2(q')$. Indeed, we have $w_2(-q') = w_2(q') + (-1, (-1)^{m(m-1)/2} d^{m-1})$, and $w_2(Q) = w_2(q) + w_2(q') + (d, (-1)^m d)$. Using this, a computation shows that $w_2(Q) = w_2(q) + w_2(q') + (-1, (-1)^{m(m-1)/2})$. On the other hand, we have $e_2(Q) = w_2(Q)$ if $m \equiv 0, 1 \pmod 4$, $e_2(Q) = w_2(Q) + (-1, -1)$ if $m \equiv 2, 3 \pmod 4$. Therefore, we get $e_2(Q) = w_2(q) + w_2(q')$. □

Let $\phi \in I^{d-2}$. Then $\phi \otimes q \simeq \phi \otimes q'$ if and only if $\phi \otimes Q$ is hyperbolic. This is equivalent to $e_{d-2}(\phi) \cup e_2(Q) = 0$, hence to $e_{d-2}(\phi) \cup w_2(q) = e_{d-2}(\phi) \cup w_2(q')$.

2 Hermitian forms over Division Algebras with Involution

Let D be a division algebra over k. An *involution* of D is a k-linear antiautomorphism $\sigma : D \to D$ of order 2. Let K be the center of D. We say that (D, σ) is a *division algebra with involution over* k if the fixed field of σ in K is equal to k. If $K = k$, then σ is said to be of the *first kind*. After extension to k_s, the involution σ is determined by a symmetric or a skew-symmetric form. In the first case, σ is said to be of *orthogonal type*, in the second one, of *symplectic type*. If $K \neq k$, then K is a quadratic extension of k and the restriction of σ to K is the nontrivial automorphism of K over k. In that case, the involution is said to be of the *second kind*, or a *unitary involution*, or a K/k-involution. Details on algebras with involution are in Chap. 8 of Scharlau's book [10].

Let (D, σ) be a division algebra with involution over k. A *hermitian form* over (D, σ) is by definition a pair (V, h), where V is a finite dimensional D-vector space, and $h : V \times V \to D$ is hermitian with respect to σ. We say that (V,h) is *hyperbolic* if there exists a sub D-vector space W of V with $\dim(V) = 2\dim(W)$ and such that $h(x,y) = 0$ for all $x,y \in W$. This leads to a notion of Witt group $W(D,\sigma)$ (see for instance [10, Chap. 7, Sect. 2]). Note that the tensor product of a quadratic form over k with a hermitian form over (D,σ) is a hermitian form over (D,σ), hence $W(D,\sigma)$ is a $W(k)$-module.

Let (V,h) be a hermitian form over (D,σ), as above. Let $n = \dim_D(V)$, and let H be the matrix of h with respect to some D-basis of V. Let us denote by $\mathrm{Nrd} : M_n(D) \to k$ the reduced norm. The *discriminant* of h is by definition $\mathrm{disc}(h) = (-1)^{n(n-1)/2}\mathrm{Nrd}(H) \in k^*/k^{*2}$.

Let (D,σ) be a division algebra with involution over k. Let us denote by J the sub $W(k)$-module of $W(D,\sigma)$ consisting of the hermitian forms (V,h) with $\dim_D(V)$ even. Suppose that $\mathrm{cd}_2(\Gamma_k) \leq d$. The following is proved in [3, Sect. 2]:

Theorem 2.1.1.

(a) We have $I^d J = 0$.
(b) If σ *is of the second kind, then* $I^{d-1}J = 0$.
(c) If σ *is of the first kind and of the symplectic type, then* $I^{d-2}J = 0$.

Part (a) was proved by Chabloz in [7].

The following three results follow from theorems of Parimala, Sridharan and Suresh [9], and of Berhuy [6], and are proved in [3, Sect. 2]:

Theorem 2.1.2. *Suppose that D is a quaternion algebra, and that σ is of the first kind and of the orthogonal type. Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$*. Let $h \in J$, and let $\phi \in I^{d-1}$. Then $\phi \otimes h$ is hyperbolic if and only if* $e_{d-1}(\phi) \cup (\mathrm{disc}(h)) = 0$.

Corollary 2.1.3. *Suppose that D is a quaternion algebra, and that σ is of the first kind and of the orthogonal type. Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$*. Let h and h' be two hermitian forms over (D,σ) with* $\dim(h) = \dim(h')$*, and let $\phi \in I^{d-1}$. Then $\phi \otimes h \simeq \phi \otimes h'$ if and only if* $e_{d-1}(\phi) \cup (\mathrm{disc}(h)) = e_{d-1}(\phi) \cup (\mathrm{disc}(h'))$.

Let us denote by J_2 the sub-$W(k)$-module of J consisting of the classes of the hermitian forms h such that $\mathrm{disc}(h) = 1$. Then we have (cf. [3, Sect. 2]):

Corollary 2.1.4. *Suppose that D is a quaternion algebra, and that σ is of the first kind and of the orthogonal type. Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$*. Then* $I^{d-1}J_2 = 0$.

Let h be a hermitian form over a quaternion algebra D endowed with an involution σ of the first kind and of orthogonal type. Suppose that $h \in J_2$. Then one can define the *Clifford invariant* $\mathscr{C}(h) \in Br_2(k)/(D)$, cf. [5, Sect. 2]. We have the following:

Theorem 2.1.5. *Suppose that D is a quaternion algebra, and that σ is of the first kind and of the orthogonal type. Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$*. Let $h \in J_2$, and let $\phi \in I^{d-2}$. Then $\phi \otimes h$ is hyperbolic if and only if* $e_{d-2}(\phi) \cup \mathscr{C}(h) = 0$.

Proof. By Berhuy [6, Th. 13], it suffices to show that $e_{d-2}(\phi) \cup \mathscr{C}(h) = 0$ if and only if $e_{n,D}(\phi \otimes h) = 0$ for all $n \geq 0$ (see [6, 2.2] for the definition of the invariant $e_{n,D}$). As $\mathrm{cd}_2(\Gamma_k) \leq d$, we have $e_{n,D}(\phi \otimes h) = 0$ for $n > d$, so it suffices to check that $e_{d-2}(\phi) \cup \mathscr{C}(h) = 0$ is equivalent with $e_{n,D}(\phi \otimes h) = 0$ for all $n = 0, \ldots, d$. Let $k(D)$ be the function field of the quadric associated to D. Then $D \otimes k(D) \simeq M_2(k(D))$, and $h_{k(D)}$ corresponds via Morita equivalence to a quadratic form q_h over $k(D)$. Note that $e_2(q_h) = \mathscr{C}(h)$. Similarly, the hermitian form $(\phi \otimes h)_{k(D)}$ corresponds to a quadratic form $q_{\phi h}$ over $k(D)$, and we have $q_{\phi h} \simeq \phi \otimes q_h$.

For all $n = 0, \ldots, d$, we have by construction that $e_{n,D}(\phi \otimes h) = 0$ if and only if $e_n(q_{\phi h}) = 0$ (cf. [6, 2.2]). But $q_{\phi h} \simeq \phi \otimes q_h$, hence

$$e_n(q_{\phi h}) = e_n(\phi \otimes q_h) = e_{n-2}(\phi) \cup e_2(q_h) = e_{n-2}(\phi) \cup \mathscr{C}(h).$$

If $n < d$, then $e_{n-2}(\phi) = 0$ as $\phi \in I^{d-2}$. We have $e_d(q_{\phi h}) = e_{d-2}(\phi) \cup (\mathscr{C}(h))$. Hence $e_n(q_{\phi h}) = 0$ for all $n \geq 0$ if and only if $e_{d-2}(\phi) \cup \mathscr{C}(h) = 0$. This concludes the proof. □

Let us denote by J_2 the sub $W(k)$-module of J_2 consisting of the classes of the hermitian forms h such that $\mathscr{C}(h) = 0$.

Corollary 2.1.6. *Suppose that D is a quaternion algebra, and that σ is of the first kind and of the orthogonal type. Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Then* $I^{d-2}J_3 = 0$.

Proof. This is an immediate consequence of 2.1.5. □

3 Galois Cohomology of Unitary Groups

Let k be a field of characteristic $\neq 2$. Let A be a finite dimensional k-algebra, and let $\sigma : A \to A$ be a k-linear involution. Let U_A be the linear algebraic group over k defined by

$$U_A(E) = \{x \in A_E \mid x\sigma(x) = 1\}$$

for any commutative k-algebra E. The group U_A is called the *unitary group* of (A, σ). Let us denote by U'_A the connected component of the identity. Let ϕ be a quadratic form of dimension n, set $A_\phi = M_n(k) \otimes_k A$, and let $\sigma_\phi : A_\phi \to A_\phi$ be the involution given by the tensor product of the involution on $M_n(k)$ induced by ϕ with the involution σ.

Recall that k_s is a separable closure of k, that $\Gamma_k = \mathrm{Gal}(k_s/k)$, and that for any linear algebraic group U, we use the standard notation $H^1(k, U) = H^1(\Gamma_k, U(k_s))$ (see [11, 12] for basic facts concerning nonabelian Galois cohomology). With the notation as above, we have natural maps $H^1(k, U'_A) \to H^1(k, U_A)$ and $H^1(k, U_A) \to H^1(k, U_\phi)$.

Let R_A be the radical of the algebra A, and set $\overline{A} = A/R_A$. We have

$$\overline{A} \simeq A_1 \times \cdots \times A_s \times (A_{s+1} \times A'_{s+1}) \times \cdots \times (A_m \times A'_m),$$

where A_i is a simple algebra for all $i = 1,\dots,m$, with $\sigma(A_i) = A_i$ for $i = 1,\dots,s$ and $\sigma(A_i) = A_i'$ for $i = s+1,\dots,m$. Let a_i be the index of A_i.

Theorem 3.1.1. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \le d$.

(i) Let $\phi \in I^d$. Then the map $H^1(k,U_A) \to H^1(k,U_\phi)$ is trivial.
(ii) Let $\phi \in I^{d-1}$. Suppose that if σ_i is orthogonal and $i = 1,\dots,s$, then $a_i = 1$. Then the composition $H^1(k,U_A') \to H^1(k,U_A) \to H^1(k,U_\phi)$ is trivial.

Proof. The projection $A \to \overline{A}$ induces a bijection of pointed sets $H^1(k,U_A) \to H^1(k,U_{\overline{A}})$. Let F_i be the maximal subfield of the center of A_i such that σ_i is F_i-linear if $i = 1,\dots,s$, and let U_i be the norm-one group of (A_i,σ_i). For $i = s+1,\dots,m$, let F_i be the center of A_i, and let U_i be the norm-one group of $((A_i \times A_i),\sigma_i)$. Then U_i is a linear algebraic group defined over F_i for all $i = 1,\dots,m$. We have a bijection of pointed sets

$$H^1(k,U_A) \to \prod_{i=1,\dots,m} H^1(F_i,U_i).$$

If $i = s+1,\dots,m$, then U_i is a general linear group, hence $H^1(F_i,U_i) = 0$. Hence we have a bijection of pointed sets $H^1(k,U_A) \to \prod_{i=1,\dots,s} H^1(F_i,U_i)$. For all $i = 1,\dots,s$, the simple algebra A_i is a matrix algebra over a division algebra with involution D_i. The group U_i is the unitary group of a hermitian form h_i over D_i, and it is well-known that $H^1(F_i,U_i)$ is in bijection with the isomorphism classes of the hermitian forms over D_i of the same dimension as h_i.

Let R_ϕ be the radical of A_ϕ. The map $f : H^1(k,U_A) \to H^1(k,U_\phi)$ induces $\overline{f} : H^1(k,U_{\overline{A}}) \to H^1(k,U_{\overline{\phi}})$, and

$$f_i : H^1(F_i,U_i) \to H^1(F_i,U_{M_n(A_i)})$$

for all $i = 1,\dots,s$. The image of the isomorphism class of the hermitian form h_i' is the hermitian form $\phi \otimes h_i'$.

If $\phi \in I^d$, then by 2.1.1 (a) $\phi \otimes h_i \simeq \phi \otimes h_i'$ for every hermitian form h_i' with $\dim(h_i') = \dim(h_i)$. This implies that f_i is trivial for all $i = 1,\dots,s$, hence $\overline{f}$ is trivial. Therefore f is trivial, which proves (i).

Let us prove (ii). Let us denote by f' the composition $H^1(k,U_A') \to H^1(k,U_A) \to H^1(k,U_\phi)$. Let U_i' be the connected component of the identity in U_i. If σ_i is unitary or symplectic, then $U_i = U_i'$. If σ_i is orthogonal, then by hypothesis $a_i = 1$, so $H^1(F_i,U_i)$ is in bijection with the isomorphism classes of the hermitian (actually, quadratic) forms over $D_i = F_i$ of the same dimension and same discriminant as h_i.

Let us denote by f_i' the composition $H^1(F_i,U_i') \to H^1(F_i,U_i) \to H^1(k,U_{M_r(A_i)})$ for all $i = 1,\dots,s$. Suppose that $\phi \in I^{d-1}$. Then 2.1.1 (b) and (c) imply that f_i' has trivial image if σ_i is unitary or symplectic. If σ_i is orthogonal, then we have $d_i = 1$, therefore by 1.2.3 the map f_i' is trivial. This implies that f' is trivial, and this completes the proof. □

4 Systems of Quadratic and Hermitian Forms

Let V be a finite dimensional k-vector space, and let $S = \{q_1, \ldots, q_r\}$ be a *system of quadratic forms*, $q_i : V \times V \to k$. We say that two systems S and $S' = \{q'_1, \ldots, q'_r\}$ are *isomorphic* if there exists a k-linear isomorphism $f : V \to V$ such that $q'_i(fx, fy) = q_i(x,y)$ for all $x, y \in V$ and for all $i = 1, \ldots, r$.

Let K be a quadratic extension of k, and let W be a finite dimensional K-vector space. Let us denote by $x \mapsto \bar{x}$ the involution of K given by the unique nontrivial k-automorphism of K. We can then consider *systems of hermitian forms* $\Sigma = \{h_1, \ldots, h_r\}$. We say that two systems Σ and $\Sigma' = \{h_1, \ldots, h_r\}$ are *isomorphic* if there exists a K-linear isomorphism $f : W \to W$ such that $h'_i(fx, fy) = h_i(x,y)$ for all $x, y \in W$ and for all $i = 1, \ldots, r$.

Let ϕ be a quadratic form over k. Then the tensor product $\phi \otimes S$ of ϕ with a system of quadratic forms is a system of quadratic forms, and the tensor product $\phi \otimes S$ of ϕ with a system of hermitian forms is a system of hermitian forms.

Theorem 4.1.1. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \le d$.

(i) Let S and S' be two systems of quadratic forms, and suppose that S and S' are isomorphic over k_{s}. Let $\phi \in I^d$. Then $\phi \otimes S \simeq \phi \otimes S'$.
(ii) Let Σ and Σ' be two systems of hermitian forms, and suppose that Σ and Σ' are isomorphic over k_{s}. Let $\phi \in I^{d-1}$. Then $\phi \otimes \Sigma \simeq \phi \otimes \Sigma'$.

Proof. Write $A(S)$ for the set of all $(e, f) \in \mathrm{End}(V) \times \mathrm{End}(V)$ such that $q_i(ex, y) = q_i(x, fy)$ for all $i = 1, \ldots, r$ and write $A(\Sigma)$ for the set of $(e, f) \in \mathrm{End}(W) \times \mathrm{End}(W)$ such that $h_i(ex, y) = h_i(x, fy)$ for all $i = 1, \ldots, r$. These are the algebras associated to the systems S and Σ, cf. [1]. They are endowed with involutions defined by $(e, f) \mapsto (f, e)$, and the automorphism groups of the systems can be identified with the unitary groups of these algebras, see [1] for details.

The isomorphism classes of the systems of quadratic forms that become isomorphic to S over k_{s} are in bijection with $H^1(k, U_{A(S)})$. Hence (i) follows from 3.1.1(i).

The isomorphism classes of the systems of hermitian forms that become isomorphic to Σ over k_{s} are in bijection with $H^1(k, U_{A(\Sigma)})$. As the forms are hermitian with respect to the nontrivial involution $x \mapsto \bar{x}$, the decomposition of the algebra $A(\Sigma)$ as in Sect. 3 has no orthogonal components. Therefore, the hypothesis of 3.1.1(ii) are satisfied, and this implies part (ii) of the theorem. □

5 *G*-Quadratic Forms

Let G be a finite group, and let us denote by $k[G]$ the associated group ring. A *G-quadratic form* is a pair (M, q), where M is a $k[G]$-module that is a finite dimensional k-vector space, and $q : M \times M \to k$ is a nondegenerate symmetric bilinear form such that

$$q(gx, gy) = q(x, y) \quad \text{for all } x, y \in M \text{ and all } g \in G.$$

We say that two G-quadratic forms (M,q) and (M',q') are *isomorphic* if there exists an isomorphism of $k[G]$-modules $f : M \to M'$ such that $q(f(x), f(y)) = q'(x,y)$ for all $x, y \in M$. If this is the case, we write $(M,q) \simeq_G (M',q')$, or $q \simeq_G q'$.

If ϕ is a quadratic form over k, and q a G-quadratic form, then the tensor product $\phi \otimes q$ is a G-quadratic form.

For any G-quadratic form (M,q), let

$$A = A(M,q) = \left\{ (e,f) \in \mathrm{End}_{k[G]}(M) \times \mathrm{End}_{k[G]}(M) \;\middle|\; \begin{array}{l} q(ex,y) = q(x,fy) \text{ for all} \\ x,y \in M \end{array} \right\}$$

be the associated algebra (cf. [1]). Then the unitary group U_A can be identified with the group of automorphisms of (M,q), and the set of isomorphism classes of G-quadratic forms (M,q') is in bijection with the set $H^1(k,U_A)$.

Theorem 5.1.1. *Suppose* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Let* (M,q) *and* (M,q') *be two G-quadratic forms.*

(i) Let $\phi \in I^d$. *Then* $\phi \otimes q \simeq \phi \otimes q'$.
(ii) Suppose moreover that G has no quotient of order 2, and let $\phi \in I^{d-1}$. *Then* $\phi \otimes q \simeq \phi \otimes q'$.

Proof. Part (i) follows immediately from 3.1.1(i). In order to prove part (ii), note that as G has no quotient of order 2, the group G has no nontrivial orthogonal characters, hence $U_A = U'_A$. Therefore, 3.1.1(ii) implies part (ii) of the theorem. □

Acknowledgements The author was partially supported by the Swiss National Science Fundation, grant 200020-109174/1.

References

1. E. Bayer–Fluckiger, Principe de Hasse faible pour les systèmes de formes quadratiques, *J. Reine Angew. Math.* **378** (1987), 53–59.
2. ———, Galois cohomology and the trace form, *Jahresber. DMV* **96** (1994), 35–55.
3. ———, Multiples of trace forms and algebras with involution, *IMRN* (2007), no 23, Art. ID rnm112, 15 pp.
4. E. Bayer–Fluckiger, M. Monsurrò, R. Parimala, R. Schoof, Trace forms of Galois algebras over fields of cohomological dimension ≤ 2, *Pacific J. Math.*, **217** (2004), 29–43.
5. E. Bayer–Fluckiger and R. Parimala, Galois cohomology of the classical groups over fields of cohomolgical dimension ≤ 2, *Invent. Math.* **122** (1995), 195–229.
6. G. Berhuy, Cohomological invariants of quaternionic skew-hermitian forms, *Archiv. Math.* **88** (2007), 434–447.
7. Ph. Chabloz, Anneau de Witt des G-formes et produit des G-formes trace par des formes quadratiques, *J. Algebra* **266** (2003), 338–361.
8. D. Orlov, A. Vishik, V. Voedovsky, An exact sequence for Milnor's K-theory with applications to quadratic forms, *Ann. Math.* **165** (2007), 1–13.
9. R. Parimala, R. Sridharan and V. Suresh, Hermitian analogue of a theorem of Springer, *J. Algebra* **243** (2001), 780–789.

10. W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren der Math. Wiss, Springer–Verlag, Berlin (1985).
11. J-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics, Springer–Verlag, Berlin (1964 and 1994).
12. ______, *Corps locaux*, Hermann (1968).

On Saltman's p-Adic Curves Papers

Eric Brussel

For Parimala on her 60th birthday

Summary We present a synthesis of Saltman's work (Adv. Math. 43(3):250–283, 1982; J. Alg. 314(2):817–843, 2007) on the division algebras of prime-to-p degree over the function field K of a p-adic curve. Suppose Δ is a K-division algebra. We prove that (a) Δ's degree divides the square of its period; (b) if Δ has prime degree (different from p), then it is cyclic; (c) Δ has prime index different from p if and only if Δ's period is prime, and its ramification locus on a certain model for K has no "hot points".

These notes are based on Saltman's seminal work on the Brauer group $\mathrm{Br}(K)$ of the function field K of a p-adic curve $X_{\mathbb{Q}_p}$. In [S1, S2] Saltman showed the index of an element in the prime-to-p part of $\mathrm{Br}(K)$ divides the square of its period, and that all division algebras of prime degree $q \neq p$ are cyclic. He also gave a geometric criterion for a class of prime period $q \neq p$ to have index q. We reprove these theorems, modulo some of [S2, Sect. 1], expanding some proofs, consolidating some results, and providing some additional background along the way.

Eric Brussel
Department of Mathematics & Computer Science, Emory University, Atlanta, GA 30322, USA
e-mail: brussel@mathcs.emory.edu

2010 Mathematics subject classification. Primary: 16K20. Secondary: 11S15, 13A20, 16H05, 16K50.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_2,

Saltman based his analysis on four observations: First, that while K is the function field of the curve $X_{\mathbb{Q}_p}$ over $\mathbb{Q}_p$, it is also the function field of a regular model X of that curve, over $\mathbb{Z}_p$; second, that associated to every $\alpha \in \mathrm{H}^2(K)$ is a divisor $D_\alpha \subset X$, which may be assumed to have normal crossings; third, that purity holds for all such X; and fourth, that the unramified Brauer group $\mathrm{H}^2_{\mathrm{nr}}(K)$ is trivial. The goal in splitting, then, is to construct a field extension L/K over which α is unramified:

$$\partial_w(\alpha_L) = 0 \quad \text{for all } w \in V(L).$$

In particular, we avoid the construction of an explicit model for X_L, over which α would have zero ramification divisor. Constructing L turns out to be tricky, mainly due to the prospect of divisors in the ramification locus of α_L, on any (hypothetical) model of X_L that are centered on closed points of X. The general strategy is to use local equations for D_α to construct an element $f \in K$, set $L = K(f^{1/n})$, compute the residue of α_L at all w using a local structure theorem (this uses purity), and adjust f accordingly, if necessary. The methods are extremely valuation-theoretic. If we can manage $\alpha_L = 0$ and $\mathrm{ind}(\alpha) = n$ is prime, we have cyclicity, by a theorem of Albert.

It is possible to see why the index should divide the square of the period; in light of the triviality of $\mathrm{H}^2_{\mathrm{nr}}(K)$, it is traceable to the dimension of X (see also the excellent summary of [S1] in the review [C-T2], which includes additional citations and context). The existence of a radical splitting field in prime degree is not apparent, even locally, and the proof is quite technical.

Examples. The following two examples illustrate the approach. Write

$$K^* \longrightarrow \mathrm{H}^1(K, \mu_n) \quad \text{via} \quad a \longmapsto (a)$$

for the Kummer homomorphism, suppressing the n because it is always implicit. We write $a \cdot b$ for the cup product of cohomology classes a and b, but we write

$$(a,b) \stackrel{\mathrm{df}}{=} a \cdot (b) \in \mathrm{H}^p(K, \mu_n^{\otimes(p-1)})$$

when $a \in \mathrm{H}^{p-1}(K, \mu_n^{\otimes(p-2)})$ and $b \in K^*$, especially when $a \in \mathrm{H}^1(K, \mathbb{Z}/n)$.

Suppose $\alpha = (\theta, \pi)$ for $\theta \in \mathrm{H}^1(K, \mathbb{Z}/n)$ and $\pi \in K^*$, and let $L = K(\pi^{1/n})$. Since $(\pi)_L = 0$, we compute $\alpha_L = (\theta, \pi)_L = 0$, so L splits α. More difficult: Suppose $\alpha = (\theta_0, \pi_0) + (\theta_1, \pi_1)$, where $\mathrm{div}\, \pi_0$ and $\mathrm{div}\, \pi_1$ are prime divisors on X, and $\theta_i \in \mathrm{H}^1_{\mathrm{nr}}(K, \mathbb{Z}/n)$. Let $L = K((\pi_0\pi_1)^{1/n})$. Since $(\pi_0\pi_1)_L = 0 = (\pi_0)_L + (\pi_1)_L$, $\alpha_L = (-\theta_0 + \theta_1, \pi_1)_L$. If $w \in V(L)$, then

$$\partial_w(\alpha_L) = w(\pi_1)(-\theta_0 + \theta_1)_{\kappa(w)}.$$

If w's center on X has codimension one, then it is easy to show $w(\pi_1) = 0 \pmod{n}$. However, if the center is a closed point, in general $w(\pi_1) \neq 0$, and since we cannot expect $(-\theta_0 + \theta_1)_{\kappa(w)}$ to be zero, the strategy fails in general. We try to salvage it as follows. Let w_0 be a discrete valuation on L extending the valuation v_0 on K defined by π_0, and let $\alpha(w_0) = \alpha_{K_{v_0}(\theta_0)}$ be the value of α at w_0. Then $\alpha(w_0)$ is defined over $\kappa(v_0)$, and we can prove

$$\partial_w(\alpha_L) = w(\pi_1)\,\partial_{v_0,\bar{v}_1}(\alpha(w_0))$$

where $\bar{v}_1$ is the valuation induced by the image of π_1 in $\kappa(v_0)$. If we could zero out $\alpha(w_0)$, we could solve the problem for all w. This strategy turns out to be viable. If α has prime degree, then $\alpha(w_0)$ is cyclic, and the parameter part of $\alpha(w_0)$ varies with $f = \pi_0\pi_1$. Finding an "anti-parameter" $u \in K$, we zero out $\alpha(w_0)$ by replacing f with uf. But now, $\operatorname{div} uf$ may no longer match D_α and if $(\operatorname{div} u) \cap D_\alpha$ is not empty, there is a problem.

In general, there are other, more serious problems. D_α may not be principal in the first place, forcing us to contend with the extra "rogue" components in any $\operatorname{div} f$. If D_α has more than one nodal point, there is a globalization problem. In the end we produce f by a type of successive approximation, and at each stage we must check that the earlier stages have not come undone.

1 Discrete Valuations

Let X be an integral noetherian scheme, and let K be a field containing the function field $F(X)$ of X. If v is a discrete valuation on K, let $\mathrm{O}_v \subset K$ denote the corresponding discrete valuation ring, $\mathfrak{p}_v \subset \mathrm{O}_v$ the prime ideal, and $\kappa(v)$ the residue field. $\operatorname{Spec} K$ is an open subset of $\operatorname{Spec} \mathrm{O}_v$, so $\operatorname{Spec} K \to X$ induces a rational map $\operatorname{Spec} \mathrm{O}_v \dashrightarrow X$. We say v has a *center on* X if this is a morphism, and then denote by x_v the image of the closed point $\operatorname{Spec} \kappa(v)$. Thus, v has a center on X if there is a point $x_v \in X$ such that $\mathrm{O}_{X,x_v} \subset \mathrm{O}_v$ and $\mathfrak{m}_{x_v} = \mathfrak{p}_v \cap \mathrm{O}_{X,x_v}$ (see [Liu, Def. 8.3.17]). We then say v is an *X-valuation of* K. Denote the set of all normalized X-valuations of K by

$$V_X(K).$$

If S is a fixed base, or by default if $S = \operatorname{Spec} \mathbb{Z}$, write $V(K)$ instead of $V_S(K)$. Similarly, we write $V_x(K)$ for those centered on x, and $V(X)$ for the discrete valuations on $F(X)$ that have codimension-one center on X. Substitute $\kappa(x)$ and A for x and X when $x = \operatorname{Spec} \kappa(x)$ and $X = \operatorname{Spec} A$. If x_v belongs to the set $X^{(1)}$ of codimension-one points on X, we have a prime divisor

$$D_v \stackrel{\text{df}}{=} \overline{\{x_v\}}.$$

Remark 1.1. If $v \in V_x(K)$, then $\kappa(x) \subset \kappa(v)$, and $v \in V_{\mathrm{O}_{X,z}}(K)$ for all $z \in \overline{\{x\}}$. If $\phi : Y \to X$ is a morphism of integral schemes, then $V_y(F(Y)) \subset V_{\phi(y)}(F(Y))$ for all $y \in Y$, and conversely, if ϕ is proper then $V_Y(F(Y)) = V_X(F(Y))$.

Lemma 1.2. *Suppose $A = (A, \mathfrak{m}, k)$ is a two-dimensional regular local domain with fraction field K, and $\mathfrak{m} = (\pi_0, \pi_1)$. Suppose $f \in A$, $L = K(f^{1/n})$, and $v \in V(K)$*

extends to $w \in V(L)$. *Then* $w|_K = e(w/v)\,v$, *and* $e(w/v) = n/\gcd(v(f),n)$. *In particular, if* $v(f) \in (\mathbb{Z}/n)^*$, *then* v *is totally ramified in* L.

Proof. Since $\mathfrak{p}_v \cap A = \mathfrak{m}$, $k \subset \kappa(v)$, both v and w are normalized; so $e(w/v) = [\mathbb{Z} : w(K^*)]$. After replacing f by a prime-to-n power of f if necessary, we may assume $v(f) = m$ divides n. At the completions

$$w = \frac{e(w/v)}{[L_w : K_v]} v \circ N_{L_w/K_v}$$

so $w|_K = e(w/v)\,v$. Over K_v, we write $f = \pi_v^m u$, where $v(u) = 0$. The polynomial $T^m - u$ is separable over $\kappa(v)$, and $K_v(u^{1/m})$ is unramified by Hensel's lemma. Then $T^{n/m} - u^{1/m}\pi_v$ is an Eisenstein polynomial over $K_v(u^{1/m})$, and since $L_w = K_v(u^{1/m}, (u^{1/m}\pi_v)^{n/m})$, we conclude $e(w/v) = n/m$. □

2 Residue Map

The material in this section is standard; see [C-T, GMS] or [GS] for additional background. Let X be a scheme, and let n be invertible on X, meaning that n is prime to the residue characteristic of $\kappa(x)$ for all $x \in X$. We write

$$\mathrm{H}^q(X) \overset{\mathrm{df}}{=} \mathrm{H}^q(X_{\text{ét}}, \mu_n^{\otimes(q-1)})$$

If $f : Y \to X$ is a map of schemes, then $f^*\mathbb{Z}/n = \mathbb{Z}/n$ and we have a restriction map

$$\mathrm{res}_{X|Y} : \mathrm{H}^q(X) \to \mathrm{H}^q(Y).$$

If $\alpha \in \mathrm{H}^q(X)$, we will sometimes write α_Y instead of $\mathrm{res}_{X|Y}(\alpha)$, and if $X = \operatorname{Spec} A$ and/or $Y = \operatorname{Spec} B$, we write $\mathrm{H}^q(A)$ and α_B.

Let K be a field, and let $v \in V(K)$. Suppose n is prime to $\operatorname{char}\kappa(v)$. By [C-T, 3.10, p. 26], for any $r \in \mathbb{Z}$ and $q \geq 1$ we have an exact sequence

$$0 \to \mathrm{H}^q(\mathrm{O}_v) \to \mathrm{H}^q(K) \xrightarrow{\partial_v} \mathrm{H}^{q-1}(\kappa(v)) \to 0 \tag{2.1}$$

such that if $\pi_v \in \mathrm{O}_v$ is a uniformizer and $\theta \in \mathrm{H}^{q-1}(\mathrm{O}_v)$, then

$$\partial_v(\theta \cdot (\pi_v)) = \theta_{\kappa(v)}. \tag{2.2}$$

The map ∂_v is called the *residue map*, the images are called *residues*, and $\alpha \in \mathrm{H}^q(K)$ is said to be *unramified at* v if $\partial_v(\alpha) = 0$.

Definition 2.3. If $\alpha \in \mathrm{H}^q(K)$ and $T = X$, A, etc., the *ramification locus of* α *with respect to* T is the set

$$\mathrm{div}_T(\alpha) \overset{\mathrm{df}}{=} \{v \in V(T) : \partial_v(\alpha) \neq 0\}.$$

The *ramification locus* or *ramification divisor for α on X* is

$$D_\alpha \stackrel{\text{df}}{=} \Big\{\sum_v D_v : v \in \operatorname{div}_X(\alpha)\Big\}.$$

Diagrams 2.4. If L/K is a finite separable extension and $w \in V(L)$, then for $v = w|_K$ we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^q(\mathrm{O}_w) \arrow[r] & \mathrm{H}^q(L) \arrow[r, "\partial_w"] & \mathrm{H}^{q-1}(\kappa(w)) \arrow[r] & 0 \\
0 \arrow[r] & \mathrm{H}^q(\mathrm{O}_v) \arrow[r] \arrow[u] & \mathrm{H}^q(K) \arrow[r, "\partial_v"] \arrow[u] & \mathrm{H}^{q-1}(\kappa(v)) \arrow[r] \arrow[u, "e(w/v)\,\mathrm{res}_{\kappa(v)|\kappa(w)}"'] & 0.
\end{tikzcd}$$

Let K_v denote the completion of K with respect to v, and let $\widehat{\mathrm{O}}_v$ be the valuation ring of v on K_v. Then the inflation map $\mathrm{H}^q(\kappa(v)) \to \mathrm{H}^q(\widehat{\mathrm{O}}_v)$ is an isomorphism, and we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^q(\kappa(v)) \arrow[r] & \mathrm{H}^q(K_v) \arrow[r, "\partial_v"] & \mathrm{H}^{q-1}(\kappa(v)) \arrow[r] & 0 \\
0 \arrow[r] & \mathrm{H}^q(\mathrm{O}_v) \arrow[r] \arrow[u] & \mathrm{H}^q(K) \arrow[r, "\partial_v"] \arrow[u] & \mathrm{H}^{q-1}(\kappa(v)) \arrow[r] \arrow[u, equal] & 0
\end{tikzcd}$$

If $\pi_v \in K_v$ is a uniformizer, then any $\alpha \in \mathrm{H}^q(K_v)$ may be expressed as

$$\alpha = \alpha^\circ + (\theta_v, \pi_v)$$

where $\alpha^\circ \in \mathrm{H}^q(\kappa(v))$ and $\theta_v = \partial_v(\alpha) \in \mathrm{H}^{q-1}(\kappa(v))$ are defined over $\widehat{\mathrm{O}}_v$ via inflation. The element α°, of course, depends on the choice of π_v. If $\alpha \in \mathrm{H}^p(K_v)$ and $\beta \in \mathrm{H}^q(K_v)$, then by (2.2) we have the formula

$$\partial_v(\alpha \cdot \beta) = \alpha \cdot \partial_v(\beta) + (-1)^q \partial_v(\alpha) \cdot \beta + \partial_v(\alpha) \cdot \partial_v(\beta) \cdot (-1) \tag{2.5}$$

interpreted over K_v.

Value of a class 2.6. Suppose $\alpha \in \mathrm{H}^q(K)$, L/K is a finite separable extension, $w \in V(L)$, and $\theta_w = \partial_w(\alpha_L)$. Define the *value of α at w* to be

$$\alpha(w) = \begin{cases} \alpha_{L_w} & \text{if } \theta_w = 0 \\ \alpha_{L_w(\theta_w)} & \text{if } q = 2 \end{cases}$$

where $L_w(\theta_w)/L_w$ is the cyclic extension defined by the inflation of the character θ_w from $\kappa(w)$ to L_w. Note in any case $\alpha(w)$ is defined over $\kappa(w)(\theta_w)$.

3 Surfaces

We state some well-known facts and definitions. See [Liu, Lbm, Si] for additional background and proofs.

Definition 3.1. Let S be a Dedekind scheme.

1. A *projective curve* over a field k is a subscheme of $\mathbb{P}_k^m$ for some $m \geq 0$, whose irreducible components are one-dimensional.
2. A *projective flat S-curve* X is a 2-dimensional, integral, projective, flat S-scheme.
3. An *arithmetic surface* $X \to S$ is a regular projective flat S-curve.

Remarks 3.2. If $X \to S$ is an arithmetic surface, then for each closed point $z \in X^{(2)}$, $A = \mathrm{O}_{X,z}$ is a two-dimensional regular noetherian local domain, which is factorial by Auslander-Buchbaum's theorem ([Mat, 20.3]). If S is excellent, then X is excellent, and A is excellent. Since $X \to S$ is proper, $V(K) = V_X(K)$ by the valuative criterion for properness.

If X is a normal projective flat S-curve, and S is a one-dimensional Dedekind scheme, then the generic fiber X_K is a nonsingular integral curve over K, and each closed fiber X_s, $s \in S$, is a projective curve over $\kappa(s)$ ([Liu, 8.3.3]). If $X \to S$ is arithmetic, then each $X_s \to \kappa(s)$ is a local complete intersection ([Liu, 8.3.6]), hence X_s has no embedded points. X_s is generally not reduced. Every effective irreducible divisor $D \subset X$ is either a component of some X_s (D is *vertical*), or the closure of a closed point $x \in X_K$ of the generic fiber (D is *horizontal*).

Intersections on an arithmetic surface 3.3. See [Liu,Lbm]. Let X be an arithmetic surface. Since X is normal, every prime (Weil) divisor defines a discrete valuation $v \in V(X)$, via the local ring of its generic point. If $f \in K$, then

$$\operatorname{div} f = \sum_{V(X)} v(f) D_v,$$

the sum being finite since X is noetherian. If D and E are two effective divisors with no common irreducible components, the intersection multiplicity $(D \cdot E)_z$ at a closed point z is defined to be

$$(D \cdot E)_z \stackrel{\mathrm{df}}{=} \operatorname{length}_{\mathrm{O}_{X,z}} \mathrm{O}_{X,z}/(I_{D,z} + I_{E,z})$$

where I_D and I_E are the ideal sheaves, and the subscript z means "localized at z". If D is prime and $g \in K$ is a local equation for E at z, then $(D \cdot E)_z = v_{\bar{z}}(g)$, where $v_{\bar{z}}$ is the valuation on D induced by z.

Definition 3.4 (Normal crossings). An effective divisor D on a regular noetherian scheme X has *normal crossings at* $z \in X$ if X is regular at z, and for some system of parameters $f_1, \ldots, f_n$ for $\mathrm{O}_{X,z}$, there is an integer $0 \leq m \leq n$ and integers $r_1, \ldots,$ $r_m \geq 1$, such that $I_{D,z}$ is generated by $f_1^{r_1} \cdots f_m^{r_m}$. We say D has *normal crossings on*

X if it has normal crossings at every point. If D has normal crossings, we will also say that the set $\{v_i\}$ of discrete valuations centered on the generic points of D has normal crossings.

This definition, from [Liu, 9.1.6], is different from the relative version in [SGA1, XIII, 2.1.0]. We obtain that version by replacing "normal crossings" by "strictly normal crossings" and "smooth over" by "regular". A normal crossings divisor need not be reduced, but its irreducible components are nonsingular, and meet each other transversally, meaning their local equations form part of a system of parameters at each intersection point.

Existence of a Model 3.5. *Let S be an excellent one-dimensional affine Dedekind scheme, with function field F, and let K be a field extension of F of transcendence degree one. Then there exists a normal connected projective curve X_F with function field K, and a normal projective flat S-curve X with generic fiber X_F. If F is perfect, X_F is smooth over F.*

In fact, there is a category equivalence between normal connected projective curves over F and function fields of transcendence degree one over F, where the morphisms between curves are dominant morphisms ([Liu, 7.3.13]). For curves, normal and regular are the same, and if F is perfect, regular and smooth are the same ([Liu, 4.3.33]), so X_F is smooth if F is perfect. The rest is stated in [Liu, 10.1.6].

Strong Desingularization 3.6. *Let X be a two-dimensional, excellent, reduced, noetherian scheme. Then X admits a desingularization in the strong sense, i.e., a proper birational morphism $f : X' \to X$ with X' regular, and f an isomorphism above every regular point of X. In particular, this holds for X a projective flat S-curve over an excellent Dedekind scheme. If S is affine, $X' \to S$ is then an arithmetic surface.*

This is a theorem of Lipman ([Liu, 8.3.44]). To prove the last statement, note that since f is birational, X' is integral, and $X \to S$ is flat, the induced map $X' \to S$ is flat, since X' dominates S ([Liu, 4.3.9]). Since S is affine, f is projective by [Liu, 8.3.50], and since the composition of projective morphisms is projective, $X' \to S$ is an arithmetic surface.

Embedded Resolution 3.7. *Let $X \to S$ be an arithmetic surface over an excellent Dedekind scheme, and let D be a divisor on X. Then there exists a projective birational morphism $f : X' \to X$ with X' an arithmetic surface, such that f^*D has normal crossings.*

This is [Liu, 9.2.26]. We will need the following lemma from the proof.

Blowup Lemma 3.8. *Suppose $X \to S$ and D are as in the statement of Embedded Resolution (3.7), $f : X' \to X$ blows up a closed point $z \in X$, and D has normal crossings at z. Then $X' \to S$ is an arithmetic surface, and f^*D has normal crossings at every point of the exceptional fiber E. Moreover, E meets the irreducible components of the strict transform $\widetilde{D}$ in at most two points, and these points are rational over $\kappa(z)$.*

One of Saltman's basic observations is that the ramification locus of a Brauer class on an arithmetic surface can be conditioned to have normal crossings.

Existence of Surfaces 3.9. *Let S be an excellent one-dimensional affine Dedekind scheme, and let $s \in S$ be a closed point. Suppose $F = F(S)$, and K is a field of transcendence degree one over F. Then for any $\alpha \in \mathrm{H}^2(K)$, there exists an arithmetic surface $X \to S$ with function field $K = F(X)$ and fiber X_s, such that the union $D_\alpha \cup X_s$ has normal crossings on X.*

Proof. By Existence of a Model 3.5 there exists a normal projective flat S-curve $X'' \to S$ with function field K. Therefore by Strong Desingularization 3.6, there exists an arithmetic surface $X' \to S$ with function field K. Suppose $\alpha \in \mathrm{H}^2(K)$. Then by Embedded Resolution (3.7), there exists an arithmetic surface $X \to S$ and a projective birational morphism $f : X \to X'$ such that $f^*(D'_\alpha \cup X'_s)$ has normal crossings, where D'_α is the divisor of α on X'. Since the irreducible components of $f^*(D'_\alpha \cup X'_s)$ equal those of $D_\alpha \cup X_s$, this proves the result. $\square$

4 Unramified Brauer Group and Arithmetic Surfaces

By definition, if K is a field, $S = \operatorname{Spec} R$ is a base, and $V(K)$ is the set of discrete S-valuations on K,

$$\mathrm{H}^2_{\mathrm{nr}}(K/R) \stackrel{\mathrm{df}}{=} \bigcap_{V(K)} \mathrm{H}^2(\mathrm{O}_v).$$

We write $\mathrm{H}^2_{\mathrm{nr}}(K)$ if the sum is over all discrete valuations on K.

Purity for curves 4.1. Let C be a smooth integral projective curve over a field k, with function field F. Then

$$\mathrm{H}^2(C) = \mathrm{H}^2_{\mathrm{nr}}(F/k).$$

This is proved in the affine case for the Brauer group in [Ho, Th.], and extended using the fact that Br is a Zariski sheaf, as in [S1, Th. 1.4].

Let X be a two-dimensional regular noetherian scheme. Then by [GB, II, 2.7], $\mathrm{Br}(X) = \mathrm{H}^2(X, \mathrm{G}_m)$. Let

$$\bar{\mathrm{H}}^2(X) \stackrel{\mathrm{df}}{=} {}_n\mathrm{H}^2(X, \mathrm{G}_m)$$

denote the n-torsion subgroup, where n is as in Sect. 2. For any regular quasi-compact integral scheme X with function field K, the natural map $\mathrm{H}^2(X, \mathrm{G}_m) \to \mathrm{H}^2(K, \mathrm{G}_m)$ is injective [M, III.2.22]. Thus we may view $\bar{\mathrm{H}}^2(X)$ as the image of $\mathrm{H}^2(X)$ in $\mathrm{H}^2(K)$. Since $\mathrm{H}^2(X) \to \mathrm{H}^2(K)$ factors through $\mathrm{H}^2(\mathrm{O}_v)$ for any $v \in V_X(K)$, we have

$$\bar{\mathrm{H}}^2(X) \subset \bigcap_{V_X(K)} \mathrm{H}^2(\mathrm{O}_v).$$

Using Auslander–Goldman's theorem [AG, Prop. 7.4] and the fact that Br is a Zariski sheaf, it is not hard to prove the following ([GB, II, Prop. 2.3], or [S1, Th. 1.4]).

Purity for Surfaces 4.2. *If X is a regular integral noetherian surface, then*

$$\bar{\mathrm{H}}^2(X) = \bigcap_{V(X)} \mathrm{H}^2(\mathrm{O}_v).$$

If X is projective over $S = \operatorname{Spec} R$, then $\bar{\mathrm{H}}^2(X) = \mathrm{H}^2_{\mathrm{nr}}(K/R)$.

We will use purity for surfaces in two ways, first to show that when $S = \operatorname{Spec} \mathbb{Z}_p$, to split $\alpha \in \mathrm{H}^2(K)$ it is sufficient to construct a finite separable extension L/K over which $\partial_w(\alpha) = 0$ for all $w \in V(L)$ (Theorem 4.5); and second, to prove a local structure theorem for $\mathrm{H}^2(K)$, which provides the computational foothold we need in order to construct such an L locally.

Lemma 4.3. *Let S be a henselian local scheme, let $Y \to S$ be a proper S-scheme, and let $Y_0 \to S_0$ be the closed fiber. Then for all $q \geq 0$,*

$$\mathrm{H}^q(Y) = \mathrm{H}^q(Y_0).$$

This is a corollary to the proper base change theorem ([GB, III, 3] or [M, VI.2.7]).

Lemma 4.4. *Let Y_0 be a normal crossings divisor on an arithmetic surface Y, and let $\{D_i\}$ denote Y_0's irreducible components. Then the natural map $\mathrm{H}^2(Y_0) \to \bigoplus_i \mathrm{H}^2(D_i)$ is injective.*

This is [S1, Lemma 3.2], and it is also in [GB, III]. The following fundamental result is [S2, Th. 0.9].

Theorem 4.5. *If L is the function field of a p-adic curve, and n is prime-to-p, then $\mathrm{H}^2_{\mathrm{nr}}(L) = 0$. Thus if $\alpha_L \in \mathrm{H}^2(L)$, and $\partial_w(\alpha_L) = 0$ for all $w \in V(L)$, then $\alpha_L = 0$.*

Proof. Let $S = \operatorname{Spec} \mathbb{Z}_p$. By Existence of Surfaces (3.9) there is an arithmetic surface $Y \to S$ with function field L, such that the closed fiber Y_0 has normal crossings. Every discrete valuation on L has a center on S, so $\mathrm{H}^2_{\mathrm{nr}}(L/\mathbb{Z}_p) = \mathrm{H}^2_{\mathrm{nr}}(L)$. We then have $\mathrm{H}^2_{\mathrm{nr}}(L) = \bar{\mathrm{H}}^2(Y)$ by Purity for Surfaces (4.2), and $\mathrm{H}^2(Y) = \mathrm{H}^2(Y_0)$ by Lemma 4.3. Therefore since $\mathrm{H}^2(Y) \to \bar{\mathrm{H}}^2(Y)$ is surjective, it suffices to show $\mathrm{H}^2(Y_0) = 0$. The second statement then follows immediately.

Let $k = \mathbb{F}_p$. Y_0 is projective over k by [Liu, 8.3.6(a)], and since Y_0 has normal crossings, the irreducible components C of Y_0 are regular and projective over k, and $\mathrm{H}^2(Y_0) \subset \bigoplus \mathrm{H}^2(C)$ by Lemma 4.4. Let $F = k(C)$. Since k is finite, $V_k(F) = V(F)$ is the set of all normalized discrete valuations on F, and C is smooth over k by [Liu, 8.3.33]. Therefore, by Purity for Curves (4.1),

$$\mathrm{H}^2(C) \;=\; \bigcap_{V(F)} \mathrm{H}^2(\mathrm{O}_v)$$

On the other hand, by Class Field Theory we have an exact sequence

$$0 \to \mathrm{H}^2(F) \to \bigoplus_{V(F)} \mathrm{H}^1(\kappa(v)) \to \mathrm{H}^1(k) \to 0$$

(see [M, III.2.22(g)] and [GB, III, Remark 2.5b]). We conclude $\mathrm{H}^2(C) = 0$ by (2.1), hence $\mathrm{H}^2(Y_0) = 0$, as desired. □

5 Modified Picard Group

We briefly summarize [S2, Sect. 1], which shows how, on an arithmetic surface over a complete discrete valuation ring, we can represent a divisor class whose restriction to the closed fiber is an n-th power by a divisor that is itself an n-th power, while avoiding a fixed finite set of closed points. The results of this section will not be applied until the very end.

Let X be a projective scheme with no embedded points over an affine scheme. This hypothesis applies to an arithmetic surface over an affine Dedekind scheme, or one of its closed fibers. Let $\underline{z} = \{z_i\}_I \subset X$ be a finite set of closed points, and let $\iota : \underline{z} \to X$ be the closed immersion so that $\iota_* \mathrm{O}^*_{\underline{z}} = \bigoplus_I \iota_{i*} \kappa(z_i)^*$. Let ${}_{\underline{z}}\mathrm{O}^*_X$ denote the sheaf of units with value 1 at each z_i, defined by the exact sequence

$$1 \longrightarrow {}_{\underline{z}}\mathrm{O}^*_X \longrightarrow \mathrm{O}^*_X \longrightarrow \iota_* \mathrm{O}^*_{\underline{z}} \longrightarrow 1.$$

Let K_X denote the (quasi-coherent) sheaf of total fractions of X. We have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & {}_{\underline{z}}\mathrm{O}^*_X & \longrightarrow & K^*_X & \longrightarrow & K^*_X/{}_{\underline{z}}\mathrm{O}^*_X & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{O}^*_X & \longrightarrow & K^*_X & \longrightarrow & K^*_X/\mathrm{O}^*_X & \longrightarrow & 1 \end{array} \tag{5.1}$$

Set

$$\operatorname{Div} X = \mathrm{H}^0(X, K^*_X/\mathrm{O}^*_X) \qquad \operatorname{Pic} X = \mathrm{H}^1(X, \mathrm{O}^*_X)$$
$${}_{\underline{z}}\operatorname{Div} X = \mathrm{H}^0(X, K^*_X/{}_{\underline{z}}\mathrm{O}^*_X) \qquad {}_{\underline{z}}\operatorname{Pic} X = \mathrm{H}^1(X, {}_{\underline{z}}\mathrm{O}^*_X)$$

${}_{\underline{z}}\operatorname{Div} X = \mathrm{H}^0(X, K^*_X/{}_{\underline{z}}\mathrm{O}^*_X)$ is the set of $\{(U_j, f_j)\}$ such that not only is f_j/f_k a unit on $U_j \cap U_k$, but $(f_j/f_k)(z) = 1$ for each $z \in \underline{z} \cap (U_j \cap U_k)$. By definition, we have an exact sequence

$$1 \longrightarrow \iota_* \mathrm{O}^*_{\underline{z}} \longrightarrow K^*_X/{}_{\underline{z}}\mathrm{O}^*_X \longrightarrow K^*_X/\mathrm{O}^*_X \longrightarrow 1. \tag{5.2}$$

Since $\iota_* \mathrm{O}^*_{\underline{z}}$ and K^*_X are flasque, by (5.1) we have an exact diagram

$$\begin{array}{ccccccc}
\mathrm{H}^0(X,K^*_X) & \longrightarrow & {}_{\underline{z}}\mathrm{Div}\,X & \longrightarrow & {}_{\underline{z}}\mathrm{Pic}\,X & \longrightarrow & 1 \\
\| & & \downarrow & & \downarrow & & \\
\mathrm{H}^0(X,K^*_X) & \longrightarrow & \mathrm{Div}\,X & \longrightarrow & \mathrm{Pic}\,X & \longrightarrow & 1 \\
& & \downarrow & & \downarrow & & \\
& & 1 & & 1 & &
\end{array}$$

Let ${}_{\underline{z}}\mathrm{Div}'X \le {}_{\underline{z}}\mathrm{Div}\,X$ and $\mathrm{Div}'X \le \mathrm{Div}\,X$ denote the groups of divisors whose support avoids $\underline{z}$. By [S2, Prop. 1.5], the map ${}_{\underline{z}}\mathrm{Div}'X \to \mathrm{Div}'X$ is onto, hence we have

$$\begin{array}{ccccccc}
{}_{\underline{z}}K^* & \longrightarrow & {}_{\underline{z}}\mathrm{Div}'X & \longrightarrow & {}_{\underline{z}}\mathrm{Pic}\,X & \longrightarrow & 1 \\
\| & & \downarrow & & \downarrow & & \\
{}_{\underline{z}}K^* & \longrightarrow & \mathrm{Div}'X & \longrightarrow & \mathrm{Pic}\,X & \longrightarrow & 1 \\
& & \downarrow & & \downarrow & & \\
& & 1 & & 1 & &
\end{array} \tag{5.3}$$

where ${}_{\underline{z}}K^* \le \mathrm{H}^0(X,K^*_X)$ is the inverse image of the subgroup ${}_{\underline{z}}\mathrm{Div}'X \le {}_{\underline{z}}\mathrm{Div}\,X$ in $\mathrm{H}^0(X,K^*_X)$. These are the meromorphic functions whose values at $z \in \underline{z}$ are invertible.

The long exact sequence associated to (5.2) induces a split exact sequence

$$1 \longrightarrow \bigoplus\nolimits_{\underline{z}} \kappa(z_i)^* \longrightarrow {}_{\underline{z}}\mathrm{Div}'X \longrightarrow \mathrm{Div}'X \longrightarrow 1.$$

The injection splits via the evaluation map, which is well defined since $(f_j/f_k)(z) = 1$ for all $z \in \underline{z} \cap (U_j \cap U_k)$, whenever $\{(U_j, f_j)\} \in {}_{\underline{z}}\mathrm{Div}'X$. We obtain

$${}_{\underline{z}}\mathrm{Pic}\,X \simeq \left(\left(\bigoplus\nolimits_{\underline{z}} \kappa(z_i)^*\right) \oplus \mathrm{Div}'X\right) / {}_{\underline{z}}K^* \tag{5.4}$$

where $f \in {}_{\underline{z}}K^*$ maps to the pair $((f(z_i))_{\underline{z}}, \{(X,f)\})$. This is [S2, Prop. 1.6]. Thus, ${}_{\underline{z}}\mathrm{Pic}\,X$ comprises the classes of divisors on X whose support avoids $\underline{z}$, paired with a tuple of nonzero values at each $z \in \underline{z}$.

Proposition 5.5. *Suppose $S = \mathrm{Spec}\,R$ for a complete discrete valuation ring R, and $X \to S$ is an arithmetic surface such that X_0 has normal crossings. Let n be a number invertible on X. Then the canonical map induces an isomorphism*

$${}_{\underline{z}}\mathrm{Pic}\,X/n \xrightarrow{\sim} {}_{\underline{z}}\mathrm{Pic}((X_0)_{\mathrm{red}})/n.$$

This is [S2, Prop. 1.7]. The proof uses standard algebraic geometry facts and an elementary version of Grothendieck's Existence Theorem [Liu, 10.Exercise 4.4]. If $\underline{z} = \varnothing$, we obtain $\mathrm{Pic}\,X/n \simeq \mathrm{Pic}(X_0)_{\mathrm{red}}/n$, which is [S2, Th. 1.2].

6 An Exact Sequence for Local Surfaces

Standing setup 6.1. We need to consider splitting at the three types of closed points that may occur when D has normal crossings on an arithmetic surface. We say z is a *distant point of* D if it does not belong to D, a *curve point of* D if it belongs to exactly one component of D, and a *nodal point of* D if it belongs to two. We will use the following notation for the rest of the paper.

- $S = \operatorname{Spec} R$ is an excellent one-dimensional affine Dedekind scheme.
- $X \to S$ is an arithmetic surface with function field $K = F(X)$.
- X_0 is a closed fiber of $X \to S$.
- z is a closed point on X.
- $A = (A, \mathfrak{m}, k)$ is the local ring $\mathrm{O}_{X,z}$, a two-dimensional excellent regular noetherian local ring with fraction field K.
- π_0, π_1 are two (regular) primes of A generating $\mathfrak{m}$.
- $v_0, v_1 \in V(A)$ are the discrete valuations corresponding to π_0, π_1.
- n is a number relatively prime to char $\kappa(x)$ for all $x \in X$.
- $\alpha \in \mathrm{H}^2(K) = \mathrm{H}^2(K, \mu_n)$.
- $\theta_v = \partial_v(\alpha) \in \mathrm{H}^1(\kappa(v))$ for each $v \in V(K)$.
- D_α is the ramification divisor of α on X.
- $D_\alpha^+ = D_\alpha \cup (X_0)_{\mathrm{red}}$.
- If D_α has normal crossings and α ramifies on A, then $\operatorname{div}_A(\alpha) = \{v_0\}$ if $z \in D_\alpha$ is a curve point, and $\operatorname{div}_A(\alpha) = \{v_0, v_1\}$ if $z \in D_\alpha$ is a nodal point.

The excellent hypothesis on R induces excellence on A and X, and this is needed for Lipman's embedded resolution theorem, to produce an arithmetic surface on which α ramifies at at most two normal crossings divisors.

Assume Setup 6.1. There is an exact sequence

$$0 \to \mathrm{H}^2(A) \to \mathrm{H}^2(K) \to \bigoplus_{v \in V(A)} \mathrm{H}^1(\kappa(v)). \tag{6.2}$$

Exactness at $\mathrm{H}^2(K)$ is Purity for Surfaces 4.2, and at $\mathrm{H}^2(A)$ it is [AG, Th. 7.2].

6.3. Assume Setup 6.1, and suppose $v \in V(A)$, $\mathfrak{p} = \mathfrak{p}_v \cap A$, and $R_v = A/\mathfrak{p} \subset \kappa(v)$. Let z be the closed point of $\operatorname{Spec} A$, and $\bar{z}$ its image on $\operatorname{Spec} R_v$. Let $\widetilde{R}_v$ denote the normalization of R_v in $\kappa(v)$, a one-dimensional semi-local normal noetherian ring. Let $\mathfrak{n}_1, \ldots, \mathfrak{n}_d$ denote the primes of $\widetilde{R}_v$ extending the image $\bar{\mathfrak{m}}$ of $\mathfrak{m}$ in R_v, let $w_1, \ldots, w_d$ denote the corresponding discrete valuations on $\kappa(v)$, let $\widetilde{R}_i$ be the localization of $\widetilde{R}_v$ at $\mathfrak{n}_i$, and let $k_i = \widetilde{R}_i/\mathfrak{n}_i$. Define

$$\partial_{v,\bar{z}} \stackrel{\mathrm{df}}{=} \sum_{i=1}^{d} \operatorname{cor}_{k_i|k} \circ \partial_{w_i} : \mathrm{H}^q(\kappa(v)) \to \mathrm{H}^{q-1}(k)$$

$$\partial_z \stackrel{\mathrm{df}}{=} \sum_{V(A)} \partial_{v,\bar{z}} : \bigoplus_{V(A)} \mathrm{H}^q(\kappa(v)) \to \mathrm{H}^{q-1}(k)$$

Let $m_i = |\mu_n(k_i)|$ and fix a primitive n-th root of unity ζ_n. Then

$$\mathrm{H}^0(k_i) = \mu_n^{-1}(k_i) = \mathrm{Hom}(\mu_n, \tfrac{1}{m_i}\mathbb{Z}/\mathbb{Z})$$

is generated by the element $\zeta_{m_i}^*$ defined by $\zeta_{m_i}^*(\zeta_n) = 1/m_i$.

Theorem 6.4. *Let A be a two-dimensional excellent regular noetherian local ring with residue field k and fraction field K. Then the following sequence is exact.*

$$0 \to \mathrm{H}^2(A) \to \mathrm{H}^2(K) \to \bigoplus_{v \in V(A)} \mathrm{H}^1(\kappa(v)) \xrightarrow{\partial_z} \mathrm{H}^0(k) \to 0.$$

Exactness at the direct sum is [S3, Th. 5.2, Th. 6.12], and the rest is (6.2).

7 Computations

Suppose K is the function field of a p-adic curve, n is a number not divisible by p, and $\alpha \in \mathrm{H}^2(K)$. By Existence of Surfaces (3.9), there is an arithmetic surface $X \to S = \mathrm{Spec}\,\mathbb{Z}_p$ with function field K. To split α we will construct a finite separable extension L/K over which $\partial_w(\alpha_L) = 0$ for all $w \in V_A(L)$, for all two-dimensional local rings $A = \mathrm{O}_{X,z}$ on X. Since each $w \in V(L)$ has a center on X, we obtain $\partial_w(\alpha_L) = 0$ for all $w \in V(L)$, so $\alpha_L = 0$ by Theorem 4.5.

To carry out this program we will lift z-unramified elements of $\mathrm{H}^1(\kappa(v))$ (in Theorem 6.4) to $\mathrm{H}^1(A) \subset \mathrm{H}^1(K)$, in order to compute α and α_L explicitly. In general such lifts do not exist, as shown by the classic Wang counterexample [AT, Chap. X]. Therefore, we are led to impose the following.

Hypothesis 7.1. Assume Setup 6.1, and D_α has normal crossings at z. Then (a) $\mu_r \subset A$, where $r = |\partial_z(\theta_{v_0})|$, and (b) the map $\mathrm{H}^1(A) \to \mathrm{H}^1(A/(\pi_i))$ is onto, for $i = 0, 1$.

Proposition 7.2. *In Setup 6.1, assume D_α has normal crossings at z. Then Hypothesis 7.1(b) holds if $\mu_n \subset K$, or if n is prime. In particular, if $\mu_n \subset K$, or if n is prime and $\partial_z(\theta_{v_0}) = 0$, then Hypothesis 7.1 holds.*

Proof. Suppose $\mu_n \subset K$. Then $\mu_n(K) = \mu_n(A)$ since A is integrally closed. Let $R_i = A/(\pi_i)$. Since μ_n is contained in A and R_i, we have $\mathrm{H}^1(A) \simeq \mathrm{H}^1(A, \mu_n)$ and $\mathrm{H}^1(R_i) \simeq \mathrm{H}^1(R_i, \mu_n)$, and since A and R_i are factorial, $\mathrm{H}^1(A) \to \mathrm{H}^1(R_i)$ is equivalent to the Kummer map $A^*/n \to R_i^*/n$. This map is onto since A is a local ring: If $u \in A$ and $\bar{u} \in R_i^*$, then $\bar{u}\bar{v} = 1$ in R_i^* lifts to $uv = 1 - x$ for a nonunit $x \in A$, and since A is local, uv is a unit, hence $u \in A^*$. Therefore (7.1) holds.

Suppose n is prime. Let R_i be as above. Let $A \to A'$ and $R_i \to R_i'$ be the étale base changes with respect to $\mathbb{Z}[T]/(1 + T + \cdots + T^{n-1})$. Then A' is normal by [M, I.3.17], so it is a product of normal domains ([Mat, p. 64]), each an excellent two-dimensional regular noetherian semilocal ring. Similarly R_i' is a product of excellent one-dimensional normal noetherian semilocal domains. The map $A' \to R_i'$

is onto by base change. We *claim* $\mathrm{H}^1(A') \to \mathrm{H}^1(R_i')$ is onto. Since A' and R_i' are factorial, and each contains n-th roots of unity, we have compatible isomorphisms $\mathrm{H}^1(A') \simeq (A')^*/n$ and $\mathrm{H}^1(R_i') \simeq (R_i')^*/n$, and it suffices to show $(A')^* \to (R_i')^*$ is onto. It then suffices to show every nonunit of A' maps to a nonunit R_i'. But $A' \to A' \otimes_A A/\mathfrak{p}$ is surjective by base change, and $\mathfrak{p}A' \subset \mathfrak{m}A'$ is contained in every maximal ideal of A', since $A \to A'$ is étale. Thus each nonunit of A' maps to a nonunit of $A'/\mathfrak{p}A'$, so $(A')^* \to (R_i')^*$ is onto, which proves the claim.

If $\theta_i \in \mathrm{H}^1(R_i)$, then $\mathrm{cor} \circ \mathrm{res}(\theta_i) = (n-1)\theta_i$. Let $\theta' \in \mathrm{H}^1(A')$ map to $\theta_i' = \mathrm{res}(\theta_i)$. Then $\mathrm{cor}(\theta') \in \mathrm{H}^1(A)$ maps to $(n-1)\theta_i$ by the compatibility of corestriction and base change, and since $n-1$ is invertible (mod n), we conclude θ_i has a preimage in $\mathrm{H}^1(A)$. Therefore $\mathrm{H}^1(A) \to \mathrm{H}^1(R_i)$ is onto. Therefore (7.1(b)) holds. □

The next result gives us our main computational foothold, the second main application of Purity for Surfaces (4.2).

Local Structure Theorem 7.3. *Assume Hypothesis 7.1. Let ζ_m^* be as in (6.3), with $m = |\mu_n(K)|$. Then there exist elements $\alpha^\circ \in \mathrm{H}^2(A)$ and $\theta_i \in \mathrm{H}^1(A)$ such that*

$$\alpha = \alpha^\circ + (\theta_0, \pi_0) + (\theta_1, \pi_1) + (s\zeta_m^* \cdot (\pi_1), \pi_0)$$

where $s\zeta_m^* = \partial_{v_0,\bar{z}}(\theta_{v_0}) = -\partial_{v_1,\bar{z}}(\theta_{v_1})$, for $\theta_{v_i} = \partial_{v_i}(\alpha)$. If z is a curve point of D_α, $\theta_1 = 0$ and $s = 0$.

Proof. Since $\{v_0, v_1\}$ has normal crossings, we have $\partial_{v_0,\bar{z}}(\theta_{v_0}) + \partial_{v_1,\bar{z}}(\theta_{v_1}) = 0$ by Theorem 6.4, hence $\partial_{v_0,\bar{z}}(\theta_{v_0}) = -\partial_{v_1,\bar{z}}(\theta_{v_1}) = s\zeta_m^*$, for some $0 \le s < m$. Of course, if z is a curve point for α then $\theta_{v_1} = 0$ and $s = 0$.

Since $\{v_0, v_1\}$ has normal crossings, v_1 defines a discrete valuation on $\kappa(v_0)$ with residue field k. Let $R_i = A/(\pi_i)$. By Hypothesis 7.1, $\mu_r \subset A$, where $r = |s\zeta_m^*|$. The choice of π_1 then determines a splitting $\mathrm{H}^0(k, \mu_r^{-1}) \to \mathrm{H}^1(\kappa(v_0), \mathbb{Z}/r) \le \mathrm{H}^1(\kappa(v_0), \mathbb{Z}/n)$ of (2.1), so that $\theta_{v_0} = \theta_{v_0}^\circ + s\zeta_m^* \cdot (\bar{\pi}_1)$ for some $\theta_{v_0}^\circ \in \mathrm{H}^1(R_0)$. Since $\mathrm{H}^1(A) \to \mathrm{H}^1(R_i)$ is onto by (7.1), $\theta_{v_0}^\circ$ lifts to some $\theta_0 \in \mathrm{H}^1(A)$. Choose θ_1 similarly, and set

$$\beta = (\theta_0, \pi_0) + (\theta_1, \pi_1) + (s\zeta_m^* \cdot (\pi_1), \pi_0).$$

Then $\partial_v(\alpha) = \partial_v(\beta)$ at all $v \in V(K)$ by (2.2), so $\alpha^\circ = \alpha - \beta$ is in $\mathrm{H}^2(A)$ by Purity for Surfaces (4.2). □

Lemma 7.4. *Assume Hypothesis 7.1. Then in the notation of Theorem 7.3, for each $v \in V(K)$,*

$$\partial_v(\alpha) = \left[a(\theta_0 + s\zeta_m^* \cdot (\pi_1)) + b(\theta_1 - s\zeta_m^* \cdot (\pi_1)) + abs\zeta_m^* \cdot (-1)\right]_{\kappa(v)}$$

where the terms are interpreted in K_v, $a = v(\pi_0)$, and $b = v(\pi_1)$. If $v \in V_z(K)$, then ∂_v factors through k.

Proof. Since we assume (7.1) we can apply Theorem 7.3. Using (2.2) and formula (2.5), we compute directly over K_v

$$\begin{aligned}\partial_v(\alpha) &= [a\theta_0 + b\theta_1 + \partial_v(s\zeta_m^* \cdot (\pi_1)\cdot(\pi_0))]_{\kappa(v)}\\ &= [a\theta_0 + b\theta_1 + s\zeta_m^* \cdot (a(\pi_1) - b(\pi_0) + ab(-1))]_{\kappa(v)}.\end{aligned}$$

If $v \in V_z(K)$ then $k \subset \kappa(v)$ by (1.1), and since the terms in $\partial_v(\alpha)$ are originally defined over A, over $\kappa(v)$ they are defined over k. Thus ∂_v factors through k. □

The following simple computation gives us the main tool we need for splitting α's residues.

Lemma 7.5. *Assume Hypothesis 7.1, and*

$$\alpha = \alpha^\circ + (\theta_0, \pi_0) + (\theta_1, \pi_1) + (s\zeta_m^* \cdot (\pi_1), \pi_0)$$

as in Theorem 7.3. Suppose

$$L = K(f^{1/n})$$

where, if z is a nodal point of D_α, $f = u\pi_0^{c_0}\pi_1^{c_1} \in A$, for some $u \in A^*$ and numbers $c_i \geq 0$; and if z is a curve point of D_α, so $\theta_1 = 0$ and $s = 0$, then $f = u_0\pi_0^{c_0}$, with $c_0 \geq 0$ and $u_0 \in A$ not divisible by π_0. Then when z is a nodal point of D_α,

$$\begin{aligned}c_0\alpha_L &= [c_0\alpha^\circ - (\theta_0, u) + (-c_1\theta_0 + c_0\theta_1 + (s\zeta_m^* \cdot ((u) + c_1(-1)), \pi_1)]_L\\ -c_1\alpha_L &= [-c_1\alpha^\circ + (\theta_1, u) + (-c_1\theta_0 + c_0\theta_1 + (s\zeta_m^* \cdot ((u) + c_0(-1)), \pi_0)]_L\end{aligned}$$

and when z is a curve point of D_α, $c_0\alpha_L = (c_0\alpha^\circ - (\theta_0, u_0))_L$.

Proof. The first part is proved by substituting the relations $(f)_L = ((u) + c_0(\pi_0) + c_1(\pi_1))_L = 0$ and $(\pi)\cdot(-\pi) = 0$ into the given expression for α_L. All of this is formal, so the last part is immediate. □

Corollary 7.6. *Assume the situation and notation of Lemma 7.5, and let $w \in V_A(L)$. Then:*

a. If $z \notin D_\alpha$ then $\partial_w(\alpha) = 0$.
b. If $z \in D_\alpha$ is a nodal point,

$$c_0\partial_w(\alpha) = w(\pi_1)(-c_1\theta_0 + c_0\theta_1 + s\zeta_m^* \cdot ((u) + c_1(-1)))_{\kappa(w)}.$$

If $z \in D_\alpha$ is a curve point, then $c_0\partial_w(\alpha) = -w(u_0)(\theta_0)_{\kappa(w)}$.
c. If $z \in D_\alpha$ is a nodal point and $c_0, c_1 \in (\mathbb{Z}/n)^*$, or if $z \in D_\alpha$ is a curve point and $c_0 \in (\mathbb{Z}/n)^*$, then $\partial_w(\alpha) = 0$ whenever w has codimension-one center on A.
d. If $z \in \operatorname{div} f$ is a curve point and $c_0 \in (\mathbb{Z}/n)^*$, then $\partial_w(\alpha) = 0$.
e. Suppose $z \in D_\alpha$ is a nodal point, $c_0, c_1 \in (\mathbb{Z}/n)^*$, w_i extends v_i for $i = 0, 1$, $c_1\theta_0(z) = c_0\theta_1(z)$, and $s = 0$. Then

$$\alpha(w_0)(\bar{z}) = \alpha^\circ - (c_0^{-1}\theta_0(z), u) = \alpha^\circ - (c_1^{-1}\theta_1(z), u) = \alpha(w_1)(\bar{z}).$$

f. Suppose $z \in D_\alpha$ is a nodal point, $c_0, c_1 \in (\mathbb{Z}/n)^*$, and w_i extends v_i for $i = 0, 1$. Then $\alpha_{L_{w_i}} = \alpha(w_i)$ is defined over $\kappa(v_i)$ for $i = 0, 1$, and

$$c_0 \cdot \partial_{v_0,\bar{z}}(\alpha(w_0)) = -c_1 \cdot \partial_{v_1,\bar{z}}(\alpha(w_1)).$$

Proof. In (a), if $z \notin D_\alpha$, then $\partial_v(\alpha) = 0$ for all $v \in V(A)$ by definition, hence $\alpha \in \mathrm{H}^2(\mathrm{O}_v)$ for all $v \in V(K)$ by Purity for Surfaces (4.2), hence $\partial_w(\alpha) = 0$ by (2.4). Part (b) is immediate by Lemma 7.5 and (2.2).

In (c), let $v \in V(K)$ be the normalized valuation corresponding to $w|_K$, and assume $v \in V(A)$. If z is a nodal point of D_α then $f = u\pi_0^{c_0}\pi_1^{c_1}$, and by Lemma 1.2, $w(\pi_1) = e(w/v)v(\pi_1)$ and $e(w/v) = n/\gcd(v(f), n)$. Since $v \in V(A)$, $v(\pi_1)$ equals 0 or 1, and in the latter case $v(f) = c_1 \in (\mathbb{Z}/n)^*$, so $e(w/v) = 0 \pmod n$. Therefore, $w(\pi_1) = 0 \pmod n$. If z is a curve point of D_α then $f = u_0\pi_0^{c_0}$, and since π_0 does not divide u_0 and $v \in V(A)$, we compute similarly $w(u_0) = 0(\mod n)$. In any case $c_0\partial_w(\alpha) = 0$, and since $c_0 \in (\mathbb{Z}/n)^*$, we conclude $\partial_w(\alpha) = 0$ by (b).

In (d), if z is a curve point of $\operatorname{div} f$ then $D_\alpha = \operatorname{div} \pi_0$, $\theta_1 = 0$, $s = 0$, and u_0 is a unit of A. Since $c_0 \in (\mathbb{Z}/n)^*$ this implies $\partial_w(\alpha) = 0$ by (b). Part (e) is immediate by Lemma 7.5 and (2.2).

In (f), each w_i/v_i is totally ramified of degree n by Lemma 1.2, hence $\kappa(w_i) = \kappa(v_i)$, and $\alpha_{L_{w_i}} = \alpha(w_i)$ by definition, since $\partial_{w_i}(\alpha) = 0$ by (2.4). Using the computation of $c_0\alpha_L$ and $-c_1\alpha_L$ in (7.5), we find the computation of $\partial_{v_i,\bar{z}}(\alpha(w_i))$ is now simple, and we obtain $c_0\,\partial_{v_0,\bar{z}}(\alpha(w_0)) = -c_1\,\partial_{v_1,\bar{z}}(\alpha(w_1))$. Note (-1) has order 2, so if n is odd, then $s\zeta_m^* \cdot (-1) = 0$, and if n is even, then both c_0 and c_1 are odd, so $(c_0 + c_1)s\zeta_m^* \cdot (-1) = 0$ in any case. □

The following elementary lemma, which appears as [S1′, Lemma], was supplied by Colliot-Thélène.

Weak Approximation Lemma 7.7. *Let X be an arithmetic surface over an affine scheme, let D be an effective divisor, let $p_1, \dots, p_r$ be closed points on X not on D, and let $q_1, \dots, q_s$ be closed points on D. Then for any $a_i \in \kappa(p_i)^*$, there exists $f \in F(X)^*$ such that*

(i) $\operatorname{div} f = D + E$, *where D and E have no common components and E does not go through any of the p_i or q_j.*
(ii) $f \in \mathrm{O}_{X,p_i}^*$ for each p_i, and the image of f in $\kappa(p_i)^*$ is a_i.

Global Splitting Lemma 7.8. *Assume Setup 6.1 and $\mu_n \subset K$. Then there exists a field extension L/K of degree n^2 such that $\partial_w(\alpha_L) = 0$ for all $w \in V(L)$.*

Proof. Since $\mu_n \subset K$, (7.1) holds, by Proposition 7.2. Since every $w \in V(L)$ has a center on X, by Purity for Surfaces 4.2 it is enough to construct an L such that $\partial_w(\alpha) = 0$ for all $w \in V_A(L)$, for all $A = (A, \mathfrak{m}_z, \kappa(z))$. Apply Lemma 7.7 to choose $f \in K$ such that

$$\operatorname{div} f = D_\alpha + D_\varepsilon$$

where D_ε contains none of the (finitely many) self-intersection points of D_α. Let L be an extension containing $K(f^{1/n})$, $w \in V_A(L)$. By Corollary 7.6(a), (c), and (d), we may assume z lies on D_α, on more than one irreducible component of $\operatorname{div} f$, and that $w \in V_z(L)$. By Lemma 7.5, $\alpha_{K(f^{1/n})}$ has the form

$$\alpha_{K(f^{1/n})} = \alpha_0 + (\lambda, \pi_0)$$

where α_0 and λ are defined over A. Since A contains the n-th roots of unity, $\lambda = \zeta_m^* \cdot (u_z)$ for some $u_z \in A^*$ by Kummer theory. By Lemma 7.7, there exists $g \in K^*$ such that $g \in A$ and $g = u_z \pmod{\mathfrak{m}_z}$, for each z. Let

$$L = K(f^{1/n}, g^{1/n}).$$

We compute $\partial_w(\alpha) = w(\pi_0)\lambda_{\kappa(w)}$. Since $w \in V_z(L)$, $\kappa(z) \subset \kappa(w)$ by (1.1). Since λ is defined over A, its restriction to $\kappa(w)$ factors through $\kappa(z)$, and by construction $\lambda_{\kappa(w)} = 0$, since $(u_z)_{\kappa(w)} = 0$. Therefore, $\partial_w(\alpha) = 0$ for all $w \in V(L)$. □

Period-Index Theorem 7.9. *Suppose K has transcendence degree one over a p-adic field, and $\alpha \in \mathrm{Br}(K)$ has prime-to-p period. Then* $\mathrm{ind}(\alpha)$ *divides* $\mathrm{per}(\alpha)^2$

Proof. Recall $\mathrm{ind}(\alpha)$ is the smallest degree of any separable splitting field, and $\mathrm{per}(\alpha)$ is the order of α in $\mathrm{Br}(K)$. Suppose $\alpha \in \mathrm{H}^2(K)$ has period n. If $\mu_n \subset K$ and L is as in Lemma 7.8, then $\alpha_L = 0$ by Theorem 4.5. If n is prime, then $K(\mu_n)/K$ has prime-to-n degree, and we obtain the result by the standard restriction-corestriction argument. In the general case, we induct on the prime degree case. For if q is a prime dividing n, and $q\alpha$, which has period n/q, has index dividing $(n/q)^2$, then there is a separable extension F/K of degree $(n/q)^2$ such that $q\alpha_F = 0$, hence α_F has period q, so by the base case there is an extension L/F of degree q^2 splitting α, and now L/F has degree n^2. □

8 Program for Splitting in Prime Degree

Assume $\alpha \in \mathrm{H}^2(K)$ has prime index q. By a theorem of Albert, α is cyclic if it is split by a field extension of the form $L = K(f^{1/q})$, for $f \in K$. Therefore by Theorem 4.5, if K is the function field of a p-adic curve, then to show α is cyclic it is enough to find an f such that $\partial_w(\alpha) = 0$ for all $w \in V(L)$. In this section, we produce a blueprint for constructing such an f.

Semiramified case 8.1. We say α is *semiramified at v* if α_{K_v} is semiramified, i.e., $\alpha_{K_v} = (\theta_v, \pi_v) \neq 0$ for some uniformizer $\pi_v \in K_v$, where $\theta_v = \mathrm{inf}_{\kappa(v)|K_v}(\partial_v(\alpha))$. We will usually suppress notation for the inflation map in this context. Since $\alpha(v) = \alpha_{K_v(\theta_v)}$,

$$\mathrm{ind}(\alpha_{K_v}) = |\theta_v| \,\mathrm{ind}(\alpha(v))$$

by Nakayama-Witt's index formula. Thus if $\mathrm{ind}(\alpha) = |\theta_v| \neq 1$ then $\alpha(v) = 0$, and α is semiramified at v. For example, when $\mathrm{ind}(\alpha)$ is prime, α is semiramified at each $v \in \mathrm{div}_K(\alpha)$.

Lemma 8.2. *Assume Setup 6.1. Suppose $\alpha \in \mathrm{H}^2(K)$ is semiramified at $v \in V(K)$, $L = K(f^{1/n})$, and $v(f) = c$. If w extends v to L, then $c \cdot \alpha_{L_w} = (-\theta_v, u)$ where $\theta_v = \partial_v(\alpha)$, and $u \in \mathrm{O}_v^*$ is defined by $f = u\pi_v^c$, for a uniformizer π_v in O_v.*

Proof. Since α is semiramified at v, $\alpha_{K_v} = (\theta_v, \pi_v)$ for a uniformizer $\pi_v \in \mathrm{O}_v$. Since $v(f) = c$, $f = u\pi_v^c$ for some $u \in \mathrm{O}_v^*$. Then $(f)_L = 0 = c(\pi_v) + (u)$, so $c\,\alpha_{L_w} = (-\theta_v, u)$. □

Remark 8.3. In Saltman's terminology ([S2, p. 821]), $\alpha(w)$ is *split by the ramification* whenever L/K is v-totally ramified and $\alpha(w) \in \mathrm{H}^2(\kappa(v))$ is split by $\kappa(v)(\theta_v)$. Since we are calling the images of ∂_v "residues" instead of "ramification", we would say instead that $\alpha(w)$ is *split by the residue*. When α is semiramified at v, the values of α are split by the residue at all v-totally ramified L/K. This happens, for example, whenever α has prime index and $D_\alpha \neq \varnothing$.

Nodal points 8.4. Assume Hypothesis 7.1. In the notation of Theorem 7.3,

$$\alpha = \alpha^\circ + (\theta_0, \pi_0) + (\theta_1, \pi_1) + (s\zeta_m^* \cdot (\pi_1), \pi_0).$$

If $L = K(f^{1/n})$ for $f = u\pi_0\pi_1^c$ and $u \in A^*$, with $c \in (\mathbb{Z}/n)^*$, then by Corollary 7.6(b),

$$\partial_w(\alpha) = w(\pi_1)(-c\theta_0 + \theta_1 + s\zeta_m^* \cdot ((u) + c(-1))_{\kappa(w)}.$$

If $x_w = z \in X^{(2)}$, then $k \subset \kappa(w)$, and the term of interest is

$$-c\,\theta_0(z) + \theta_1(z) + s\zeta_m^* \cdot ((\bar{u}) + c(-1))$$

where if $\theta_{v_i} = \partial_{v_i}(\alpha)$, we have $s\zeta_m^* = \partial_{v_0,\bar{z}}(\theta_{v_0}) = -\partial_{v_1,\bar{z}}(\theta_{v_1})$. If $s = 0$, then $\theta_{v_i}(\bar{z}) = \theta_i(z) \in \mathrm{H}^1(k)$. This guides the following classification scheme:

Definition 8.5. Suppose that z is a nodal point for α, and $\mathrm{div}_A(\alpha) = \{v_0, v_1\}$ has normal crossings. In the notation of (8.4), we say that, with respect to D_α, z is a

1. *Cold point* if $s \neq 0$.
2. *Cool point* if $s = 0$ and $\langle\theta_0(z)\rangle = \langle\theta_1(z)\rangle = 0$.
3. *Chilly point* if $s = 0$ and $\langle\theta_0(z)\rangle = \langle\theta_1(z)\rangle \neq 0$.
4. *Hot point* if $s = 0$ and $\langle\theta_0(z)\rangle \neq \langle\theta_1(z)\rangle$.

If z is a chilly point, the *coefficient of z with respect to v_0* is the number c such that $\theta_1(z) = c\,\theta_0(z)$.

The next lemma shows that when α is semiramified we can ignore hot points.

Lemma 8.6. *Assume Hypothesis 7.1 and the notation of (8.4), and suppose $s = 0$. Let $v_{\bar{z}}$ denote a discrete valuation extending $v_{\bar{z}}$ from $\kappa(v_0)$ to $\kappa(v_0)(\theta_{v_0})$. Then*

$$\partial_{v_{\bar{z}}}(\alpha(v_0)) = \theta_1(z)_{k(\theta_0(z))}.$$

In particular, if α is semiramified at v_0 and v_1, then $\langle\theta_0(z)\rangle = \langle\theta_1(z)\rangle$.

Proof. Note $\kappa(v_0)$ has a discrete valuation $v_{\bar{z}}$ induced by v_1 since $\{v_0, v_1\}$ has normal crossings. Since θ_{v_0} is $v_{\bar{z}}$-unramified, any extension $v_{\bar{z}}$ from $\kappa(v_0)$ to $\kappa(v_0)(\theta_{v_0})$ measures $v_{\bar{z}}(\pi_1) = 1$, and by definition, the residue field of $\kappa(v_0)(\theta_{v_0})$ with respect to $v_{\bar{z}}$ is $k(\theta_0(z))$. Since we assume (7.1), we can invoke Theorem 7.3, which implies $\alpha(v_0) = (\alpha^\circ + (\theta_1, \pi_1))_{\kappa(v_0)(\theta_{v_0})}$, where $\theta_1 = 0$ if z is a curve point for D_α. We then compute directly $\partial_{v_{\bar{z}}}(\alpha(v_0)) = \theta_1(z)_{k(\theta_0(z))}$, as desired. If α is semiramified at v_0 and v_1, then $\alpha(v_0) = \alpha(v_1) = 0$, hence $\theta_1(z) \in \langle\theta_0(z)\rangle$ and $\theta_0(z) \in \langle\theta_1(z)\rangle$, hence $\langle\theta_0(z)\rangle = \langle\theta_1(z)\rangle$. □

Definition 8.7. A *chilly loop* for α is a (reducible) component of D_α that forms a simple closed curve whose intersection points are chilly points for α.

Chilly loops present the following obstacle. Suppose $D = \sum_{i=1}^m D_i$ is a chilly loop, where each D_i is prime. Let c_{ij} be the coefficient of $z_{ij} = D_i \cap D_j$ with respect to v_i so that $\theta_i(z_{ij}) = c_{ij}\,\theta_j(z_{ij})$. If $L = K(f^{1/n})$ where $v_i(f) = c_i \in (\mathbb{Z}/n)^*$ and $c_j/c_i = c_{ij}$, then we compute $\partial_w(\alpha) = 0$ for all $w \in V_{z_{ij}}(L)$ by Corollary 7.6(b). But then proceeding around the loop we find $\prod_{i \pmod n} c_{ij} = 1$. There is no reason to expect such a relation from a general set of residues $\{\theta_i\}$, so such an f does not exist in general. We then resort to the strategy of zeroing out the values $\alpha(w_i)$, or at least showing they are unramified, cf. Proposition 8.11(C) below. However, we find this strategy is also blocked, by the same compatibility problem! The solution is to eliminate chilly loops, as follows.

Definition 8.8. Let $D_\alpha^+ = D_\alpha \cup (X_0)_{\mathrm{red}}$. We say D_α *is well-conditioned* if D_α has normal crossings, no cool points, no chilly loops, and no hot points; and D_α^+ *is well-conditioned* if D_α is well-conditioned and D_α^+ has normal crossings.

Lemma 8.9. *Assume $\alpha \in \mathrm{H}^2(K)$ has prime period, and is semiramified at every $v \in \mathrm{div}_K(\alpha)$. This holds, for example, if α has prime index. Then there exists an arithmetic surface X with function field K on which D_α^+ is well-conditioned.*

Proof. By (3.9), there exists an arithmetic surface X on which D_α^+ has normal crossings. Since α is semiramified at each $v \in \mathrm{div}_A(\alpha)$, D_α has no hot points by Lemma 8.6. Since D_α^+ has finitely many irreducible components, there can only be finitely many cool points or chilly loops.

Let $f : \tilde{X} \to X$ be the blow-up centered at z, and let $v \in V_z(K)$ be the valuation defined by the exceptional divisor. Then by Lemma 3.8, $\tilde{X}$ is an arithmetic surface, isomorphic to X away from z, and $\tilde{D}_\alpha^+ \subset \tilde{X}$ has normal crossings.

Suppose $z = D_0 \cap D_1$ is a cool point with respect to D_α. Since $\mathrm{per}(\alpha)$ is prime, Hypothesis 7.1 holds, by Proposition 7.2. Since v is centered on z, by Lemma 7.4, we compute $\partial_v(\alpha) = v(\pi_0)\theta_0(z) + v(\pi_1)\theta_1(z) = 0$, by the definition of cool point. Since D_0 and D_1 intersect transversally, they do not intersect on $\tilde{X}$, so the cool point z is transformed into two curve points on $\tilde{X}$. In this way, we eliminate all cool points with finitely many blow-ups.

Suppose $z = D_0 \cap D_1$ is a chilly point in a chilly loop, with coefficient c with respect to v_0. Again Hypothesis 7.1 holds. Since v is the valuation of the exceptional divisor, $v(\pi_0) = v(\pi_1) = 1$, and $\partial_v(\alpha) = \theta_0(z) + \theta_1(z) = (c+1)\theta_0(z)$ by Lemma 7.4. If $c+1$ is a multiple of n, then $\partial_v(\alpha) = 0$, and we have replaced z with two curve points on $\tilde{X}$. Otherwise we have replaced z with two chilly points, and one has coefficient $c+1$. Since n divides $c+r$ for some r, with enough iterations we break the chilly loop. In this way we will eliminate all chilly loops, and produce an arithmetic surface on which D_α^+ is well-conditioned. □

Local Parallel Transport 8.10. Assume Setup 6.1, and $n = q$ is prime. If $\partial_z(\theta_{v_0}) = s\zeta_q^* \neq 0$, and $\mu_q \notin A$, then Hypothesis 7.1 does not hold, and the local structure theorem (7.3) fails. However, we can still apply the results of Sect. 7 to this situation, using *local parallel transport* by the base extension defined by a primitive q-th root of unity ζ_q.

Let $K' = K(\zeta_q)$, and let B be the normalization of A in K'. Then $A \to B$ is a finite étale extension, and the localizations of B at its maximal ideals are (regular) two-dimensional local rings $A' = (A', \mathfrak{m}', k')$ dominating A. Fix one.

If $v \in V(A)$ extends to $v' \in V(A')$, and $w_1, \ldots, w_d$ are discrete valuations on $\kappa(v)$ corresponding to z as in (6.3), then $\kappa(w_i) \otimes_A A' = \kappa(w_i) \otimes_k k'$ is the product of the residue fields of w_i's extensions to $\kappa(v')$. Since $A \to A'$ is unramified, we construct from this data, (2.4), and (6.4), a diagram (for $n = q$)

$$\begin{array}{ccccccccc}
0 \to \mathrm{H}^2(A') \to \mathrm{H}^2(K') & \xrightarrow{\oplus\partial_{v'}} & \bigoplus\limits_{v' \in V(A')} \mathrm{H}^1\left(\kappa(v')\right) & \xrightarrow{\partial_{z'}} & \mathrm{H}^0(k') \to 0 \\
\uparrow \qquad\quad \uparrow & & \uparrow \oplus\mathrm{res}_{\kappa(v)|\kappa(v')} & & \uparrow \mathrm{res}_{k|k'} \\
0 \to \mathrm{H}^2(A) \to \mathrm{H}^2(K) & \xrightarrow{\oplus\partial_v} & \bigoplus\limits_{v \in V(A)} \mathrm{H}^1\left(\kappa(v)\right) & \xrightarrow{\partial_z} & \mathrm{H}^0(k) \to 0
\end{array}$$

Since q is prime, the field extensions have prime-to-q degree, hence the vertical restriction arrows are injective by the standard restriction-corestriction argument. Moreover, since $A \to A'$ is flat, each $v' \in V(A')$ lies over some $v \in V(A)$, so that the residues of $\alpha' = \mathrm{res}_{K|K'}(\alpha)$ at the $v' \in V(A')$ are exactly those restricted from residues of α at $v \in V(A)$. Since $\mathfrak{m}' = \mathfrak{m}A' = (\pi_0, \pi_1)$, $D_{\alpha'}$ has normal crossings at $z' = \mathrm{Spec}(k')$ on Spec A', and Hypothesis 7.1 holds for α' on A' by Proposition 7.2. Thus the classification of z' in Definition 8.5 is identical to that of z, should z be a nodal point of D_α.

Note the splitting of residues at z can now be computed at z'. For if L/K is a finite separable field extension of degree q, $L' = L \otimes_K K'$, and $\partial_{w'}\left(\alpha'_{L'}\right) = 0$ for $w' \in V(L')$ extending $w \in V(L)$, then $\partial_w(\alpha) = 0$ by (2.4), the injectivity of the restriction, and the fact that L'/L is unramified. If L/K is v_0-totally ramified, $w_0' \in V(L')$ extends v_0 to L' and restricts to w_0 and v_0' on L and K', then L'/K' is v_0'-totally ramified, $\alpha(w_0)$ and $\alpha'(w_0')$ are defined over $\kappa(v_0)$ and $\kappa(v_0')$, respectively, and $\alpha'(w_0') = \mathrm{res}_{\kappa(v_0)|\kappa(v_0')}(\alpha(w_0))$ by the compatibility of restriction maps. Then, since restriction commutes with the residue map (2.4), $\partial_{v_0', \bar{z}'}(\alpha'(w_0')) = \mathrm{res}_{k|k'}(\partial_{v_0, \bar{z}}(\alpha(w_0)))$.

Proposition 8.11. *In Setup 6.1, assume $\alpha \in H^2(K)$ has prime period n, D_α^+ is well-conditioned, and $D_\alpha = \sum_I D_i$, where I indexes the prime divisors D_i. Suppose $L = K(f^{1/n})$, where $f \in K$ satisfies*

A. div $f = c_I D_\alpha + D_\varepsilon$, *where $c_I = (c_i)_I$, for $c_i \in (\mathbb{Z}/n)^*$, and D_ε contains no components or nodal points of D_α.*

B. If $(D_i \cdot D_\varepsilon)_z \neq 0 \pmod{n}$ *for some* $i \in I$, *then* $\theta_{v_i}(\bar{z}) = 0$.
C. $\partial_{v_i,\bar{z}}(\alpha(w_i)) = 0$ *whenever* z *is a nodal point of* D_α *on* D_i, *and* $w_i \in V(L)$ *extends* v_i.

Then $\alpha_L \in \mathrm{H}^2_{\mathrm{nr}}(L/R)$.

Proof. Assume f satisfies (A), (B), and (C), and set $A = \mathrm{O}_{X,z}$. If z is a cold point and $A \to A'$ is as in (8.10), then the hypotheses transfer to A' by local parallel transport, and the conclusion, which is verified locally, descends back to K. Therefore we may assume $\mu_n \subset K$, so that Hypothesis 7.1 holds, by Proposition 7.2. Let $w \in V_A(L)$, and let v be the normalized valuation corresponding to $w|_K$. By Purity for Surfaces (4.2), it is enough to show $\partial_w(\alpha) = 0$, and invoking (A), we may assume by Corollary 7.6(a), (c), and (d) that $z \in D_\alpha$, $w \in V_z(L)$, and z lies on more than one component of div f.

Suppose z is a curve point of D_α, so $\mathrm{div}_A(\alpha) = \{v_0\}$. By (A) we have $f = u_0\pi_0^{c_0}$, where $c_0 \in (\mathbb{Z}/n)^*$, and $u_0 \in A$ is not divisible by π_0. Since $k \subset \kappa(w)$, $c_0\partial_w(\alpha) = -w(u_0)\theta_0(z)$ by Corollary 7.6(b). If $w(u_0) \neq 0 \in \mathbb{Z}/n$, then $\theta_0(z) = 0$ by (B), so, since $c_0 \in (\mathbb{Z}/n)^*$, $\partial_w(\alpha) = 0$.

Suppose z is a nodal point of D_α, so $\mathrm{div}_A(\alpha) = \{v_0, v_1\}$. By (A), $f = u\pi_0^{c_0}\pi_1^{c_1}$, where $u \in A^*$ and $c_0, c_1 \in (\mathbb{Z}/n)^*$. Since $v \in V_z(K)$, $\alpha(w_0) = \alpha_{L_{w_0}}$ by Corollary 7.6(f), hence $\partial_w(\alpha) = c_0^{-1}w(\pi_1)\partial_{v_0,\bar{z}}(\alpha(w_0))$ by Corollary 7.6(b). Therefore, $\partial_w(\alpha) = 0$ by (C). $\square$

9 Splitting in Prime Degree

For any $\alpha \in \mathrm{H}^2(K)$ of prime index relatively prime to all char k, there exists an arithmetic surface $X \to S$ on which α's ramification locus is well-conditioned, by Lemma 8.9. Proposition 8.11 provides us with a blueprint for splitting the residues of such a class, under Hypothesis 7.1. We want to produce an element $f \in K^*$ satisfying

A. div $f = c_ID_\alpha + D_\varepsilon$, where $c_I = (c_i)_I$, for $c_i \in (\mathbb{Z}/n)^*$, and D_ε contains no components or nodal points of D_α.
B. If $(D_i \cdot D_\varepsilon)_z \neq 0 \pmod{n}$ for some $i \in I$, then $\theta_{v_i}(\bar{z}) = 0$.
C. $\partial_{v_i,\bar{z}}(\alpha(w_i)) = 0$ whenever z is a nodal point of D_α on D_i, and $w_i \in V(L)$ extends v_i.

We now carry out the program when K is the function field of a p-adic curve. The following lemma is the technical heart of the computation (see [S2, Th. 4.6]).

Lemma 9.1. *Suppose* $n = q$ *is prime,* $\mathrm{per}(\alpha) = q$, X *is an arithmetic surface on which* D_α^+ *is well conditioned, and* α *is semiramified at all* $v_i \in \mathrm{div}_X(\alpha)$. *Then there exists an* $f \in K$ *satisfying* (A) *and* (C), *such that* $\alpha(w_i) = 0$ *whenever* z *is a nodal point on* $D_i \subset D_\alpha \subset X$. *Furthermore,* D_ε *(as in* (A)*) contains no components or nodal points of* D_α^+ *(not just of* D_α*).*

Proof. Note the arithmetic surface $X \to S$ on which D_α^+ is well-conditioned exists by Lemma 8.9. By Lemma 7.7, we may choose f so that $\operatorname{div} f = c_I D_\alpha + D_\varepsilon$, where D_ε contains no component points or nodal points of D_α^+, and $c_I = (c_i)_I$ is any set of coefficients, which we take to be in $(\mathbb{Z}/q)^*$. Thus f satisfies (A).

It is more difficult to satisfy (C). We will zero out the values $\alpha(w_i)$, though later, in satisfying (B), we will be content to leave them unramified. Since D_α^+ is well-conditioned, it has no chilly loops, so we may assign $c_i \in (\mathbb{Z}/q)^*$ to each component D_i of D_α, such that if $z = D_i \cap D_j$ is a chilly point, then c_j/c_i is the chilly point coefficient with respect to v_i.

Define D^+ to be the union of irreducible components of X_0 that are not part of D_α, so $D_\alpha^+ = D_\alpha + D^+$. We call irreducible components of D_α^+ *isolated* if they contain no nodal points of D_α^+. To each isolated component of D_α^+ we assign a (curve) point, and call this an *isolated-component point*. Define the following sets of closed points, abusing notation in the obvious way.

- $\mathscr{N} = D_\alpha \cap D_\alpha$.
- $\mathscr{P} = (D^+ \cap D^+) \cup \{\text{isolated-component points of } D^+\}$.
- $\mathscr{Q} = (D_\alpha \cap D^+) \cup \{\text{isolated-component points of } D_\alpha\}$.

We use v_0 and v_1 as general elements of $\operatorname{div}_X(\alpha)$. Since $\operatorname{per}(\alpha)$ is prime and α is semiramified at v_0, the residue θ_{v_0} has order q. By Lemma 8.2, the value of α at an extension w_0 of v_0 to $L = K(f^{1/q})$ is

$$\alpha(w_0) = (-c_0^{-1}\theta_{v_0}, t_0) \in \mathrm{H}^2(\kappa(v_0))$$

for $t_0 \in \mathrm{O}_{v_0}^*$ defined by $f = t_0 \pi_{v_0}^{c_0}$, for some uniformizer $\pi_{v_0} \in \mathrm{O}_{v_0}$. If $t \in K$ is in $\mathrm{O}_{v_0}^*$, the value over $L' = K((f/t)^{1/q})$ is $\alpha(w_0') = (-c_0^{-1}\theta_{v_0}, t_0/t)$, where w_0' is an extension of v_0 to L'. To prove the lemma we will find a $t \in K$ with $(t_i/t) = 0$ for each $i \in I$, zeroing out each $\alpha(w_i)$, while maintaining (A). There are two steps.

Step 1. If $z \in D_i$, we say $t_i \in \kappa(v_i)$ or $t_i \in \mathrm{O}_{v_i}^*$ is a *unit at* z when $t_i \in \mathrm{O}_{D_i,\bar{z}}^*$. We claim that in the expression for $\alpha(w_i)$, we may assume

a. the t_i are units at all $z \in \mathscr{N} \cup \mathscr{Q}$ and
b. $\bar{t}_i = \bar{t}_j$ in $k = \kappa(z)$, for $z \in \mathscr{N}$ on $D_i \cap D_j$.

We show that (without modifying f) we may assume $t_0 \in \kappa(v_0)$ in each $\alpha(w_0)$ is a unit at $z \in D_0$ whenever $z \in \mathscr{N} \cup \mathscr{Q}$. For such z, let $l = \kappa(v_0)(\theta_{v_0})$, $l_z = l \otimes_{\kappa(v_0)} \kappa(v_0)_{\bar{z}}$, and let $N = N_{l/\kappa(v_0)}$, and $N_z = N_{l_z/\kappa(v_0)_{\bar{z}}}$ denote the norms. Note $l/\kappa(v_0)$ and $l_z/\kappa(v_0)_{\bar{z}}$ have degree q, and l_z may not be a field. If we can find $u_z \in l_z$ such that $v_{\bar{z}}(N_z(u_z)) = -v_{\bar{z}}(t_0)$, for each z, then by weak approximation there exists a $u \in l$ such that $v_{\bar{z}}(N(u)) = v_{\bar{z}}(N_z(u_z))$. Replacing t_0 by $t_0' = N(u)t_0$, we obtain $v_{\bar{z}}(t_0') = 0$, and since t_0'/t_0 is a norm from $\kappa(v_0)(\theta_{v_0})$, $(-c_0^{-1}\theta_{v_0}, t_0) = (-c_0^{-1}\theta_{v_0}, t_0')$, as desired. Therefore, it is enough to find the u_z.

Suppose $z \in D_0$ is in $\mathscr{N}$. By considering the $v_{\bar{z}}$-values of the group of norms from the prime-degree extension $l/\kappa(v_0)$, we see that finding u_z is trivial unless

θ_{v_0} is $\bar{z}$-unramified and $v_{\bar{z}}(t_0) \in (\mathbb{Z}/q)^*$. Therefore we are finished at cold points, since for them θ_{v_0} is $\bar{z}$-totally ramified. At chilly points, we compute directly $\partial_{v_0,\bar{z}}(\alpha(w_0)) = -c_0^{-1} v_{\bar{z}}(t_0)\theta_{v_0}(\bar{z})$. But $\alpha(w_0) = \alpha_{L_{w_0}}$ by Corollary 7.6(f), and since $s = 0$ and $-c_1\theta_0(z) + c_0\theta_1(z) = 0$ by the choice of the c_i, by Corollary 7.6(b) we have $\partial_{v_0,\bar{z}}(\alpha(w_0)) = 0$. Since $\theta_{v_0}(\bar{z})$ is nontrivial (definition of chilly point), we conclude $v_{\bar{z}}(t_0) = 0 \pmod q$. Therefore there is no problem at chilly points, and we have u_z for all $z \in \mathscr{N}$.

Suppose $z \in D_0$ is in $\mathscr{Q}$. By the choice of f, D_ε avoids z, so f has only one irreducible component going through z, and since by definition $f = t_0\pi_{v_0}^{c_0}$, again $v_{\bar{z}}(t_0) = 0 \pmod q$, and there is no problem. Thus each t_i is a unit at all $z \in \mathscr{N} \cup \mathscr{Q}$, and we have (a).

Suppose $z \in \mathscr{N}$ is on $D_0 \cap D_1$. Since t_0 and t_1 are units at z, each has an image $\bar{t}_i$ in $\kappa(z)$. We show that we may assume $\bar{t}_0 = \bar{t}_1$. If z is a chilly point, then $c_1\theta_0(z) = c_0\theta_1(z)$, so $\alpha(w_0)(\bar{z}) = \alpha(w_1)(\bar{z})$ by Corollary 7.6(e). That is, $(-c_0^{-1}\theta_0(z), \bar{t}_0) = (-c_1^{-1}\theta_1(z), \bar{t}_1)$. Since $c_1^{-1}\theta_1(z) = c_0^{-1}\theta_0(z)$, $\bar{t}_0$ and $\bar{t}_1$ differ by a norm from $\kappa(z)(\theta_0(z))$ to $\kappa(z)$. If z is a cold point, then by Corollary 7.6(f) (applying (8.10) if necessary),

$$c_0 \cdot \partial_{v_0,\bar{z}}(\alpha(w_0)) = -c_1 \cdot \partial_{v_1,\bar{z}}(\alpha(w_1)).$$

We have $c_0\alpha(w_0) = (-\theta_{v_0}, t_0)$. Writing $\theta_{v_0} = \theta_{v_0}^\circ + s\zeta_m^* \cdot (\pi_1)$ over $\kappa(z)(v_0)_{\bar{z}}$, and noting that $v_{\bar{z}}(t_0) = 0$ by (a), we compute

$$c_0 \cdot \partial_{v_0,\bar{z}}(\alpha(w_0)) = s\zeta_m^* \cdot (t_0)_{\kappa(z)}$$

and similarly $-c_1 \cdot \partial_{v_1,\bar{z}}(\alpha(w_1)) = s\zeta_m^* \cdot (t_1)_{\kappa(z)}$. Since $s\zeta_m^*$ has order q, we conclude $\bar{t}_0 = \bar{t}_1 \pmod{\kappa(z)^q}$. In any case, whether z is a chilly or cold point, using (standard) weak approximation we may adjust t_0 by a norm from $\kappa(v_0)(\theta_{v_0})$ to $\kappa(v_0)$ so that $\bar{t}_0 = \bar{t}_1$ simultaneously at each $z \in \mathscr{N}$ on D_0. We may apply the same procedure on D_1 without affecting the result on D_0, and by induction we may arrange so that the $\bar{t}_i$ are all equal, at all $z \in \mathscr{N}$. This proves (b), and completes Step 1.

Step 2. Next we produce a $t \in K^*$ whose image in $\kappa(v_i)$ is defined and equals t_i, and such that $\operatorname{div}(f/t)$ satisfies (A), for D_α^+. First we reduce to ring theory. By [Liu, 3.3.36], if X is a quasi-projective scheme over an affine scheme S, then any given finite set of points of X is contained in an affine open subset of X. Thus we have an affine open subset $U \subset X$ with affine ring T that includes all points of $\mathscr{N} \cup \mathscr{P} \cup \mathscr{Q}$. The poles and zeros of the t_i on D_i are not in $\mathscr{N} \cup \mathscr{P} \cup \mathscr{Q}$: by Step 1, $t_i \in \mathrm{O}_{D_i,\bar{z}}^*$ for all $z \in D_i \cap (\mathscr{N} \cup \mathscr{Q})$, and $D_i \cap \mathscr{P} = \varnothing$. Therefore, taking a distinguished open set if necessary, we may assume U excludes these poles and zeros, hence that $t_i \in \mathrm{O}_{D_i \cap U}^*$ for each $i \in I$. Note $\mathscr{N} \cup \mathscr{P} \cup \mathscr{Q}$ contains a closed point from each component of D_α^+, so U contains the generic point of each component of D_α^+.

Let $\{\mathfrak{p}_i\}_I$ denote the set of prime ideals of T corresponding to the irreducible components of D_α, and let $\{\mathfrak{m}_j\}_J$ denote the set of maximal ideals corresponding to the closed points $z_j \in \mathscr{P}$. These are either nodal points of D^+, or isolated-component points on D^+. Then, for notational convenience, set

$$\mathfrak{q}_i = \begin{cases} \mathfrak{p}_i & \text{if } i \in I \\ \mathfrak{m}_i & \text{if } i \in J. \end{cases}$$

To go along with the $t_i \in (T/\mathfrak{q}_i)^*$ $(i \in I)$, for each $j \in J$ let $t_j \in (T/\mathfrak{q}_j)^*$ be any (nonzero) element. We *claim* there exists a $t \in T$ such that $t = t_i \pmod{\mathfrak{q}_i}$ for each $i \in I \cup J$. Since then $\bar{t}$ is nonzero in $\kappa(z)$ for each $z \in \mathscr{N} \cup \mathscr{P} \cup \mathscr{Q}$, div t contains none of these points, and none of D_α^+'s irreducible components. Then $\mathrm{div}(f/t)$ satisfies (A) with respect to D_α^+, and if $L' = K((f/t)^{1/q})$,

$$\alpha(w_i') = (-c_i^{-1}\theta_{v_i}, t_i/t) = (-c_i^{-1}\theta_{v_i}, 1) = 0$$

where w_i' is an extension of v_i to $L = K((f/t)^{1/q})$. Thus the claim will give us (C).

We prove the claim, as in [S2, Prop. 4.5]. Order $I \cup J$, and set $\mathfrak{a} = \bigcap_{i=1}^{n-1} \mathfrak{q}_i$, the ideal of the scheme $\bigcup_{i=1}^{n-1} V(\mathfrak{q}_i)$. The map $(a,b) \mapsto a - b$ defines an exact sequence

$$0 \longrightarrow T/(\mathfrak{a} \cap \mathfrak{q}_n) \longrightarrow T/\mathfrak{a} \oplus T/\mathfrak{q}_n \longrightarrow T/(\mathfrak{a} + \mathfrak{q}_n) \longrightarrow 0.$$

We sketch this argument. The sequence is easily seen to be a complex, and the injectivity and surjectivity are immediate. To prove exactness in the middle, we may assume $T = T_\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and then T is factorial, since X is regular. If $\mathfrak{a} + \mathfrak{q}_n = T$, the result follows by the Chinese Remainder Theorem. If $\mathfrak{a} + \mathfrak{q}_n \neq T$ then all of the $\mathfrak{q}_i$ for $i \leq n$ are (regular) principal primes, so $\mathfrak{a} = (x^c)$ and $\mathfrak{q}_n = (y)$ for some $c > 0$ and primes x and y, and since D_α has normal crossings, $\mathfrak{m} = (x,y)$. If the pair $(a + \mathfrak{a}, b + \mathfrak{q}_n)$ maps into the ideal (x^c, y) then we may assume $b = ux^d$ for some $d \geq 0$ and $u \in T^*$, and $a = ux^d + sy^e$, for $e > 0$ and $s \in T$, and then $(a + \mathfrak{a}, b + \mathfrak{q}_n)$ is in the image of $t = ux^d + sy^e$, proving exactness in the middle.

Now induct on the cardinality of $I \cup J$, the base case $n = 1$ being trivial. Assume there exists a $t' \in T$ such that $t' = t_i \pmod{\mathfrak{q}_i}$ for $i \leq n-1$ in $I \cup J$. If $\mathfrak{q}_n = \mathfrak{m}_n$, i.e., $V(\mathfrak{q}_n) = z_n \in \mathscr{P}$, or if $\mathfrak{q}_n = \mathfrak{p}_n$ for an isolated component D_n (of D_α), or if $V(\mathfrak{a}) = \varnothing$, then $V(\mathfrak{a} + \mathfrak{q}_n) = \varnothing$, and since $T/(\mathfrak{a} + \mathfrak{q}_n) = 0$, by exactness of the above sequence there exists a $t \in T$ mapping to $(t', t_n) \in T/\mathfrak{a} \oplus T/\mathfrak{q}_n$, and then $t = t_i \pmod{\mathfrak{q}_i}$ for each $i \leq n$. If $\mathfrak{q}_n = \mathfrak{p}_n$ and $V(\mathfrak{a} + \mathfrak{q}_n) \neq \varnothing$, then since D_α has normal crossings, $V(\mathfrak{a} + \mathfrak{q}_n)$ is a finite subset of $\mathscr{N}$. If $z \in D_i \cap D_n$ is one of these points, then $t_i = t_n \pmod{\mathfrak{m}_z}$ by Step 1. Therefore (t', t_n) maps into each $\mathfrak{m}_z$ containing $\mathfrak{a} + \mathfrak{q}_n$. Again by the normal crossings hypothesis it follows that (t', t_n) maps to zero in $T/(\mathfrak{a} + \mathfrak{q}_n)$, and by exactness again we find $t \in T$ mapping to (t', t_n) so that $t = t_i \pmod{\mathfrak{q}_i}$ for each $i \leq n$. By induction, there exists $t \in T$ such that $t = t_i \pmod{\mathfrak{q}_i}$, for each $i \in I \cup J$, as claimed. This completes the proof of Lemma 9.1. □

Problematic curve points 9.2. We call the $z \in D_\varepsilon \cap D_\alpha$, which appear in (B), *problematic curve points*. If we choose $f \in K$ as in Lemma 9.1, then we have (A) and (C). There is no reason why (B) should follow, though we have the following.

Proposition 9.3. *Assume the hypotheses of Lemma 9.1, $f \in K$ satisfies* (A) *and* (C)*, X is as in Lemma 9.1, and $D_0 \subset D_\alpha$ is an irreducible component. If $z \in D_0 \cap D_\varepsilon$ is a problematic curve point, then either $\theta_{v_0}(\bar{z}) = 0$ or $(D_0 \cdot D_\varepsilon)_z$ is a multiple of q.*

Proof. Write $f = u_0 \pi_0^{c_0}$, where $u_0 \in \mathrm{O}_{v_0}^*$, and set $L = K(f^{1/q})$. Since $c_0 \in (\mathbb{Z}/q)^*$ by (A), and θ_{v_0} has order q, $\alpha_{L_{w_0}} = \alpha(w_0)$ and $\kappa(w_0) = \kappa(v_0)$ by Corollary 7.6(f). By Lemma 7.5, $c_0\,\alpha(w_0) = c_0\,\alpha^\circ - (\theta_0, u_0)$, hence

$$c_0\,\partial_{v_0,\bar{z}}(\alpha(w_0)) = -v_{\bar{z}}(u_0)\theta_0(z) = -(D_0 \cdot D_\varepsilon)_z\,\theta_0(z).$$

Since $\partial_{v_0,\bar{z}}(\alpha(w_0)) = 0$ by (C), either $\theta_0(z) = 0$ or $(D_0 \cdot D_\varepsilon)_z$ is a multiple of q. $\square$

We still do not have (B): $(D_0 \cdot D_\varepsilon)_z$ being a multiple of q only helps if D_ε has only one irreducible component passing through z; as it stands, D_ε could have up to q distinct components all intersecting at z. To resolve this problem we will invoke Proposition 5.5, and for this we now take $S = \operatorname{Spec} R$, where $R = \mathbb{Z}_p$.

Proposition 9.4. *Assume the hypotheses of Lemma 9.1 with $X \to S = \operatorname{Spec}\mathbb{Z}_p$, as in Lemma 9.1. Then there exists an $f \in K$ satisfying* (A), (B)*, and* (C).

Proof. Let $\underline{z}$ denote the set of all nodal points of D_α^+, and write $\underline{\bar{z}}$ for the image of $\underline{z}$ on X_0. Choose f as in Lemma 9.1, and write $\operatorname{div} f = c_I D_\alpha + D_\varepsilon$. We will show that if $z \in D_\alpha \cap D_\varepsilon$ and $(D_0 \cdot D_\varepsilon)_z$ is a multiple of q, then we may assume D_ε is a q-multiple at z. Then f satisfies (B) by Proposition 9.3.

By Lemma 9.1, D_ε contains no irreducible component of X_0, so all of its components are horizontal. Since S is henselian, by [Liu, 8.3.35] there exists a divisor D_{good} that is the sum of horizontal divisors, with correct multiplicities, cutting out exactly those points of $D_\varepsilon \cap (X_0)_{\text{red}}$ of multiplicity not divisible by q. Let $D_{\text{bad}} = D_\varepsilon - D_{\text{good}}$. The restriction $(D_{\text{bad}})_0$ to the closed fiber is an effective divisor that has multiplicity q; we want to replace D_{bad} with an effective divisor that has multiplicity q.

Since D_{bad} avoids $\underline{z}$, by (5.3), it has a preimage ${}_{\underline{z}}D_{\text{bad}}$ in ${}_{\underline{z}}\operatorname{Div}' X$. Let ${}_{\underline{z}}\delta_{\text{bad}}$ denote the image in ${}_{\underline{z}}\operatorname{Pic} X$, again using (5.3). Since the image of ${}_{\underline{z}}\delta_{\text{bad}}$ in ${}_{\underline{\bar{z}}}\operatorname{Pic}(X_0)_{\text{red}}$ is a q-th power, so is ${}_{\underline{z}}\delta_{\text{bad}}$ by Proposition 5.5. Thus by (5.4), there is an element $g \in {}_{\underline{z}}K^*$ such that $\operatorname{div} g = q \cdot {}_{\underline{z}}E - {}_{\underline{z}}D_{\text{bad}}$, for some ${}_{\underline{z}}E \in {}_{\underline{z}}\operatorname{Div}' X$. By (5.3), we then have

$$\operatorname{div} g \;=\; qE - D_{\text{bad}}$$

in $\operatorname{Div}' X \leq \operatorname{Div} X$. By (5.4) and the definition of ${}_{\underline{z}}K^* \leq K^*$, E avoids $\underline{z}$, and $g(z) \in \kappa(z)^{*q}$ for each $z \in \underline{z}$. Now

$$\operatorname{div} fg = c_I D_\alpha + D_{\text{good}} + qE$$

where D_{good} intersects D_α only at curve points of multiplicity not divisible by q. We show that fg satisfies (A) and (C). The values of the c_i modulo q are unchanged by qE, even if E contains (isolated) components of D_α. Since D_{good} contains no components of D_α by construction, we have (A). Let $L' = K((fg)^{1/q})$, and suppose z is a nodal point of D_α on D_0. Let w_0' be an extension of v_0 to L'. There is no reason why $\alpha(w_0')$ should be zero, but computing as in the proof of Proposition 9.3, we set $u_0' = gu_0 \in \mathrm{O}_{v_0}^*$, $c_0\alpha(w_0') = c_0\alpha^\circ - (\theta_0, u_0')$, and $c_0\partial_{v_0,\bar{z}}(\alpha(w_0')) = -v_{\bar{z}}(u_0')\theta_0(z)$. Therefore since $g(z)$ is in $\kappa(z)^{*q}$, $v_{\bar{z}}(u_0') = v_{\bar{z}}(u_0) \pmod q$, hence $\partial_{v_0,\bar{z}}(\alpha(w_0')) = 0$, and we have (C). In light of Proposition 9.3, we now have (B). □

Theorem 9.5. *Let K be the function field of a p-adic curve, and let Δ be a K-division algebra of prime index $q \neq p$. Then Δ is cyclic.*

Proof. This is [S2, Th. 5.1]. Let $\alpha \in \mathrm{H}^2(K)$ be the class of Δ in $\mathrm{Br}(K)$. Since $\mathrm{ind}(\alpha) = q$ is prime, α is semiramified at all $v \in \mathrm{div}_K(\alpha)$ by (8.1). Let $X \to S = \mathrm{Spec}\,\mathbb{Z}_p$ be any arithmetic surface on which D_α^+ is well-conditioned, as in Lemma 8.9. By Proposition 9.4, there is an element $f \in K$ satisfying (A), (B), and (C). Let $L = K(f^{1/q})$. Since f satisfies (A), (B), and (C), $\alpha_L \in \mathrm{H}^2_{\mathrm{nr}}(L) = \bigcap_{V(L)} \mathrm{H}^2(\mathrm{O}_v)$ by Proposition 8.11. Since L is the function field of a p-adic curve, $\alpha_L = 0$ by Theorem 4.5. Finally, since Δ is split by a radical extension of degree q, Δ is cyclic by a theorem of Albert [S2, Prop. 0.1]. □

Finally, we have the following geometric criterion for a Brauer class to have prime index.

Corollary 9.6. *Let K be the function field of a p-adic curve, and let $\alpha \in \mathrm{Br}(K)$ be an element of prime period $q \neq p$. Let $X \to \mathrm{Spec}\,\mathbb{Z}_p$ be an arithmetic surface on which D_α has normal crossings. Then $\mathrm{ind}(\alpha) = q$ if and only if D_α has no hot points.*

Proof. This is [S2, Cor. 5.2]. If $\mathrm{ind}(\alpha) = q$, then α is semiramified at all $v_i \in \mathrm{div}_X(\alpha)$ by (8.1), and D_α has no hot points on X by Lemma 8.6.

Suppose $\mathrm{per}(\alpha) = q$ and D_α has no hot points on X. We do not introduce hot points if we blow up X to remove cool points and chilly loops, by the proof of Lemma 8.9, or to establish normal crossings on the closed fiber. Thus we may assume D_α^+ is well-conditioned. We claim that α is semiramified at each $v_i \in \mathrm{div}_X(\alpha)$. Then the proof of Theorem 9.5 applies directly, and we are done. If $v_0 \in \mathrm{div}_X(\alpha)$, then, writing $\alpha_{K_{v_0}} = \alpha_0 + (\theta_{v_0}, \pi_{v_0})$ with $\alpha_0 \in \mathrm{H}^2(\kappa(v_0))$ as in (2.4), we compute

$$\mathrm{ind}(\alpha_{K_{v_0}}) = |\theta_{v_0}|\,\mathrm{ind}((\alpha_0)_{\kappa(v_0)(\theta_{v_0})}).$$

We must show $\kappa(v_0)(\theta_{v_0})$ splits α_0.

If D_0 is horizontal, then $\kappa(v_0)$ is a p-adic field, and since θ_{v_0} has order q, it splits α_0 by (Hasse's) local field theory, and we are done. If D_0 is vertical, then it is a smooth projective curve over a finite field k, and it suffices to show $\kappa(v_0)(\theta_{v_0})$ splits α_0 at all $z \in D_0$, by the local global splitting principle, as in the proof of Theorem 4.5. Again by local field theory, this is only an issue if θ_{v_0} is split at the completion $\kappa(v_0)_{\bar{z}}$. However, in that case we have $s = 0$, and since there are no hot points, we find $\partial_{v_0,\bar{z}}(\alpha(v_0)) = 0$ by Lemma 8.6. Since the residue field of $\kappa(v_0)_{\bar{z}}$ is finite, we conclude $(\alpha_0)_{\kappa(v_0)_{\bar{z}}} = 0$ by the split exact sequence for a completion in (2.4). Therefore α_0 is split by θ_{v_0} at each z, hence $\kappa(v_0)(\theta_{v_0})$ splits α_0, and α is semiramified at v_0. □

Acknowledgements The author thanks Skip Garibaldi for encouraging him to take on this project, and Colliot-Thélène, and especially Suresh and his staff for organizing a wonderful conference in Hyderabad, in honor of Professor Parimala.

References

[AT] Artin, E., Tate, J.: *Class Field Theory*, AMS Chelsea Publishing, Am. Math. Soc., Rhode Island, 2009.

[AG] Auslander, M., Goldman, O.: The Brauer group of a commutative ring, *Trans. Am. Math. Soc.*, **97** (1960) 367–409.

[C-T] Colliot-Thélène, J.-L.: Birational invariants, purity and the Gersten conjecture, in *K-Theory and Algebraic Geometry: Connections with Quadratic Forms and Division Algebras* (B. Jacob and A. Rosenberg, eds.), Proceedings of Symposia in Pure Mathematics, vol. 58.1, Am. Math. Soc., Providence, RI, 1995.

[C-T2] ———: Review of [S1], Zentralblatt MATH database 1931–2009, Zbl 0902.16021.

[GMS] Garibaldi, S., Serre, J.-P., Merkurjev, A.: *Cohomological Invariants in Galois Cohomology, (University Lecture Series Volume 28)*, American Mathematical Society, 2003.

[GS] Gille, P., Szamuely, T.: *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, Cambridge, 2006.

[GB] Grothendieck, A.: Le groupe de Brauer I, II, III, in *Dix Exposés sur la Cohomologie des Schémas*, North-Holland, Amsterdam/Masson, Paris, 1968, 46–188.

[Ho] Hoobler, R.T.: A cohomological interpretation of Brauer groups of rings, *Pact. J. Math.* **86** no. 1, (1980) 89–92.

[Lbm] Lichtenbaum, S.: Curves over discrete valuation rings, *Am. J. Math.*, **90** no. 2, (1968) 380–405.

[Liu] Liu, Q.: *Algebraic Geometry and Arithmetic Curves,* Oxford University Press, New York, 2002.

[Mat] Matsumura, H.: *Commutative Ring Theory, (Cambridge Studies in Advanced Mathematics 8)*, Cambridge University Press, Cambridge, 1989.

[M] Milne, J. S.: *Etale Cohomology.* Princeton University Press, New Jersey, 1980.

[S1] ———: Division algebras over p-adic curves, *J. Raman. Math. Soc.*, **12** (1997) 25–47.

[S1′] ———: Correction to division algebras over p-adic curves, *J. Raman. Math. Soc.*, **13** (1998) 125–129.

[S2] ———: Cyclic algebras over p-adic curves, *J. Alg.*, **314** no. 2 (2007), 817–843.

[S3] ———: Division algebras over surfaces, *J. Alg.*, **315**, no. 4 (2008), 1543–1585.

[SGA1] Grothendieck, A., Raynaud, M.: *Séminaire de géométrie algébrique du Bois Marie 1960–1961: Revêtements étales et groupe fondamental*, Documents mathématiques, vol. 3, Société Mathématique de France, 2003.

[Si] Silverman, J. H.: *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

Serre's Conjecture II: A Survey

Philippe Gille

Dedicated to Parimala

Summary We provide a survey of Serre's conjecture II (1962) on the vanishing of Galois cohomology for simply connected semisimple groups defined over a field of cohomological dimension at most 2.

1 Introduction

Serre's original conjecture II (1962) states that the Galois cohomology set $H^1(k,G)$ vanishes for a semisimple simply connected algebraic group G defined over a perfect field of cohomological dimension ≤ 2 [52, Sect. 4.1] [53, II.3.1]. This means that G-torsors (or principal homogeneous spaces) over $\mathrm{Spec}(k)$ are trivial.

For example, if A is a central simple algebra defined over a field k and $c \in k^\times$, the subvariety

$$X_c := \{\mathrm{nrd}(y) = c\} \subset \mathbf{GL}_1(A)$$

of elements of reduced norm c is a torsor under the special linear group $G = \mathbf{SL}_1(A)$ which is semisimple and simply connected. If $\mathrm{cd}(k) \leq 2$, we thus expect that this G-torsor is trivial, i.e., $X_c(k) \neq \emptyset$. Applying this to all $c \in k^\times$, we thus expect that the reduced norm map $A^\times \to k^\times$ is surjective.

For imaginary number fields, the surjectivity of reduced norms goes back to Eichler in 1938 (see [39, Sect. 5.4]). For function fields of complex surfaces, this follows from the Tsen-Lang theorem because the reduced norm is a homogeneous form of degree $\deg(A)$ in $\deg(A)^2$-indeterminates [53, II.4.5]. In the general case, the surjectivity of reduced norms is due to Merkurjev–Suslin in 1981 [59, Th. 24.8],

Philippe Gille
DMA, UMR 8553 du CNRS, Ecole normale supérieure, 45 rue d'Ulm, F-75005 Paris, France,
e-mail: gille@ens.fr

2010 Mathematics subject classification. 20G05.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_3,

and this fact essentially characterizes fields of cohomological dimension ≤ 2 (see below).

One can discuss the conjecture with respect to the group classification or with respect to fields. With respect to groups, the main evidence for the conjecture is provided by classical groups, for which the result was established by Bayer–Parimala (1995, [4]). With respect to fields, evidence for the conjecture was provided by imaginary number fields (Kneser [39], Harder [35], Chernousov [9], see [50, Sect. 6]) and more recently by function fields of complex surfaces. Over the latter fields, the result for exceptional groups with no factors of type E_8 was pointed out in 2002 in the paper [15] by Colliot–Thélène–Gille–Parimala. It was completed in 2008 for all types by He–de Jong–Starr [37], who used deformation methods. This result has a clear geometric meaning. If $G/\mathbf{C}$ is a semisimple simply connected group and X a smooth complex surface, then a G-torsor over X (or a G-bundle) is locally trivial with respect to the Zariski topology (see Sect. 6.6).

There are previous surveys on Galois cohomology discussing this topic. Tits' lectures at Collège de France in 1990–1991 discuss the Hasse principle and group classification [63]. Serre's Bourbaki seminar [54] deals among other things with progress on the conjecture up to 1994; see also Bayer's survey on classical groups [2]. For function fields of surfaces, see the surveys by Starr [58] and by Lieblich [41].

For exceptional groups (trialitarian, type E_6, E_7 and E_8), the general conjecture is still open despite some progress [11, 15, 17, 28].

We take this opportunity to point out that Serre's conjecture has some analogy with topology. Indeed, if $\mathbf{G}$ is a semisimple simply connected complex group, we know that $\pi_1(\mathbf{G}) = \pi_2(\mathbf{G}) = 0$, hence $\mathbf{G}$ is 2-connected. Then for every CW-complex of dimension ≤ 2, the $\mathbf{G}$-bundles over X are trivial (cf. [60, Th. 11.34]).

2 Fields of Cohomological Dimension ≤ 2

Let k be a field and l be a prime. Recall that k is of l-cohomological dimension $\mathrm{cd}_l(k) \leq d$ if $H^i(k, A) = 0$ for every finite l-primary Galois module A and for all $i \geq d+1$. We know that it is equivalent to the vanishing of $H^{d+1}(L, \mathbf{Z}/l\mathbf{Z})$ for any finite separable extension L/k.

Examples 2.1. Recall the following examples of fields of cohomological dimension 2.

(1) Imaginary number fields;
(2) Function fields of complex surfaces;
(3) Merkurjev's tower of fields F_∞, namely an extension of $\mathbf{C}(X_1, ..., X_{2n})$ such that the u-invariant is $u(F_\infty) = 2n$. Every $(2n+1)$-dimensional quadratic form over F_∞ is isotropic, but the form $\langle X_1, X_2, \ldots, X_{2n} \rangle$ remains anisotropic over F_∞. Furthermore, the tensor product of the quaternion algebras (X_{2i-1}, X_{2i}) for $i = 1, ..., n$ is a division algebra over F_∞ [44], [45, Th. 3].

The third example shows that central simple algebras and quadratic forms are not in general low dimensional objects. We already mentioned the following characterization which uses Merkurjev–Suslin's theorem [47].

Theorem 2.2. *[59, Th. 24.8] Let l be an invertible prime in k. The following are equivalent:*

1. $\mathrm{cd}_l(k) \leq 2$.
2. *For any finite separable extension L/k and any l-primary central simple L-algebra A/L, the reduced norm* $\mathrm{nrd} : A^\times \to L^\times$ *is surjective.*
3. *For any finite extension L/k and any l-primary central simple L-algebra A/L, the reduced norm* $\mathrm{nrd} : A^\times \to L^\times$ *is surjective.*

We added here the easy implication $(2) \Longrightarrow (3)$ which follows from the usual transfer argument. We say that k is of cohomological dimension $\leq d$ if k is of l-cohomological dimension $\mathrm{cd}_l(k) \leq d$ for all primes l.

If k is of positive characteristic p, we always have $\mathrm{cd}_p(k) \leq 1$; this explains the necessary change in the following analogous statement.

Theorem 2.3. *[27, Th. 7] Assume that* $\mathrm{char}(k) = p > 0$. *The following are equivalent:*

1. $H^3_p(L) = 0$ *for any finite separable extension L/k;*
2. *For any finite separable extension L/k and any l-primary central simple L-algebra A/L, the reduced norm* $\mathrm{nrd} : A^\times \to L^\times$ *is surjective.*

Here $H^3_p(k)$ is Kato's cohomology group, defined by means of logarithmic differential forms [38], see [32, Sect. 9]. We shall say that k is of separable p-dimension $\leq d$ if $H^{d+1}_p(L) = 0$ for all finite separable extension L/k, this defines the separable dimension $\mathrm{sd}_p(k)$ of k. For $l \neq p$, we let[1] $\mathrm{sd}_l(k) = \mathrm{cd}_l(k)$. If k is perfect, then $H^i_p(L) = 0$ for every finite extension L/k and for every $i \geq 2$. Hence if k is perfect and of cohomological dimension ≤ 2, k is of separable dimension ≤ 2.

Examples 2.4.

(1) The function field of a curve over a finite field is of separable dimension 2.
(2) The function field $k_0(S)$ of a surface over an algebraically closed field k_0 of characteristic $p \geq 0$ is of separable dimension 2.
(3) Given an arbitrary field F, Theorems 2.2 and 2.3 provide a way to construct a "generic" field extension E/F of separable dimension 2, see Ducros [19].

We can now state the strong form of Serre's conjecture II. For each simply connected group G, Serre defined the set $S(G)$ of primes in terms of the Cartan-Killing type of G, cf. [54, Sect. 2.2]. For absolutely almost simple groups, the primes are listed in Table 1.

[1] Kato defined the p-dimension $\dim_p(k)$ as follows [38]. If $[k : k^p] = \infty$, define $\dim_p(k) = \infty$. If $[k : k^p] = p^r < \infty$, $\dim_p(k) = r$ if $H^{r+1}_p(L) = 0$ for any finite extension L/k, and $\dim_p(k) = r + 1$ otherwise.

Table 1 $S(G)$ for absolutely almost simple groups

Type	$S(G)$
A_n $(n \geq 1)$	2 and the prime divisors of $n+1$
B_n $(n \geq 3)$, C_n $(n \geq 2)$, D_n (non-trialitarian for $n=4$)	2
G_2	2
trialitarian D_4, F_4, E_6, E_7	2, 3
E_8	2, 3, 5

Conjecture 2.5. *Let G be a semisimple and simply connected algebraic group. If* $\mathrm{sd}_l(k) \leq 2$ *for every prime* $l \in S(G)$*, then* $H^1(k,G) = 0$.

In the original conjecture, k was assumed perfect and of cohomological dimension ≤ 2. In characteristic $p > 0$, Serre's strengthened question furthermore assumed that $[k : k^p] \leq p^2$ if p belongs to $S(G)$ [54, Sect. 5.5]. Known results do not seem to indicate that this restriction is necessary.

So Conjecture 2.5 is indeed stronger than the original one. Theorems 2.2 and 2.3 show that the conjecture holds for groups of inner type A and that the hypothesis on k is sharp.

3 Link Between the Conjecture and the Classification of Groups

The classification of semisimple groups essentially reduces to that of semisimple simply connected groups G which are absolutely almost simple [40, Sect. 31.5][61]. This means that $G \times_k k_s$ is isomorphic to $\mathbf{SL}_{n,k_s}$, $\mathbf{Spin}_{2n+1,k_s}$, $\mathbf{Sp}_{2n,k_s}$, $\mathbf{Spin}_{2n,k_s}$,...

Let G/k be such a k-group and let $G \to G_{\mathrm{ad}}$ be the adjoint quotient of G. Denote by G^{q} its quasi-split form and by $G^{\mathrm{q}}_{\mathrm{ad}}$ its adjoint quotient. Then G is an inner twist of G^{q}, i.e., there exists a cocycle $z \in Z^1(k_s/k, G^q_{\mathrm{ad}}(k_s))$ such that $G \cong {}_zG^q$. We then identify G and ${}_zG^q$.

The other way around, we know that there exists a unique class $v_G = [a] \in H^1(k, G_{\mathrm{ad}})$ such that $G^q \cong {}_aG$ [40, 31.6]. We denote by $z^{\mathrm{op}} \in Z^1(k, {}_zG^q_{\mathrm{ad}})$ the opposite cocycle of z, it is defined by $\sigma \mapsto z_\sigma^{-1} \in {}_zG(k_s)$.

We have $G^q \cong {}_{z^{\mathrm{op}}}\left({}_zG^q\right)$. Hence the image of v_G under $H^1(k, G_{\mathrm{ad}}) \xrightarrow{\sim} H^1(k, {}_zG^q{}_{\mathrm{ad}})$ is nothing but $[z^{\mathrm{op}}]$. We have an exact sequence

$$1 \to Z(G) \to G \to G_{\mathrm{ad}} \to 1$$

of k-algebraic groups with respect to the $fppf$-topology (faithfully flat of finite presentation, see [18, III] or [56]). This gives rise to an exact sequence of pointed sets [5, app. B]

$$\begin{aligned} 1 \to Z(G)(k) \to G(k) \to G_{\mathrm{ad}}(k) \xrightarrow{\varphi_G} H^1_{fppf}(k, Z(G)) \to \\ \to H^1_{fppf}(k, G) \to H^1_{fppf}(k, G_{\mathrm{ad}}) \xrightarrow{\delta_G} H^2_{fppf}(k, Z(G)). \quad (3.1) \end{aligned}$$

The homomorphism φ_G is called the characteristic map and the mapping δ_G is the boundary. Since G (resp. G_{ad}) is smooth, the $fppf$-cohomology of G (resp. G_{ad}) coincides with Galois cohomology [55, XXIV.8], i.e., we have a bijection $H^1(k,G) \xrightarrow{\sim} H^1_{fppf}(k,G)$. Following [40, 31.6], one defines the Tits class of G by the following formula

$$t_G = -\,\delta_G\big(\nu_G\big) \in H^2_{fppf}(k,Z(G)).$$

By the compatibility property[2] under the torsion bijection τ_z [33, IV.4.2],

$$\begin{array}{ccc} H^1(k,G_{\mathrm{ad}}) & \xrightarrow{\delta_G} & H^2_{fppf}(k,Z(G)) \\ {\scriptstyle \tau_z}\big\downarrow \wr & & {\scriptstyle ?+\delta_{G^q}([z])}\big\downarrow \wr \\ H^1(k,G^q_{\mathrm{ad}}) & \xrightarrow{\delta_{G_{\mathrm{ad}}}} & H^2_{fppf}(k,Z(G^q)), \end{array}$$

we see that $t_G = \delta_{G^q}([z])$ which is indeed Tits' definition [63, Sect. 1].

Proposition 3.2. *Assume that $H^1(k,G)=1$.*

(1) The boundary map $H^1(k,G_{\mathrm{ad}}) \to H^2_{fppf}(k,Z(G))$ has trivial kernel.
(2) Let G' be an inner k-form of G^q. Then G and G' are isomorphic if and only if $t_G = t_{G'}$.

Proof. (1) follows from the exact sequence (3.1). For (2), let $z' \in Z^1(k,G^q_{\mathrm{ad}})$ be a cocycle such that $G' \cong {}_{z'}G$. We assume that $t_G = t_{G'}$. Hence $\delta_{G^q}([z]) = \delta_{G^q}([z']) \in H^2_{fppf}(k,Z(G^q))$. The compatibility above shows that

$$\tau_z^{-1}([z']) \in \ker\big(H^1(k,G_{\mathrm{ad}})\big) \to H^2_{fppf}(k,Z(G))\big).$$

By 1), we have $\tau_z^{-1}([z']) = [1] \in H^1(k,G_{\mathrm{ad}})$, hence $[z]=[z'] \in H^1(k,G_{\mathrm{ad}})$. Thus G and G' are k-isomorphic. $\square$

In conclusion, Serre's conjecture II implies that semisimple k-groups are classified by their quasi-split forms and their Tits classes. For more precise results for classical groups, see Tignol–Lewis [42]. The classification is of special importance in view of the rationality question for groups (Chernousov–Platonov [13], see also Merkurjev [46]) and then also for the Kneser-Tits problem (Gille [31]).

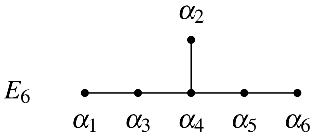
4 Approaches to the Conjecture

We would like to describe a few ways to attack the conjecture and their limitations. This is somehow artificial because in practice we work with all tools.

[2] Note that $Z(G) = Z(G^q)$ since G^q_{ad} acts trivially on $Z(G^q)$.

4.1 Subgroup Trick

Let Us Explain it within the following example due to Tits [64]. Let G/k be the split semisimple simply connected group of type



Assume that k is infinite. Let $z \in Z^1(k_s/k, G)$ and consider the twisted group $G' = {}_zG$. Since $t_{G'} = 0$, the 27-dimensional standard representation of G of highest weight $\overline{\omega}_6$ descends to G' by [62]. We then have a representation $\rho' : G' \to \mathbf{GL}(V)$. The point is that G' has a dense orbit in the projective space $X = \mathbf{P}(V)$, so there exists a k-rational point $[x]$ in that orbit. The connected stabilizer $(G'_x)^0$ is then semisimple of type F_4 [22, 9.12]. Assuming that Conjecture 2.5 holds for groups of type F_4, it follows that $(G'_x)^0$ is split. Hence G' has relative rank ≥ 4 and a glance at Tits' tables [61] tells us that G' is split. It is then easy to conclude that $[z] = 1 \in H^1(k,G)$.

The subgroup trick (and variants) was fully investigated by Garibaldi in his Lens lectures [22]. The underlying topic is that of prehomogeneous spaces, namely projective G-varieties with a dense orbit.

Unfortunately, this trick works only in few cases. Tits has shown that the general form of type E_8 is "almost abelian" namely has no nontrivial other reductive subgroups than maximal tori [64]. Together with Garibaldi, we have shown that the general trialitarian group is almost abelian [23].

4.2 Rost Invariant

In this case, the idea is to derive Serre's conjecture II from a more general setting. The Rost invariant [25] generalizes the Arason invariant for 3-fold Pfister form which (in characteristic $\neq 2$) attaches to a Pfister form $\phi = \langle\langle a,b,c\rangle\rangle$ the cup-product $e_3(\phi) = (a) \cup (b) \cup (c) \in H^3(k, \mathbf{Z}/2\mathbf{Z})$. We now see it as the cohomological invariant $H^1(k, \mathbf{Spin}_8) \to H^3(k, \mathbf{Z}/2\mathbf{Z}(2))$. More generally, for G/k simply connected and absolutely almost simple, there is a cohomological invariant

$$r_k : H^1(k,G) \to H^3(k, \mathbf{Q}/\mathbf{Z}Z(2))$$

where the p-primary part has to be understood in Kato's setting [25]. If this invariant has trivial kernel, then $H^1(k,G) = 1$ for G/k satisfying the hypothesis of Conjecture 2.5. This is the case for $\mathbf{Spin}_8$ by Arason's theorem, namely the invariant $e_3(\phi)$ determines ϕ.

4.3 Serre's Injectivity Question

A special case of a question raised by Serre in 1962 ([52], see also [54, Sect. 2.4]), is the following.

Question 4.1. *Let G/k be a connected linear algebraic group. Let $(k_i)_{i=1,..,r}$ be a family of finite field extensions of k such that $g.c.d.([k_i:k]) = 1$. Is the kernel of the map*

$$H^1(k,G) \to \prod_{i=1,..,r} H^1(k_i,G)$$

trivial ?

Remarks.

(1) The hypothesis of connectedness is necessary since there are counterexamples with finite constant groups [34, 49].
(2) The question was generalized by Totaro [65, question 0.2], see also [24].
(3) If k is of positive characteristic p, there exists a complete DVR R with residue field k and field of fractions $K = \mathrm{Frac}(R)$ of characteristic zero, and an R-group scheme $\mathbf{G}$ with special fiber G. An answer for $\mathbf{G}_K$ to Serre's question yields an answer for G. A fortiori and without lost of generality we can assume that the extensions k_i/k are separable.

We shall rephrase the question in terms of "special fields".

Definition 4.2. Let l be a prime. We say that a field k is l-special if every finite separable extension of k is of degree a power of l.

The subfield k_l of k consisting of elements fixed by a p-Sylow subgroup of $\mathcal{G}al(k_s/k)$ is l-special. We call k_l a *co-l-closure* of k. If we restrict Serre's question to finite separable extensions k_i/k and consider all cases, it can be rephrased by asking whether the map

$$H^1(k,G) \to \prod_l H^1(k_l,G)$$

has trivial kernel for l running over all primes. If the answer to this question is yes, then Conjecture II becomes a question for l-special fields for primes l in $S(G)$.

Here are the few cases where a positive answer to Serre's question is known: unitary groups (Bayer–Lenstra [3]), groups of type G_2, quasi-split groups of type D_4, F_4, E_6, E_7 [11, 21, 26].

If we know that the Rost invariant has zero kernel, then we easily deduce that the answer to Question 4.1 is yes. Thus we can answer Serre's question for groups of type G_2, and quasi-split semisimple simply connected groups of type D_4, F_4, E_6, and E_7.

5 Known Cases in Terms of Groups

5.1 Classical Groups

Recall that a semisimple simply connected group is called classical if its factors are of type A, B, C, or D, and there is no triality involved.

Theorem 5.1. *Let G be an absolutely almost simple and simply connected classical group over a field k as in Conjecture 2.5. Then $H^1(k,G) = 1$.*

If k is perfect or $\mathrm{char}(k) \neq 2$, this is the original Serre's conjecture II proven by Bayer–Parimala [4]. The general case is a recent work by Berhuy–Frings–Tignol [5]. Its proof is based on Weil's presentation of classical groups in terms of unitary groups of algebras with involutions [66]. This proof is characteristic free; in particular, it provides a somewhat different proof of Bayer–Parimala's theorem.

Possibly the trickiest case is that of outer groups of type A, namely unitary groups of central simple algebras equipped with an involution of the second kind. The proof in the number field case (which uses Landherr's Theorem) is already difficult, see [39, Sect. 5.5].

5.2 Quasi-split Exceptional Groups

For such groups, the best approach is by investigating the Rost invariant.

Theorem 5.2. *Let G/k be a quasi-split semisimple simply connected group of Cartan-Killing type G_2, F_4, D_4, E_6, or E_7. Then the Rost invariant $H^1(k,G) \to H^3(k,\mathbf{Q}/\mathbf{Z}(2))$ has trivial kernel.*

Here the field k is arbitrary, but proving the theorem boils down to the characteristic zero case by a lifting argument [27]. For the cases G_2, F_4, see [4] or [54]. As pointed out by Garibaldi, the D_4 case is done in *The Book of Involutions* but not stated in that shape. We need to know that a trialitarian algebra whose underlying algebra is split arises as the endomorphism of a twisted composition [40, 44.16] and to use results on degree 3 invariants of twisted compositions (ibid., 40.16). For type E_6 and E_7, this is due independently to Chernousov [11] and Garibaldi [21].

Thus Conjecture 2.5 holds for quasi-split groups of all types except E_8; we have an independent proof which is quite different since it is based on Bruhat-Tits theory [28]. For the split group of type E_8 denoted by E_8, the Rost invariant in general has a nontrivial kernel [30, appendix]. In characteristic 0, Semenov recently constructed a higher invariant

$$\ker\big[H^1(k,E_8) \to H^3(k,\mathbf{Q}/\mathbf{Z}(2))\big] \to H^5(k,\mathbf{Z}/2\mathbf{Z})$$

which is nontrivial since it is so already over the reals [57, Sect. 8]. Semenov's invariant has trivial kernel for two-special fields.

By means of norm group of varieties of Borel subgroups, the case of quasi-split groups is the input for proving the following.

Theorem 5.3. *[28, Th. 6] Let G/k be a semisimple simply connected group which satisfies the hypothesis of Conjecture 2.5. Let $\mu \subset G$ be a finite central subgroup of G. Then the characteristic map*

$$(G/\mu)(k) \to H^1_{fppf}(k,\mu)$$

is surjective.

Flat cohomology (see [56], [5, app. B] or [33]) is the right object if the order of μ is not invertible in k, it coincides with Galois cohomology if this order is invertible. By continuing the exact sequence of pointed sets

$$1 \to \mu(k) \to G(k) \to (G/\mu)(k) \to H^1_{fppf}(k,\mu) \to H^1_{fppf}(k,G),$$

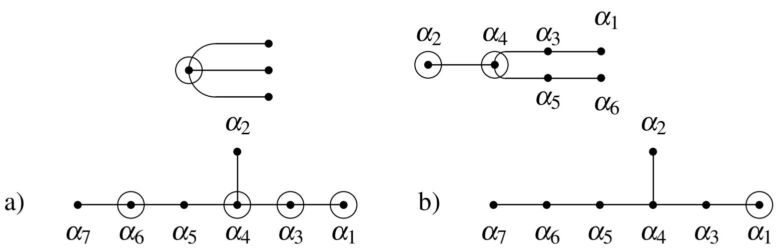
we see that $H^1_{fppf}(k,\mu) \to H^1_{fppf}(k,G)$ is the trivial map. In other words, the center of G does not contribute to $H^1(k,G)$. [The reason why we can avoid the type E_8 is that such groups have trivial center.]

5.3 Other Exceptional Groups

Theorem 5.4. *[11, 28] Let G/k be a semisimple group satisfying the hypothesis of Conjecture 2.5. Then $H^1(k,G) = 1$ in the following cases:*

1. *G is trialitarian and its Allen algebra is of index ≤ 2.*
2. *G is of quasi-split type ${}^1E_6$ or ${}^2E_6$ and its Tits algebra is of index ≤ 3.*
3. *G is of type E_7 and its Tits algebra is of index ≤ 4.*

Furthermore, those groups are quasi-split or isotropic respectively of Tits indexes



where case (a) (resp. (b)) is that of Tits algebra of index 2 (resp. 4). One more reason why other exceptional groups are not easy to work with is because they are anisotropic.

Corollary 5.5. *[15] Let G/k as in Theorem 5.4. For every separable finite field extension L/k, assume that every central simple L-algebras of period 2 (resp. 3) is of index ≤ 2 (resp. 3). If G is trialitarian or of type E_7 (resp. E_6), then $H^1(k,G)=1$.*

This is the case for function fields of surfaces as pointed out by Artin [1], thus Corollary 5.5 holds for these fields. In the paper [15] with Colliot–Thélène and Parimala, we exploited Serre's conjecture II for the study of arithmetic properties in this framework by proceeding with analogies with Sansuc's paper [51] in the number field case. On this topic, see also the paper by Borovoi and Kunyavskiĭ [7].

6 Known Cases in Terms of Fields

6.1 *l*-Special Fields

(a) If $l=2,3,5$ and k is an l-special field of separable dimension ≤ 2, Conjecture 2.5 holds for the split group of type E_8, see [10] for $l=5$ and [28, Sect. III.2].

(b) If $l=3$ and k is an l-special field of characteristic $\neq 2$ and separable dimension ≤ 2, then Conjecture 2.5 holds for trialitarian groups. For $l=3$, this follows from Theorem 5.2.

In both cases, a positive answer to Serre's injectivity question would provide Conjecture 2.5 for those groups.

6.2 Complete Valued Fields

Let K be a henselian valued field for a discrete valuation with perfect residue field κ. A consequence of the Bruhat–Tits decomposition for Galois cohomology over complete fields is the following.

Theorem 6.1. *(Bruhat–Tits [8, Cor. 3.15]) Assume that κ is of cohomological dimension ≤ 1. Let G/K be a simply connected semisimple group. Then $H^1(K,G)=1$.*

Note that the hypotheses imply that K is of separable dimension ≤ 2. Serre asked whether it can be generalized when assuming $[\kappa:\kappa^p]\leq p$ [54, 5.1]. The hypothesis $[\kappa:\kappa^p]\leq p$ alone is not enough here because $K=\mathbf{F}_p((x))((y))$ is of separable dimension 3 and is complete with residue field $\mathbf{F}_p((x))$.

But if κ is separably closed and $[\kappa:\kappa^p]\leq p$, then K is of separable dimension 1 and enough cases of the vanishing of $H^1(\kappa((x)),G)$ have been established in view of the proof of Tits conjectures on unipotent subgroups [29]. The general case is still open.

Note also that the conjecture is proven for fraction fields of henselian two dimensional local rings (e.g. $\mathbf{C}[[x,y]]$) with algebraically closed residue field of characteristic zero [15]. For the E_8 case, a key point is that the derived group of the absolute Galois group is of cohomological dimension 1 [17, Th. 2.2].

6.3 Global Fields

The number field case is due to Kneser for classical groups [39], Harder for exceptional groups except the type E_8 [35, I, II], and Chernousov for the type E_8 [9], see [50]. The function field case is due to Harder [35, III].

6.4 Function Fields

He, de Jong, and Starr have proven Conjecture 2.5 for split groups over function fields in a uniform way and in arbitrary characteristic.

Theorem 6.2. *[37, Cor. 1.5] Let k be an algebraically closed field and let K be the function field of a quasi-projective smooth surface S. Let G be a split semisimple simply connected group over k. Then* $H^1(K,G) = 1$.

For cases other than E_8, the conjecture had been establised by case by case considerations [15]. Hence Conjecture 2.5 is fully proven for function fields of surfaces. The proof of Theorem 6.2 is based on the existence of sections for fibrations in rationally simply connected varieties.

Theorem 6.3. *[37, Th. 1.4] Let S/k as in Theorem 6.2. Let X/S be a projective morphism whose geometric generic fiber is a twisted flag variety. Assume that* $\mathrm{Pic}(X) \to \mathrm{Pic}(X \times_K \overline{K})$ *is surjective. Then $X \to S$ has a rational section.*

The assumption on the Picard group means that there is no "Brauer obstruction". By application to higher Severi-Brauer schemes, this statement yields as corollary de Jong's theorem "period=index" [36] for central simple algebras over such fields; see also [14].

It is the first classification-free item in this survey.

6.5 Why Theorem 6.3 Implies Theorem 6.2

We take the opportunity to reproduce here our argument.

Lemma 6.4. *Let G/F be a semisimple simply connected group over a field F. Let E/F be a G-torsor.*

(1) $\mathrm{Pic}(E) = 0$ *and we have an exact sequence*

$$0 \to \mathrm{Br}(F) \to \mathrm{Br}(E) \to \mathrm{Br}(E \times_F F_s).$$

(2) Let P be an F-parabolic subgroup of G and let E/P be the variety of parabolic subgroups of the twisted F-group $E(G)$ of the same type as P. Then we have an exact sequence

$$0 \to \mathrm{Br}(F) \to \mathrm{Br}(E/P) \to \mathrm{Br}(E/P \times_F F_s)$$

and an isomorphism $\mathrm{Pic}(E/P) \xrightarrow{\sim} \mathrm{Pic}(E/P \times_F F_s)^{\mathcal{G}al(F_s/F)}$.

Proof. (1): We have $H^1(F, (F_s)^\times) = 0$ and $\mathrm{Pic}(E \times_F F_s) \cong \mathrm{Pic}(G \times_F F_s) = 0$ since G is simply connected [20]. The first terms of the Hochschild-Serre spectral sequence $H^p(\mathcal{G}al(F_s/F), H^q(E \times_F F_s, \mathbf{G}_m)) \Longrightarrow H^{p+q}(E, \mathbf{G}_m)$ show that $\mathrm{Pic}(E) = 0$ and that the sequence $0 \to \mathrm{Br}(F) \to \mathrm{Br}(E) \to \mathrm{Br}(E \times_F F_s)$ is exact.

(2): The morphism $E \to E/P$ (i.e., the twist of $G \to G/P$ by the torsor E) gives rise to a map $\mathrm{Br}(E/P) \to \mathrm{Br}(E)$. We claim that this map is injective. Since the generic fiber of $E \to E/P$ is isomorphic to $P \times_F F(E/P)$, the map $\mathrm{Br}(F(E/P)) \to \mathrm{Br}(F(E))$ is an injection by the specialization trick [32, lem. 5.4.6]. But $\mathrm{Br}(E/P)$ injects in $\mathrm{Br}(F(E/P))$, hence the claim. We look at the commutative diagram

$$\begin{array}{ccccccc}
 & & & & 0 & & \\
 & & & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Br}(F) & \longrightarrow & \mathrm{Br}(E/P) & \longrightarrow & \mathrm{Br}(E/P \times_F F_s) \\
 & & \| & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Br}(F) & \longrightarrow & \mathrm{Br}(E) & \longrightarrow & \mathrm{Br}(E \times_F F_s).
\end{array}$$

Since the bottom sequence is exact, we get by diagram chasing that the upper horizontal sequence is exact as well. The second isomorphism $\mathrm{Pic}(E/P) \xrightarrow{\sim} \mathrm{Pic}(E/P \times_F F_s)^{\mathcal{G}al(F_s/F)}$ comes from the Hochschild-Serre spectral sequence. □

For complete results on Picard and Brauer groups of twisted flag varieties, see Merkurjev–Tignol [48, Sect. 2].

Proposition 6.5. *[37, Th. 1.4] Let S/k be as in Theorem 6.2. Let G/K be a semisimple simply connected K-group which is an inner form and let P be a K-parabolic subgroup of G. Then the map $H^1(K,P) \to H^1(K,G)$ is bijective.*

Proposition 6.5 implies Theorem 6.2 by taking a Borel subgroup of G because $H^1(K,B) = 1$.

Proof. Injectivity is a general fact due to Borel–Tits ([6], théorème 4.13.a). Let E/K be a G-torsor of class $[E] \in H^1(K,G)$. After shrinking S, we can assume that G/K

extends to a semisimple group scheme $\mathbf{G}/S$, P/K extends to an S-parabolic subgroup scheme $\mathbf{P}/S$ and that E/K extends to a $\mathbf{G}$-torsor $\mathbf{E}/S$ [43]. By étale descent, we can twist the S-group scheme $\mathbf{G}/S$ by inner automorphisms, namely define the S-group scheme $\mathbf{E}(\mathbf{G})/S$. We then define $\mathbf{V}/S := \mathbf{E}/\mathbf{P}$, i.e., the scheme of parabolic subgroup schemes of $\mathbf{E}(\mathbf{G})/S$ ([55], exp. XXVI) of the same type as P. The morphism $\pi : \mathbf{V} \to X$ is projective, smooth and has geometrically integral fibers. Set $V = \mathbf{V} \times_S K$; this is a generalized twisted flag variety. Since G is assumed to be an inner form, $\mathrm{Pic}(V \times_K K_s)$ is a trivial $\mathcal{G}al(K_s/K)$-module. By Lemma 6.4.2, the map

$$\mathrm{Pic}(V) \to \mathrm{Pic}(V \times_K K_s)$$

is onto. Thus the composite map $\mathrm{Pic}(\mathbf{V}) \to \mathrm{Pic}(V) \to \mathrm{Pic}(V \times_K K_s)$ is onto. Theorem 6.2 applies and shows that $V(K) \neq \emptyset$. Thus the torsor E admits a reduction to P ([53], Sect. I.5, proposition 37), that is $[E] \in \mathrm{im}\big(H^1(K,P) \to H^1(K,G)\big)$. We conclude that the mapping $H^1(K,P) \to H^1(K,G)$ is surjective. □

The Grothendieck-Serre conjecture on rationally trivial torsors was proven by Colliot–Thélène and Ojanguren for torsors over a semisimple group defined over an algebraic closed field [16]. Thus He–de Jong–Starr's theorem has the following geometric application.

Corollary 6.6. *Let S/k be a smooth quasi-projective surface. Let G/k be a (split) semisimple simply connected group. Let E/S be a G-torsor. Then E is locally trivial for the Zariski topology.*

7 Remaining Cases and Open Questions

Here are some of the remaining cases and open questions.

• Provide a classification free proof for the case of totally imaginary number fields, at least in the quasi-split case.

• The first remaining cases of Conjecture 2.5 are those of trialitarian groups, groups of type E_6 over a 3-special field, groups of type E_7 over a 2-special field, and groups of type E_8.

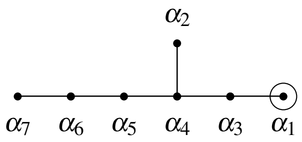
• What about higher mod 3 cohomological invariants of E_8?

• Let K be the function field of a surface over an algebraically closed field. Are K-division algebras cyclic? Is it true that $\mathrm{cd}(K_{ab}) = 1$ where K_{ab} stands for the abelian closure of K?

In the global field case, class field theory answers both questions positively. This question on K_{ab} is due to Bogomolov and makes sense for arbitrary fields. As noticed by Chernousov, Reichstein, and the reviewer, a positive answer would provide a positive answer to Serre's conjecture II for groups of type E_8 [12].

• For the Kneser-Tits conjecture for perfect fields of cohomological dimension ≤ 2, there remains only the case of a group with the following Tits index, see [31, Sect. 8.2]:

$E_{7,1}^{66}$



Acknowledgements We thank Skip Garibaldi, Fabien Morel, and Jean-Pierre Tignol for useful comments which improved the exposition.

References

1. J. Kr. Arason, *Cohomologische invarianten quadratischer Formen*, J. Algebra **36** (1975), 448–491.
2. E. Bayer-Fluckiger, *Galois cohomology of the classical groups*, Quadratic forms and their applications (Dublin, 1999), 1–7, Contemp. Math. **272** (2000), American Mathematical Society, Providence, RI.
3. E. Bayer-Fluckiger and H.W. Lenstra Jr., *Forms in odd degree extensions and self-dual normal bases*, Am. J. Math. **112** (1990), 359–373.
4. E. Bayer-Fluckiger and R. Parimala, *Galois cohomology of the classical groups over fields of cohomological dimension* ≤ 2, Invent. Math. **122** (1995), 195–229.
5. G. Berhuy, C. Frings and J.-P. Tignol, *Galois cohomology of the classical groups over imperfect fields*, J. Pure Appl. Algebra **211** (2007), 307–341.
6. A. Borel and J. Tits, *Groupes réductifs*, Pub. Math. IHES **27** (1965), 55–152.
7. M. Borovoi, B. Kunyavskiĭ, and P. Gille, *Arithmetical birational invariants of linear algebraic groups over two-dimensional geometric fields*, J. Algebra **276** (2004), 292–339.
8. F. Bruhat and J. Tits, *Groupes réductifs sur un corps local. Chap. III. Complément et applications à la cohomologie galoisienne*, J. Fasc. Sci. Tokyo **34** (1987), 671–698.
9. V. Chernousov, *The Hasse principle for groups of type* E_8, Dokl. Akad. Nauk. SSSR **306** (1989), 1059–1063 and english transl. in Math. USSR-Izv. **34** (1990), 409–423.
10. ———, *Remark on the Serre mod-5 invariant for groups of type* E_8, Math. Zametki **56** (1994), 116–121, Eng. translation Math. Notes **56** (1994), 730–733
11. ———, *The kernel of the Rost invariant, Serre's conjecture II and the Hasse principle for quasi-split groups* ${}^{3,6}D_4, E_6, E_7$, Math. Ann. **326** (2003) , 297–330.
12. V. Chernousov, P. Gille and Z. Reichstein, *Resolution of torsors by abelian extensions*, J. Algebra 296 (2006), 561–581.
13. V. Chernousov and V. P. Platonov, *The rationality problem for semisimple group varieties*, J. Reine Angew. Math. **504** (1998), 1–28.
14. J.-L. Colliot-Thélène, *Algèbres simples centrales sur les corps de fonctions de deux variables (d'après A. J. de Jong)*, Séminaire Bourbaki, Exp. No. 949 (2004/2005), Astérisque **307** (2006), 379–413.
15. J.-L. Colliot-Thélène, P. Gille and R. Parimala, *Arithmetic of linear algebraic groups over 2-dimensional geometric fields*, Duke Math. J. **121** (2004), 285–341.
16. J.–L. Colliot–Thélène and M. Ojanguren, *Espaces principaux homogènes localement triviaux*, Inst. Hautes Études Sci. Publ. Math. **75** (1992), 97–122.
17. J.–L. Colliot–Thélène, M. Ojanguren, and R. Parimala, *Quadratic forms over fraction fields of two-dimensional Henselian rings and Brauer groups of related schemes*, Algebra, arithmetic and geometry, Part I, II (Mumbai, 2000), 185–217, Tata Inst. Fund. Res. Stud. Math. **16** (2002), Bombay.
18. M. Demazure and P. Gabriel, *Groupes algébriques*, Masson, Paris, France (1970).
19. A. Ducros, *Dimension cohomologique et points rationnels sur les courbes*, J. Algebra **203** (1998), 349–354.

20. R. Fossum and B. Iversen, *On Picard groups of algebraic fibre spaces*, J. Pure Appl. Algebra **3** (1973), 269–280.
21. R.S. Garibaldi, *The Rost invariant has trivial kernel for quasi-split groups of low rank*, Comment. Math. Helv. **76** (2001), 684–711.
22. ———, *Cohomological invariants: exceptional groups and spin groups*, With an appendix by Detlev W. Hoffmann. Mem. Am. Math. Soc. **200** (2009), no. 937,
23. R.S. Garibaldi and P. Gille, *Algebraic groups with few subgroups*, J. Lond. Math. Soc. **80** (2009), 405–430.
24. R.S. Garibaldi and D.W. Hoffmann, *Totaro's question on zero-cycles on G_2, F_4 and E_6 torsors*, J. Lond. Math. Soc. **73** (2006), 325–338.
25. R.S. Garibaldi, A.A. Merkurjev and J.-P. Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, 28 (2003). American Mathematical Society, Providence.
26. P. Gille, *La R-équivalence sur les groupes algébriques réductifs définis sur un corps global*, Inst. Hautes Études Sci. Publ. Math. **86** (1997), 199–235.
27. ———, *Invariants cohomologiques de Rost en caractéristique positive*, K-Theory **21** (2000), 57–100.
28. ———, *Cohomologie galoisienne des groupes quasi-déployés sur des corps de dimension cohomologique* ≤ 2, Compositio Math. **125** (2001), 283–325.
29. ———, *Unipotent subgroups of reductive groups in characteristic* $p > 0$, Duke Math. J. **114** (2002), 307–328.
30. ———, *An invariant of elements of finite order in semisimple simply connected algebraic groups*, J. Group Theory **5** (2002), 177–197.
31. ———, *Le problème de Kneser-Tits*, Astérisque **326** (2009), 39–82.
32. P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics **101** (2006), Cambridge University Press, Cambridge.
33. J. Giraud, *Cohomologie non abélienne*, Die Grundlehren der mathematischen Wissenschaften **179** (1971), Springer-Verlag, Berlin.
34. D. Goldstein, R.M. Guralnick, E.W. Howe, M.E. Zieve, *Nonisomorphic curves that become isomorphic over extensions of coprime degrees*, J. Algebra **320** (2008), 2526–2558.
35. G. Harder, *Über die Galoiskohomologie halbeinfacher Matrizengruppen I* Math. Zeit. **90** (1965), 404–428, II Math. Zeit. **92** (1966), 396–415, III J. für die reine angew. Math. **274/5** (1975), 125–138.
36. A.J. de Jong, *The period-index problem for the Brauer group of an algebraic surface*, Duke Math. J. **123** (2004), 71–94.
37. A.J. de Jong, X. He and J.M. Starr, *Families of rationally simply connected varieties over surfaces and torsors for semisimple groups*, preprint (2008), arxiv:0809.5224.
38. K. Kato, *Galois cohomology of complete discrete valuation fields*, Lect. Notes in Math. **967** (1982), 215–238.
39. M. Kneser, *Lectures on Galois cohomology*, Tata institute (1969).
40. M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The book of involutions, avec une préface de J. Tits*, American Mathematical Society Colloquium Publications **44** (1998), American Mathematical Society, Providence, RI.
41. M. Lieblich, *Deformation theory and rational points on rationally connected varieties*, in this volume.
42. D.W. Lewis and J.-P. Tignol, *Classification theorems for central simple algebras with involution*, Manuscripta Math. **100** (1999), 259–276.
43. B. Margaux, *Passage to the limit in non-abelian Čech cohomology*, Journal of Lie Theory **17** (2007), 591–596.
44. A. S. Merkurjev, *Simple algebras and quadratic forms*, Izv. Akad. Nauk SSSR **55** (1991), 218–224.
45. ———, *K-theory of simple algebras*, K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992), 65–83, Proc. Sympos. Pure Math. **58.1** (1995) American Mathematical Society, Providence, RI.
46. ———, *K-theory and algebraic groups*, European Congress of Mathematics, Vol. II (Budapest, 1996), 43–72, Progr. Math. **169** (1998), Birkhäuser.

47. A.S. Merkurjev and A.A. Suslin, *$\mathscr{K}$-cohomology of Severi-Brauer varieties and norm residue homomorphism*, Izv. Akad. Nauk SSSR **46** (1982), 1011–1046, english translation: Math. USSR Izv. **21** (1983), 307–340.
48. A.S. Merkurjev and J.-P. Tignol, *The multipliers of similitudes and the Brauer group of homogeneous varieties*, J. Reine Angew. Math. **461** (1995), 13–47.
49. R. Parimala, *Homogeneous varieties—zero-cycles of degree one versus rational points*, Asian J. Math. **9** (2005), 251–256.
50. V. P. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure Appl. Math. **139** (1994), Academic Press, London.
51. J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires*, J. Reine Angew. Math. **327** (1981), 12–80.
52. J-P. Serre, *Cohomologie galoisienne des groupes algébriques linéaires*, Colloque sur la théorie des groupes algébriques linéaires, Bruxelles (1962), 53–68.
53. ———, *Cohomologie galoisienne*, cinquième édition révisée et complétée, Lecture Notes in Mathematics **5**, Springer-Verlag, Berlin.
54. ———, *Cohomologie galoisienne: Progrès et problèmes*, Séminaire Bourbaki, exposé 783 (1993–94), Astérisque **227** (1995).
55. *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, (1970) Springer, Berlin.
56. S. Shatz, *Cohomology of artinian group schemes over local fields*, Ann. of Math. **79** (1964), 411–449.
57. N. Semenov, *Motivic construction of cohomological invariants*, preprint (2008), arxiv:0905.4384v1.
58. J. Starr, *Rational points of rationally connected and rationally simply connected varieties*, preprint (2008).
59. A. A. Suslin, *Algebraic K-theory and the norm–residue homomorphism*, J. Soviet. **30** (1985), 2556–2611.
60. R. Switzer, *Algebraic topology—homotopy and homology*, Die Grundlehren der mathematischen Wissenschaften, Band 212 (1975), Springer-Verlag, Berlin.
61. J. Tits, *Classification of algebraic semisimple groups*, Algebraic Groups and Discontinuous Subgroups, Proc. Sympos. Pure Math., Boulder, Colo. (1965) pp. 33–62, Amer. Math. Soc.
62. ———, *Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque*, J. Reine Angew. Math. **247** (1971), 196–220.
63. ———, *Résumé des cours du Collège de France 1990–91*, Annuaire du Collège de France.
64. ———, *Sur les degrés des extensions de corps déployant les groupes algébriques simples*, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), 1131–1138.
65. B. Totaro, *Splitting fields for E_8-torsors*, Duke Math. J. **121** (2004), 425–455.
66. A. Weil, *Algebras with involutions and the classical groups*, J. Indian Math. Soc. **24** (1960), 589–623.

Field Patching, Factorization, and Local–Global Principles

Daniel Krashen

Summary The method of field patching has proven useful in obtaining results on Galois theory, central simple algebras, and quadratic forms. A crucial ingredient for this was proving certain "factorization" results for connected, rational linear algebraic groups. In this paper, we explore other possible applications of field patching by examining the relationship between factorization results and local–global principles, and also by extending the known factorization results to connected, retract rational linear algebraic groups.

1 Introduction

The goal of this paper is twofold – first to give an introduction to the method of field patching as first presented in [HH], and later used in [HHK09], paying special attention to the relationship between factorization and local–global principles and second, to extend the basic factorization result in [HHK09] to the case of retract rational groups, thereby answering a question posed to the author by J.-L. Colliot-Thélène.

Throughout, we fix a complete discrete valuation ring T with field of fractions K and residue field k. Let $t \in T$ be a uniformizer. Let X/K be a smooth projective curve and F its function field.

Broadly speaking, the method of field patching is a procedure for constructing new fields F_ξ which will be in certain ways simpler than F, and to reduce problems concerning F to problems about the various F_ξ. Overall, there are two ways in which

Daniel Krashen
Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA,
e-mail: dkrashen@math.uga.edu

2010 Mathematics subject classification. 12J25, 20G15.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_4,

this is done. Let us suppose that we are interested in studying a particular type of arithmetic object, such as a quadratic form, a central simple algebra, etc.

Constructive Strategy (Patching)

This consists in showing that under suitable hypotheses, algebraic objects defined over the fields F_ξ which are "compatible," exactly correspond to objects defined over F (see Theorem 3.2.3). One may then use this idea to construct new examples and counterexamples of such objects by building them "locally."

Deconstructive Strategy (Local–Global Principle)

We say that a particular type of algebraic object satisfies a local–global principle if whenever an object defined over F becomes "trivial" when scalars are extended to each F_ξ, it must in fact have been trivial to begin with (see Sect. 2.2).

In this paper, we will not focus on these applications, which are discussed for example in [HH,HHK09,HHK,CTPS]. Instead, we focus on elucidating and extending the underlying methods used.

2 Patches and Local–Global Principles

2.1 Fields Associated to Patches

The fields F_ξ are not canonically defined – they depend on a number of choices, beginning with the choice of a model for X over T.

Definition 2.1.1 (models). A *model* for the scheme X/K is defined to be a connected normal projective $\mathbb{P}^1_T$-scheme $\widehat{X}$ such that

1. The structure morphism $f:\widehat{X}\to\mathbb{P}^1_T$ is finite,
2. Considered as a T-scheme, the generic fiber $\widehat{X}_K$ is isomorphic to X,
3. The reduced closed fiber $\widehat{X}_k^{\mathrm{red}}$ is a normal crossings divisor in $\widehat{X}$,
4. $f^{-1}(\infty)$ contains all the singular points of the reduced closed fiber $\widehat{X}_k^{\mathrm{red}}$.

Given a model $\widehat{X}$ (we will generally suppress the morphism $f:\widehat{X}\to\mathbb{P}^1_T$ from the notation), we let $S(\widehat{X})$ denote the set of closed points in $f^{-1}(\infty)$ and $\mathscr{U}(\widehat{X})$ denote the set of connected (or equivalently, irreducible) components of $\widehat{X}_k^{\mathrm{red}}\setminus S(\widehat{X})$. These sets play a critical role in what follows.

Warning 2.1.2. In other sources such as [HH, HHK09, HHK], $\widehat{X}$ is not given the structure of a $\mathbb{P}^1_T$-scheme, but rather the structure of a T scheme together with a distinguished set of closed points S. In this context, one is allowed more general sets S. The reader must keep in mind that a model $\widehat{X}$ comes with the extra structure of a morphism to $\mathbb{P}^1$ throughout!

It is perhaps a bit odd to include the finite morphism to $\mathbb{P}^1_T$ as part of the definition of a model – by comparison, in [HH], it is only assumed that one should start with a projective T-curve with a set S of closed points such that there exists a finite T-morphism to a curve with smooth reduced closed fiber and such that the set S is the inverse image of a set of closed points under this morphism. We include the morphism to $\mathbb{P}^1_T$ as part of our definition simply as a matter of convenience of exposition. The following lemma shows that it is not much of an extra assumption, however:

Lemma 2.1.3 ([HH, Prop. 6.6]). *Suppose $\widehat{X}$ is a projective T-curve and $S \subset \widehat{X}$ a finite set of closed points. Then there exists a finite morphism $f : \widehat{X} \to \mathbb{P}^1$ such that $S \subset f^{-1}(\infty)$.*

For the remainder of the section, we will suppose that we are given such a model $\widehat{X}$, and we let $F = F(\widehat{X})$ be its function field. Given any nonempty subset of points $Z \subset \widehat{X}$, we define

$$R_Z = \{f \in F \mid \text{for all } P \in Z \text{ and } f \in \mathscr{O}_{\widehat{X},P}\}.$$

We will define fields associated to two particular types of subsets Z:

Definition 2.1.4 (Fields associated to closed points). Let $P \in \widehat{X}$ be a closed point. We define $R_P = R_{\{P\}} = \mathscr{O}_{\widehat{X},P}$, $\widehat{R}_P$ its completion with respect to its maximal ideal, and F_P the field of fractions of $\widehat{R}_P$.

Definition 2.1.5 (Fields associated to open subsets of $\widehat{X}_k^{\mathbf{red}}$). Let $U \subset \widehat{X}_k^{\mathrm{red}}$ be a nonempty irreducible Zariski-open affine subset of the reduced closed fiber which is disjoint from the singular locus of $\widehat{X}_k^{\mathrm{red}}$. We let $\widehat{R}_U$ be the completion of R_U with respect to the ideal tR_U, and F_U the field of fractions of $\widehat{R}_U$.

Note that there are natural maps $F \subset F_U, F_P$ for any such P and U, as well as inclusions $F_U \to F_V$ and $F_U \to F_P$, whenever $V \subset U$ or $P \in U$, respectively.

2.2 Some Local–Global Principles

We may now give some examples of local–global principles. For these, we assume that X/K is a smooth projective curve where K is a complete discretely valued field with valuation ring T, and that we are given a model $\widehat{X} \to \mathbb{P}^1$. We let F be the function field of X.

Theorem 2.2.1 (Local–global principle for the Brauer group [HH, Th. 4.10]). *Let* $\mathrm{Br}(\cdot)$ *denote the Brauer group. The natural homomorphism*

$$\mathrm{Br}(F) \to \left(\prod_{P \in S(\widehat{X})} \mathrm{Br}(F_P)\right) \times \left(\prod_{U \in \mathscr{U}(\widehat{X})} \mathrm{Br}(F_U)\right)$$

is injective.

We give a proof of this result on the next page. In fact, we will see later, using patching, that this may be extended to a three term exact sequence by adding a term on the right (see Theorem 3.3.1).

Theorem 2.2.2 (Local–global principle for isotropy [HHK09, Th. 4.2]). *Suppose q is a regular quadratic form of dimension at least* 3*, and* $\mathrm{char}(F) \neq 2$*. If q_{F_P} and q_{F_U} are isotropic for every $P \in S(\widehat{X})$ and $U \in \mathscr{U}(\widehat{X})$ then q is also isotropic.*

The proof is given below. See also Theorem 3.3.2 for a related result.

Both of these principles in fact, may be regarded as special cases of either of the following results, the main new results of this paper:

Definition 2.2.3. Suppose H is a variety over F and G is an algebraic group which acts on H. We say that G *acts transitively* on H if for every field extension L/F, the group $G(L)$ acts transitively on the set $H(L)$.

The following result generalizes [HHK09, Th. 3.7] by weakening the hypothesis of rationality to allow for retract rational groups as well:

Theorem 2.2.4 (Local–global principle for varieties with transitive actions). *Suppose G is a connected retract rational algebraic group defined over F, and H is a variety on which G acts transitively. Then $H(F) \neq \emptyset$ if and only if $H(F_P), H(F_U) \neq \emptyset$ for all $P \in S(\widehat{X})$ and $U \in \mathscr{U}(\widehat{X})$.*

This theorem follows quickly from Theorem 5.1.1, and its proof may be found just after the statement of this theorem on page 69. The proof of this in the case of retract rationality will occupy a good portion of this paper. Along the way, we will explore the connections between these local–global principles and the notion of "factorization" for the group G. The following corollary is particularly useful.

Corollary 2.2.5. *Suppose G is a connected retract rational reductive group over F and H is a projective homogeneous variety for G. Then $H(F) \neq \emptyset$ if and only if $H(F_P), H(F_U) \neq \emptyset$ for all $P \in S(\widehat{X})$ and $U \in \mathscr{U}(\widehat{X})$.*

Proof. This follows from the fact that the action of $G(F)$ on $H(F)$ is transitive. This in turn in a consequence of [Bor, Th. 20.9(iii)]. □

From these theorems (or even the versions assuming only rationality of G from [HHK09]), we may prove the above local–global results concerning the Brauer group and quadratic forms.

Proof (of Theorem 2.2.1). Let $\alpha \in \mathrm{Br}(F)$ and suppose $\alpha_{F_P} = 0$, $\alpha_{F_U} = 0$ for every $P \in S(\widehat{X})$, $U \in \mathscr{U}(\widehat{X})$. We need to show that $\alpha = 0$.

Let A be a central simple F algebra in the class of α and let H be the Severi-Brauer variety for A. Note that this is a homogeneous variety for the group $GL(A)$ which is rational, connected, and reductive. Recall that for a field extension L/F, $H(L)$ is nonempty exactly when $A \otimes_F L$ is a split algebra – that is to say, $\alpha_L = 0$. But since $\alpha_{F_P}, \alpha_{F_U} = 0$, we have $H(F_P), H(F_U) \neq \emptyset$ for every U, P. Consequently, by Corollary 2.2.5, it follows that $H(F) \neq \emptyset$ and so $\alpha = 0$ as desired. □

Proof (of Theorem 2.2.2). Let q be a quadratic form over F satisfying the hypotheses of the theorem. We wish to show that q is isotropic. Let H be the quadratic hypersurface of projective space defined by the equation $q = 0$. Recall that this is a homogeneous variety for the group $SO(q)$ which under the hypotheses is a rational, connected, reductive group (see [KMRT, p. 201, exercise 9]). As above, we immediately see that since $H(F_P), H(F_U)$ are nonempty for each $P \in S(\widehat{X})$ and $U \in \mathscr{U}(\widehat{X})$, we have by Corollary 2.2.5, $H(F) \neq \emptyset$ as desired. □

3 Patching

The fundamental idea of patching is that defining an algebraic object over the field F is equivalent to defining objects over each of the fields F_P for $P \in S(\widehat{X})$ and F_U for $U \in \mathscr{U}(\widehat{X})$, together with the data of how these objects agree on overlaps. This will be stated in this section in terms of an equivalence of categories. We will simply cite the results of [HH] Sects. 6 and 7 for the most part, but we focus more on the equivalence of tensor categories, and explore how to produce other examples of algebraic patching.

Suppose we are given a model $\widehat{X}$ for a curve X/K. Given a point $P \in S(\widehat{X})$, the height 1 primes of R_P which contain t correspond to the components of $\widehat{X}_k^{\mathrm{red}}$ incident to P. Each such component is the closure of a uniquely determined element $U \in \mathscr{U}(\widehat{X})$.

Definition 3.0.1 (Branches, and their fields). Given such a height 1 prime $\mathscr{P}$ of R_P, corresponding to an element $U \in \mathscr{U}(\widehat{X})$, a *branch* along U at P is an irreducible component of the scheme $\widehat{R}_P/\mathscr{P}\widehat{R}_P$. Alternately, these are in correspondence with the height one primes of $\widehat{R}_P$ containing $\mathscr{P}\widehat{R}_P$. Given such a height 1 prime $\wp$, we let $\widehat{R}_\wp$ be the t-adic completion of the localization of $\widehat{R}_P$ at $\wp$, and $F_\wp$ its field of fractions. We let $\mathscr{B}(\widehat{X})$ denote the set of all branches at all points in $S(\widehat{X})$.

The fields F_P and F_U come equipped with natural inclusions into $F_\wp$ which we now describe. We note that the natural inclusion $\widehat{R}_P \to \widehat{R}_\wp$ induces an inclusion of fields $F_P \to F_\wp$. Further, we note that $\widehat{R}_\wp$ is a 1 dimensional regular local ring, and hence a DVR, whose valuation is determined by considering the order of vanishing along the branch corresponding to $\wp$. In particular, considering the inclusion $F \subset F_P \subset F_\wp$, we find that all the elements of R_U, cannot have poles along any branch lying along U, and in particular, we see we have an inclusion $R_U \subset \widehat{R}_\wp$. Since the t-adic topology on $\widehat{R}_\wp$ is the same as the $\wp$-adic topology, we further find that $\widehat{R}_\wp$ is t-adically complete, and we therefore have an induced inclusion $F_U \to F_\wp$.

3.1 Patching Finite Dimensional Vector Spaces

Definition 3.1.1 (Patching problems). A *patching problem* is a collection V_ξ for $\xi \in S(\widehat{X}) \cup \mathscr{U}(\widehat{X})$, where V_ξ is a finite dimensional F_ξ vector space together with a collection of isomorphisms $\phi_\wp : V_P \otimes_{F_P} F_\wp \to V_U \otimes_{F_U} F_\wp$ of $F_\wp$ vector spaces for every branch $\wp$ at P on U. We denote this problem by (V, ϕ).

We define a *morphism of patching problems* $f : (V, \phi) \to (W, \psi)$ to be a collection of homomorphisms $f_\xi : V_\xi \to W_\xi$ such that whenever $\wp$ is a branch at P lying on U, the following diagram commutes:

$$\begin{tikzcd} V_P \otimes_{F_P} F_\wp \arrow[r, "f_P \otimes F_\wp"] \arrow[d, "\phi_\wp"'] & W_P \otimes_{F_P} F_\wp \arrow[d, "\psi_\wp"] \\ V_U \otimes_{F_U} F_\wp \arrow[r, "f_U \otimes F_\wp"'] & W_U \otimes_{F_U} F_\wp \end{tikzcd}$$

We see then that patching problems naturally form a category, which we denote by $\mathscr{P}\mathscr{P}(\widehat{X}, S)$. In fact, this category has a $\otimes$-structure as well defined by $(V, \phi) \otimes (W, \psi) = (V \otimes W, \phi \otimes \psi)$ where $(V \otimes W)_\xi = V_\xi \otimes_{F_\xi} W_\xi$ and

$$(\phi \otimes \psi)_\wp : (V \otimes W)_P \otimes_{F_P} F_\wp \to (V \otimes W)_U \otimes_{F_U} F_\wp$$

is given by $\phi_\wp \otimes_{F_\wp} \psi_\wp$ via the above identification. One may also verify that this monoidal structure is symmetric and closed, see [ML, VII.7].

Definition 3.1.2. If V is a vector space over F, we let $(\widetilde{V}, \mathbb{I})$ denote the patching problem defined by $\widetilde{V}_P = V_{F_P}$ and $\widetilde{V}_U = V_{F_U}$ and where $\mathbb{I}_\wp$ is induced by the natural identifications

$$(V \otimes_F F_P) \otimes_{F_P} F_\wp = V_\wp = (V \otimes_F F_U) \otimes_{F_U} F_\wp.$$

Theorem 3.1.3 ([HH, Th. 6.4]). *Consider the functor*

$$\Omega : \mathscr{V}\mathrm{ect}_{f.d.}(F) \to \mathscr{P}\mathscr{P}(\widehat{X}, S)$$

from the category of finite dimensional F-vector spaces to the category of patching problems defined by sending a finite dimensional vector space V to the patching problem $(\widetilde{V}, \mathbb{I})$. Then Ω is an equivalence of categories.

3.2 Patching Algebraic Objects

Definition 3.2.1. A *type of algebraic object* (generally abbreviated to simply a "type") is a symmetric closed monoidal category $\mathscr{T}$. If $\mathscr{T}$ is a type and L a field, then an algebraic object of type $\mathscr{T}$ over L is a strict symmetric closed monoidal functor (see [ML, Sects. VII.1, VII.7] and [Hov, Sect. 4.1] for definitions) from the category $\mathscr{T}$ to the category of finite dimensional vector spaces over L (with its natural symmetric closed monoidal structure). Morphisms between algebraic objects of type $\mathscr{T}$ are defined simply to be natural transformations between functors. We let $\mathscr{T}(L)$ denote the category of such objects.

Note that $\mathscr{T}$ in fact defines a (pseudo-)functor from the category of fields to the 2-category of categories (see [Gra] for definitions).

Despite the formality of this definition, one may observe that one may interpret an algebraic object of a given type $\mathscr{T}$ to be given by a vector space, or a collection of vector spaces, together with extra structure encoded by perhaps a collection of morphisms between various tensor powers of the vector spaces satisfying certain axioms, and where morphisms between these objects are given by collections of linear maps satisfying certain compatibilities with the extra structures given. For example, we might consider:

- Lie algebras,
- Alternative (or Jordan) algebras,
- Operads,
- Central simple algebras,
- Quadratic forms, where morphisms are isometries,
- Quadratic forms, where morphisms are similarities,
- Separable commutative or noncommutative algebras,
- G-Galois extensions of rings in the sense of [DI],
- and so on...

In these cases, the category $\mathscr{T}$ in question is simply given as the symmetric closed monoidal category generated by some set of objects (corresponding to the underlying vector spaces of the structure) and some morphisms (defining the structure of the algebra or form), such that certain diagrams commute which define the structure in question. For example, a central simple algebra is a vector space A together with a bilinear product $A \otimes A \to A$, and F-algebra structure $F \to A$ such that the canonical "sandwich map" of algebras

$$A \otimes A^{\mathrm{op}} \to \mathrm{Hom}(A, A)$$

is an isomorphism, see [DI, Chap. 2, Th. 3.4(iii)]. In this case, the category $\mathscr{T}$ is generated by a single element a, a morphism $a \otimes a \to a$ and $\mathbf{1} \to a$ (where $\mathbf{1}$ is the unit for the monoidal structure), and such that the natural map $a \otimes a \to \mathrm{Hom}(a, a)$ (where the Hom is defined by the closed structure) has an inverse.

To see quadratic forms and isometries in this way, one may simply let the category $\mathscr{T}$ be generated by a single element v a morphism $v \otimes v \to \mathbf{1}$, assumed to commute with the morphism switching the order of the v's. In the case of similarities instead of isometries, one may add a new object ℓ, and replace $v \otimes v \to \mathbf{1}$ with a morphism $v \otimes v \to \ell$. To force ℓ to correspond to a 1-dimensional vector space, one may then add to this category an inverse to the natural morphism $\mathbf{1} \to \ell \otimes \ell^* \cong \mathrm{Hom}(\ell, \ell)$.

Definition 3.2.2 (Patching problems). Let $\mathscr{T}$ be a type of algebraic object. A *patching problem of objects of type* $\mathscr{T}$ is a collection A_ξ for $\xi \in S(\widehat{X}) \cup \mathscr{U}(\widehat{X})$, where A_ξ is an object of type $\mathscr{T}$ over F_ξ, together with a collection of isomorphisms $\phi_\wp : A_P \otimes_{F_P} F_\wp \to A_U \otimes_{F_U} F_\wp$ in $\mathscr{T}(F_\wp)$. We denote this problem by (A, ϕ).

Just as with vector spaces, we may define morphisms of patching problems of objects of type $\mathscr{T}$, and again find that these form a tensor category, which we denote $\mathscr{P}\mathscr{P}_\mathscr{T}(\widehat{X})$. Again as before, if A is an algebraic object of type $\mathscr{T}$ over F, we may form a natural patching problem $(\widetilde{A}, \mathbb{I})$, and obtain a functor from $\mathscr{T}(F)$ to $\mathscr{P}\mathscr{P}_\mathscr{T}(\widehat{X})$.

Theorem 3.2.3. *Consider the functor*

$$\Omega_\mathscr{T} : \mathscr{T}(F) \to \mathscr{P}\mathscr{P}_\mathscr{T}(\widehat{X})$$

defined by sending an algebraic object A to the patching problem $(A, \mathbb{I})$. *Then* $\Omega_\mathscr{T}$ *is an equivalence of categories.*

Proof. Since we have an equivalence of categories $\mathscr{V}\mathrm{ect}_{\mathrm{f.d.}}(F) \cong \mathscr{P}\mathscr{P}(\widehat{X})$ by Theorem 3.1.3, it is immediate that this equivalence also induces an equivalence of functor categories

$$\mathscr{T}(F) = \mathrm{Fun}(\mathscr{T}, \mathscr{V}\mathrm{ect}_{\mathrm{f.d.}}(F) \cong \mathrm{Fun}(\mathscr{T}, \mathscr{P}\mathscr{P}(\widehat{X})) \cong \mathscr{P}\mathscr{P}_\mathscr{T}(\widehat{X}).$$

One may now check that this gives the desired equivalence. □

Remark 3.2.4. It would be interesting to know if one could extend this to equivalences of other kinds of objects. In particular, infinite dimensional vector spaces, finitely generated commutative algebras, or perhaps even to (some suitably restricted) categories of schemes. None of these fall under the definition of an algebraic object given above, and it is therefore not at all clear if the conclusions of Theorem 3.2.3 will still hold.

3.3 Central Simple Algebras and Quadratic Forms

For the following results, we suppose we are given $\widehat{X}$ a normal, connected, projective, finite $\mathbb{P}^1_T$-scheme. The machinery of patching gives the exactness of various exact sequences relating to field invariants derived from algebraic objects, such as the Brauer group $\mathrm{Br}(F)$ and the Witt group $W(F)$ of quadratic forms over F.

Theorem 3.3.1 (see [HH, Th. 7.2]). *We have an exact sequence:*

$$0 \to \mathrm{Br}(F) \to \left(\prod_{P\in S(\widehat{X})} \mathrm{Br}(F_P)\right) \times \left(\prod_{U\in\mathscr{U}(\widehat{X})} \mathrm{Br}(F_U)\right) \to \prod_{\wp\in\mathscr{B}(\widehat{X})} \mathrm{Br}(F_\wp).$$

Proof. Exactness on the left was noted in Theorem 2.2.1. To see exactness in the middle, suppose we have classes α_P, α_U such that $(\alpha_U)_{F_\wp} \cong (\alpha_P)_{F_\wp}$ whenever $\wp$ is a branch at P on U. Since there are only a finite number of points and components, we may choose an integer n such that each of the Brauer classes α_U, α_P may be represented by central simple algebras A_U, A_P of degree n. Now, by hypothesis, for each branch $\wp$ as above, we may find an isomorphism of central simple algebras $\phi_\wp : (A_P)_{F_\wp} \to (A_U)_{F_\wp}$. But this gives the data of a patching problem for central simple algebras, and therefore, we may find a central simple F-algebra A such that $A_{F_P} \cong A_P$ and $A_{F_U} \cong A_U$ as desired. □

Theorem 3.3.2. *We have an exact sequence:*

$$\mathrm{W}(F) \to \left(\prod_{P\in S(\widehat{X})} \mathrm{W}(F_P)\right) \times \left(\prod_{U\in\mathscr{U}(\widehat{X})} \mathrm{W}(F_U)\right) \to \prod_{\wp\in\mathscr{B}(\widehat{X})} \mathrm{W}(F_\wp)$$

Proof. The proof is very similar to the last one. Suppose we have Witt classes α_P, α_U such that $(\alpha_U)_{F_\wp} = (\alpha_P)_{F_\wp}$ whenever $\wp$ is a branch at P on U. Since there are only a finite number of points and components, we may choose an integer n such that each of the Witt classes α_U, α_P may be represented by quadratic forms q_U, q_P of the same dimension n. Now, by hypothesis and Witt's cancellation theorems, for each branch $\wp$ as above, we may find an isometry $\phi_\wp : (q_P)_{F_\wp} \to (q_U)_{F_{wp}}$. But this gives the data of a patching problem for quadratic forms, and therefore, we may obtain a form q over F such that the class α of q in $\mathrm{W}(F)$ has the property that $\alpha_{F_P} = \alpha_P$ and $\alpha_{F_U} = \alpha_U$. □

We note that exactness on the left is discussed in Theorem 2.2.2.

3.4 Properties of $\widehat{R}_P$, $\widehat{R}_U$, F_P, F_U

Let us now gather together some fundamental facts which we will need in the sequel.

Lemma 3.4.1 ([HH, Lemma 6.2]). *Suppose $\widehat{Y} \to \widehat{X}$ is a finite morphisms of projective, normal, finite $\mathbb{P}^1_T$-schemes. Then the natural inclusions of fields yield isomorphisms:*

$$F_P \otimes_{F(\widehat{X})} F(\widehat{Y}) \cong \prod F_{P'}, \quad F_U \otimes_{F(\widehat{X})} F(\widehat{Y}) \cong \prod F_{U'}, \quad F_\wp \otimes_{F(\widehat{X})} F(\widehat{Y}) \cong \prod F_{\wp'},$$

where P' (resp. U', $\wp'$) range over all the points (resp. components, branches) lying over P (resp. U, $\wp$).

Lemma 3.4.2 ([HH, Lemma 6.3]). *Let $\widehat{X}$ be a projective, normal, finite $\mathbb{P}^1_T$-scheme. Then the natural inclusions of fields yield an exact sequence of $F = F(\widehat{X})$-vector spaces:*

$$0 \to F \to \left(\prod_{P \in S(\widehat{X})} F_P\right) \times \left(\prod_{U \in \mathscr{U}(\widehat{X})} F_U\right) \to \prod_{\wp \in \mathscr{B}(\widehat{X})} F_\wp$$

Lemma 3.4.3. *Let $\mathfrak{V}, \mathfrak{W} \subset \mathfrak{U}$ be t-adically complete T-modules, and suppose that $\mathfrak{V}/t\mathfrak{V} + \mathfrak{W}/t\mathfrak{W} = \mathfrak{U}/t\mathfrak{U}$. Then $\mathfrak{V} + \mathfrak{W} = \mathfrak{U}$.*

Proof. Suppose $u \in \mathfrak{U}$. Let $v_0 = w_0 = 0$. We will inductively construct a sequence of elements $v_i \in \mathfrak{V}$ and $w_i \in \mathfrak{W}$ such that $v_i - v_{i+1} \in t^i\mathfrak{V}$, $w_i - w_{i+1} \in t^i\mathfrak{W}$, and $v_i + w_i - u \in t^i\mathfrak{U}$. By completeness, these will converge to elements $v \in \mathfrak{V}$ and $w \in \mathfrak{W}$ such that $v + w = u$.

Suppose we have constructed v_i, w_i satisfying the above hypotheses. Since $u - v_i - w_i \in t^i\mathfrak{U}$, we may write $u - v_i - w_i = t^i r$. By hypothesis, we may write $r = v' + w' + tr'$ for some $v' \in \mathfrak{V}$, $w' \in \mathfrak{W}$, and $r' \in \mathfrak{U}$. Setting $v_{i+1} = v_i + t^i v'$ and $w_{i+1} = w_i + t^i w'$ completes the inductive step. □

Lemma 3.4.4. *Considering $\mathbb{P}^1_T$, we have $\widehat{R}_{\mathbb{A}^1} + \widehat{R}_\infty = \widehat{R}_\wp$, where $\wp$ is the unique branch at ∞.*

Proof. Using Lemma 3.4.3, we only need to check that $\overline{R}_{\mathbb{A}^1} + \overline{R}_\infty = \overline{R}_\wp$, where

$$\overline{R}_{\mathbb{A}^1} \cong \widehat{R}_{\mathbb{A}^1}/t\widehat{R}_{\mathbb{A}^1}, \quad \overline{R}_\infty \cong \widehat{R}_\infty/t\widehat{R}_\infty, \quad \text{and} \quad \overline{R}_\wp \cong \widehat{R}_\wp/t\widehat{R}_\wp.$$

But we may compute that $\overline{R}_{\mathbb{A}^1} = k[\mathbb{A}^1_k]$, $\overline{R}_\infty = \widehat{\mathscr{O}_{\mathbb{P}^1_{k,\infty}}}$, and $\overline{R}_\wp = \operatorname{frac}(\widehat{\mathscr{O}_{\mathbb{P}^1_{k,\infty}}})$. Writing x for the coordinate function on the affine part of the k-line, we may explicitly identify

$$\overline{R}_{\mathbb{A}^1} = k[x], \quad \overline{R}_\infty = k[[x^{-1}]], \quad \text{and} \quad \overline{R}_\wp = k((x^{-1})),$$

and the result follows. □

4 Local–Global Principles, Factorization, and Patching

Let $\widehat{X} \to \mathbb{P}^1$ be a model for X/K, and let G be an algebraic group defined over F.

4.1 Local–Global Principles for Rational Points

Definition 4.1.1. We say that *factorization holds for G*, with respect to $\widehat{X}$, if for every tuple $(g_\wp)_{\wp \in \mathscr{B}(\widehat{X})}$, there exist collections of elements g_P for each $P \in S(\widehat{X})$ and g_U for each $U \in \mathscr{U}(\widehat{X})$ such that whenever $\wp$ is a branch at P on U we have

$$g_\wp = g_P g_U$$

with respect to the natural embeddings $F_P, F_U \to F_\wp$.

Definition 4.1.2. We say that *the local-global principle holds* for an F-scheme V, with respect to a model $\widehat{X}$ if $V(F) \neq \emptyset$ holds if and only if $V(F_P), V(F_U) \neq \emptyset$ for every $P \in S(\widehat{X})$ and $U \in \mathscr{U}(\widehat{X})$.

Definition 4.1.3. Let G be an algebraic group over F and H a scheme over F. We say that H is a *transitive* G-scheme if G acts transitively on H (see Definition 2.2.3).

Proposition 4.1.4. *If factorization holds for a group G, then the local–global principle holds for all transitive schemes over G.*

Proof. We essentially follow the proof of Theorem 3.7 in [HHK09]. Suppose have a group G such that factorization holds for G, and a transitive G-scheme H. Suppose we are given points $x_P \in H(F_P)$ and $x_U \in H(F_U)$ for all P and U. We will show that $H(F) \neq \emptyset$.

By transitivity of the action, whenever $\wp$ is a branch at P on U, we may find an element $g_\wp \in G(F_\wp)$ such that $g_\wp(x_P)_{F_\wp} = (x_U)_{F_\wp}$. By hypotheses, we may find elements $g_P \in G(F_P)$ and $g_U \in G(F_U)$ for every P and U such that $g_\wp = g_P g_U$ whenever $\wp$ is a branch at P on U. In particular, by replacing x_P by $g_P^{-1} x_P$ and x_U by $g_U x_U$, we may assume that our points satisfy $(x_P)_{F_\wp} = (x_U)_{F_\wp}$.

Now, consider these points as morphisms

$$x_P : \operatorname{Spec}(F_P) \to H, \quad x_U : \operatorname{Spec}(F_U) \to H, \quad x_\wp : \operatorname{Spec}(F_\wp) \to H$$

where $x_\wp$ is the composition of either x_P or x_U with the respective maps $\operatorname{Spec}(F_\wp) \to \operatorname{Spec}(F_P), \operatorname{Spec}(F_U)$. We claim that the scheme theoretic image of these maps consists of the same point in H, for all P, U, and $\wp$. To see this, note that if $\wp$ is a branch at P on U, then the commutativity of the diagram

$$\begin{tikzcd}
 & \operatorname{Spec}(F_P) \arrow[dr, "x_P"] & \\
\operatorname{Spec}(F_\wp) \arrow[ur] \arrow[rr, "x_\wp"] \arrow[dr] & & H \\
 & \operatorname{Spec}(F_U) \arrow[ur, "x_U"'] &
\end{tikzcd}$$

shows that the image of each of the morphisms $x_U, x_P, x_\wp$ are the same. But since the closed fiber $\widehat{X}_k^{\mathrm{red}}$ is connected, it follows that we may inductively show the image of all the morphisms corresponding to points, components or branches must coincide. Let κ be the residue field of this image point $h \in H$. Then we have field maps

$$\begin{tikzcd}
 & F_P \arrow[dl] & \\
F_\wp & & \kappa \arrow[ul] \arrow[dl] \\
 & F_U \arrow[ul] &
\end{tikzcd}$$

Using Lemma 3.4.2, we find that we obtain a map $\kappa \to F$ which one may check must be a homomorphism of fields. Therefore, we obtain a morphism $\operatorname{Spec}(F) \to H$ mapping onto the point h and so $H(F) \neq \emptyset$ as desired. $\square$

4.2 Local–Global Principles for Algebraic Objects and Torsors

Definition 4.2.1. We say that *the local–global principle holds for an algebraic object A* (of some given type) if for any algebraic object B (of the same type), we have $A \cong B$ if and only if $A_{F_P} \cong B_{F_P}$ and $A_{F_U} \cong B_{F_U}$ for all P and U. We say that the local–global principle holds for a particular type of algebraic object if it holds for all algebraic objects of this type.

Proposition 4.2.2. *The local–global principle holds for an algebraic object A' if and only for every patching problem (A,ϕ) of algebraic objects such that $A_P \cong (A')_{F_P}$ and $A_U \cong (A')_{F_U}$ for all P and U, the isomorphism class of (A,ϕ) is independent of ϕ.*

Proof. Suppose that the local–global principle holds for A', and let $(A,\phi),(A,\psi)$ be two patching problems, such that $A_P \cong (A')_{F_P}$ and $A_U \cong (A')_{F_U}$ for each P,U. Since we may patch algebraic objects, we may find algebraic objects B_1,B_2 over F whose patching problems are equivalent to $(A,\phi),(A,\psi)$, respectively. Since $(B_1)_{F_U} \cong A_{F_U} \cong (B_2)_{F_U}$ and similarly for F_P, we find that by the local–global principle, $B_1 \cong B_2$. Therefore their associated patching problems are isomorphic, implying $(A,\phi) \cong (A,\psi)$ as desired.

Conversely, suppose that (A,ϕ)'s isomorphism class is independent of ϕ for every patching problem. Suppose we are given A',B' be algebraic objects over F with associated patching problems (A,ϕ) and (B,ψ) respectively. Suppose further that $(A')_{F_U} \cong (B')_{F_U}$ and similarly for F_P. Since $A_U \cong (A')_{F_U} \cong (B')_{F_U} \cong B_U$ and $A_P \cong (A')_{F_P} \cong (B')_{F_P} \cong B_P$ for all U,P by definition, we may change ψ via these isomorphisms to find $(B,\psi) \cong (A,\psi')$ for some ψ'. But therefore by hypothesis, $(A,\phi) \cong (A,\psi') \cong (B,\psi)$. Since patching gives an equivalence of categories, we further conclude $A' \cong B'$, completing the proof. □

Remark 4.2.3. Let $\mathscr{T}$ be a type of algebraic object, and A is a particular object of type $\mathscr{T}$. Let $\mathscr{T}_A$ denote the subclass of objects that are isomorphic to A (more precisely, $\mathscr{T}_A$ is the sub-pseudofunctor of $\mathscr{T}$ that associates to every field extension L/F the category of algebraic objects of type $\mathscr{T}$ over L that are isomorphic to the object A_L). Then $\mathscr{T}_A$ satisfies the hypotheses of patching – i.e., we have an equivalence of categories between the category $\mathscr{P}\mathscr{P}_{\mathscr{T}_A}(\widehat{X})$ and $\mathscr{T}_A(F)$ – if and only if the local–global principle holds for A. Note that in general $\mathscr{T}_A$ is not a "type of algebraic object," described by some monoidal category in the sense described above.

Definition 4.2.4. Let G be an algebraic group over F. We say that *the local–global principle holds for* G if for $\alpha \in H^1(F,G)$, with α_{F_P}, α_{F_U} trivial for each P, U, we have α trivial.

Note that since elements of $H^1(F,G)$ correspond to torsors for G, we see immediately that the local–global principle will hold for G if and only if the local–global principle holds for all G-torsors, in the sense of Definition 4.1.2. Since G-torsors are transitive G-schemes, from Proposition 4.1.4, we immediately obtain:

Proposition 4.2.5. *Suppose G is a linear algebraic group defined over F, and suppose that factorization holds for G with respect to $\widehat{X}$. Then the local global principle holds for G.*

Proposition 4.2.6. *Suppose A is an algebraic object of some type $\mathscr{T}$, whose automorphism group is the linear algebraic group G. Then the following are equivalent:*

1. *The local–global principle holds for A.*
2. *The local–global principle holds for G.*
3. *Factorization holds for G.*

Proof. Since G is the automorphism group of A, by descent (see [Ser, X.Sect. 2, Prop. 4]), we may identify $H^1(L, G_L) = \mathrm{Forms}(A_L)$, the pointed set of twisted forms of A_L. In particular, it is immediate from the definition that the local–global principle for A is equivalent to the local–global principle for G.

Suppose we have a local–global principle for A, and consider a collection of elements $g_\wp \in G(F_\wp)$. Consider the patching problem (B, ϕ) where $B_P = A_{F_P}$, $B_U = A_{F_U}$, and $\phi_\wp = g_\wp$. By the local–global principle, this is isomorphic to the patching problem $(\widetilde{A}, \mathbb{I})$. By definition, we may find an isomorphism $h : (B, \mathbb{I}) \to (B, \phi)$. Let $g_P = h_P^{-1}$ and $g_U = h_U$. By definition of a morphism of patching problems, we find that $g_\wp = g_P g_U$, and that $g_P \in Aut(B_P) = G(F_P)$ and $g_U \in Aut(B_U) = G(F_U)$ as desired.

Conversely, suppose we have factorization for G. In this case, it is immediate from Proposition 4.2.5 that the local global principle must hold for G, completing the proof. □

Remark 4.2.7. Theorem 4.2.6 raises the question of whether it would be possible to show the equivalence of the local–global principle for a group G and factorization for this group without the presence of an algebraic object with G as its automorphism group. This would give a converse to Proposition 4.2.5. In turn since G-torsors are, in particular, transitive G-schemes, one would then also obtain a converse to Proposition 4.1.4.

5 Factorization for Retract Rational Groups

5.1 Overview and Preliminaries

The goal of this section will be to prove the following theorem:

Theorem 5.1.1. *Suppose $\widehat{X}$ is a connected normal finite $\mathbb{P}^1_T$-scheme, with function field F and let G be a connected retract rational algebraic group over F. Then factorization holds for G with respect to $\widehat{X}$.*

Using this theorem, we may easily proceed to the proof of the local global principle for schemes with transitive action stated earlier in Theorem 2.2.4. If G is a connected retract rational group over F, then by the theorem, factorization holds for G with respect to $\widehat{X}$. But then by Proposition 4.1.4, the local–global principle must hold for transitive G schemes, as desired.

The proof of this theorem will occupy the remainder of the section. Our strategy will be to reduce this to a more abstract factorization problem, arising from the case when $\widehat{X} = \mathbb{P}^1_T$. Overall, the proof stategy is roughly parallel to that followed in [HHK09], where retractions of open subsets of affine space take the place of open subsets of affine space.

Definition 5.1.2. Suppose we have commutative rings $F \subset F_1, F_2 \subset F_0$, and an algebraic group G over F. We will say that *factorization holds* with respect to G, F, F_1, F_2, F_0 if for every $g_0 \in G(F_0)$ there exist $g_1 \in G(F_1)$ and $g_2 \in G(F_2)$ such that $g_0 = g_1 g_2$.

Note that here we are omitting from the notation the homomorphism $G(F_i) \to G(F_0)$ for $i = 1, 2$. Suppose $\widehat{X}$ is a connected, normal, finite $\mathbb{P}^1_T$-scheme. In this case, we set $F = F(\widehat{X})$, and we let

$$F_1 = \prod\nolimits_{P \in S(\widehat{X})} F_P, \quad F_2 = \prod\nolimits_{U \in \mathscr{U}(\widehat{X})} F_U, \quad \text{and} \quad F_0 = \prod\nolimits_{\wp \in \mathscr{B}(\widehat{X})} F_\wp.$$

Remark 5.1.3. It follows immediately from the definitions that factorization holds for the group G with respect to $\widehat{X}$ in the sense of Definition 4.1.1 if and only if factorization holds for G, F, F_1, F_2, F_0 in the sense of Definition 5.1.2 where F, F_1, F_2, F_0 are as above.

Back to the somewhat more abstract setting, suppose that F is some field, and let L be a finite dimensional commutative F-algebra. Recall that if G is a linear algebraic group scheme, we may define its Weil restriction, also referred to as its corestriction or transfer, as the linear algebraic group with the functor of points defined by:

$$\mathrm{R}_{L/F}\, G(R) = G(R \otimes_F L)$$

where R ranges through all F-algebras, see [Gro62, Exp. 195, p. 13] for the definition and Exp. 221, p. 19 of ibid. for proof of existence. We note that the corestriction in fact comes from a Weil restriction functor from the category of quasi-projective L-schemes to the category of quasi-projective F-schemes, and that this functor takes open inclusions to open inclusions, and takes affine space to affine space (of a different dimension). In particular, it follows that the corestriction of a rational (or retract rational) variety is itself rational (resp. retract rational).

We note the following lemma, which is a consequence of the definition of the corestriction in terms of the functor of points given above.

Lemma 5.1.4. *Let F be a field, and suppose we are given rings $F \subset F_1$, $F_2 \subset F_0$, and a finite dimensional commutative F-algebra L. Let G be a linear algebraic group over L. Then factorization holds for G, L, $L \otimes_F F_1$, $L \otimes_F F_2$, $L \otimes F_0$ if and only if it holds for* $\mathrm{R}_{L/F}\, G$*, F, F_1, F_2, F_0.*

Lemma 5.1.5. *Suppose that we are given a morphism of connected projective normal finite $\mathbb{P}^1_T$-schemes $f : \widehat{Y} \to \widehat{X}$. Let L be the function field of $\widehat{Y}$ and F the function field of $\widehat{X}$. Then factorization holds for $G, \widehat{Y}$ if and only if it holds for $\mathrm{R}_{L/F}\, G, \widehat{X}$.*

Proof. This follows immediately from the universal property of the Weil restriction, together with Lemma 3.4.1. □

Lemma 5.1.6. *Let F be the function field of $\mathbb{P}^1_T$. Suppose that for every connected retract rational group G over F, factorization holds for G with respect to $\mathbb{P}^1_T$ (as in Definition 4.1.1). Then for every normal finite $\mathbb{P}^1_T$-scheme $\widehat{X}$ with function field L, and every connected retract rational group H over L, factorization holds for H with respect to $\widehat{X}$.*

Proof. This follows immediately from Lemma 5.1.5. □

As a consequence of this, in order to prove Theorem 5.1.1, we may restrict to the setting where F is the function field of $\mathbb{P}^1_T$, and where $F_1 = F_\infty$, $F_2 = F_{\mathbb{A}^1_k}$, and where $F_0 = F_\wp$ is the field associated to the unique branch $\wp$ along $\mathbb{A}^1_k$ at ∞. We let $\widehat{R}_0 = \widehat{R}_\wp$, $\mathfrak{V} = \widehat{R}_\infty$, and $\mathfrak{W} = \widehat{R}_{\mathbb{A}^1_k}$. For convenience, in the sequel we will often refer to the following hypothesis for factorization.

Hypothesis 5.1.7 (see [HHK09, Hypothesis 2.4]). We assume that the complete discrete valuation ring $\widehat{R}_0$ contains a subring T which is also a complete discrete valuation ring having uniformizer t, and that F_1, F_2 are subfields of F_0 containing T. We further assume that $\mathfrak{V} \subset F_1 \cap \widehat{R}_0$, $\mathfrak{W} \subset F_2 \cap \widehat{R}_0$ are t-adically complete T-submodules satisfying $\mathfrak{V} + \mathfrak{W} = \widehat{R}_0$.

Lemma 5.1.8. *With respect to the scheme $\mathbb{P}^1_T$ consider $F = F(\mathbb{P}^1_T)$, $F_0 = F_\wp$, $F_1 = F_\infty$, $F_2 = F_{\mathbb{A}^1_k}$, $\widehat{R}_0 = \widehat{R}_\wp$, $\mathfrak{V} = \widehat{R}_\infty, \mathfrak{W} = \widehat{R}_{\mathbb{A}^1_k}$. Then these rings and modules satisfy the Hypothesis 5.1.7.*

Proof. The completeness of $\mathfrak{V}, \mathfrak{W}$ is satisfied by definition. The fact that $\mathfrak{V} + \mathfrak{W} = \widehat{R}_0$ follows from Lemma 3.4.4. □

5.2 Retractions: Basic Definitions and Properties

Before attacking the problem of factorization directly, it is necessary to collect some facts concerning retractions and retract rational varieties. Retract rational varieties were introduced by Saltman in [ASS].

Definition 5.2.1. We say that a variety Y is a *retraction* of a variety U if there exist morphisms $i : Y \to U$ and $p : U \to Y$ such that $pi = id_Y$. We say that it is a *closed retraction* if i is a closed embedding.

Remark 5.2.2. In the case of a closed retraction, we will occasionally abuse notation by simply regarding i as an inclusion.

Definition 5.2.3. We say that Y is a *rational retraction* of U if there are rational maps $i : Y \dashrightarrow U$ and $p : U \dashrightarrow Y$ such that $pi = id_Y$ on some open set on which pi is defined.

Definition 5.2.4. We say a variety Y is *retract rational* if it is a rational retraction of $\mathbb{A}^n$ for some n.

In [Sal], the property of a variety being retract rational was reinterpreted in terms of lifting of torsors. Our methodology goes in a (a priori) different direction, focusing on the local geometry of retract rational varieties from the point of view of adic topologies.

Lemma 5.2.5 (Rational retractions shrink to retractions). *Suppose Y is a rational retraction of U via rational maps i, p. Then we may find dense open subsets $Y_0 \subset Y$ and $U_0 \subset U$ such that i, p make Y_0 a retraction of U_0.*

Proof. We may find open subsets $\widetilde{Y} \subset Y$ and $\widetilde{U} \subset U$ such that i, p restrict to morphisms on these sets, i.e., we have:

$$\begin{tikzcd} Y \arrow[r, dashed] & U \arrow[r, dashed] & Y \\ \widetilde{Y} \arrow[u] \arrow[ur, "i"] & \widetilde{U} \arrow[u] \arrow[ur, "p"] & \widetilde{Y} \arrow[u] \end{tikzcd}$$

We choose $Y' = i^{-1}p^{-1}\widetilde{Y} \subset \widetilde{Y}$. We note that the hypothesis implies that p is dominant, and that the image of the generic point of Y under i lies in $\tilde{U}$, from which one then concludes that Y' is not empty. As pi is defined on Y', by definition we may find $Y_0 \subset Y'$ such that $pi|_{Y_0} = id_{Y_0}$. Let $U_0 = p^{-1}(Y_0)$. Then we have $pi(Y_0) \subset Y_0$ and so $i(Y_0) \subset p^{-1}(Y_0) = U$. Since $p(U_0) \subset Y_0$ by definition, we have constructed the desired morphisms. □

Lemma 5.2.6 (Retractions shrink to closed retractions). *Suppose Y is a retraction of U via morphisms i, p. Then we may find dense open subvarieties $Y_0 \subset Y$ and $U_0 \subset U$ such that Y_0 is a closed retraction of U_0 via the restrictions of i, p.*

Proof. Since we may identify Y with the image of i, it follows that Y is locally constructible in U [EGA 4-1, p. 239 (Chevalley's theorem)]. By [EGA 3-1, p. 12], it follows that Y is the intersection of a closed and an open set in U. By setting U_0 to be this open set, and $Y_0 = Y \cap U_0$ it follows that Y_0 is closed in U_0. Now it is easy to see that the restrictions of i, p exhibit Y_0 as a retraction of U_0. □

Corollary 5.2.7 (Rational retractions shrink to closed retractions). *Suppose Y is a rational retraction of U via rational maps i, p. Then we may find dense open subsets $Y_0 \subset Y$ and $U_0 \subset U$ such that i, p make Y_0 a closed retraction of U_0.*

Proof. This follows immediately from Lemmas 5.2.5 and 5.2.6. □

The following lemma gives us a first hint that retractions inherit some of the geometry of the larger spaces.

Lemma 5.2.8 (Retractions of smooth schemes are smooth). *Suppose Y is a retraction of a smooth scheme U. Then Y is smooth.*

Proof. This follows from the formal criterion for smoothness (see for example [EGA, Sect. 17] or [Ill, Sect. 2]). From this formulation, in the language of [Ill], we must show that if $S_0 \to S$ is a thickening, and $f : S_0 \to Y$ is a morphism, then we must be able to find a cover $\{V_i\}$ of S and morphisms $g_i : V_i \to Y$ extending $f|_{S_0 \cap V_i}$. To see this, we first use the smoothness of U to find $\widetilde{g}_i : V_i \to U$ extending $i \circ f|_{S_0 \cap V_i}$. Now we set $g_i = p \circ \widetilde{g}_i$. We then have

$$g_i|_{S_0 \cap V_i} = p \circ \widetilde{g}_i|_{S_0 \cap V_i} = p \circ i \circ f|_{S_0 \cap V_i} = f|_{S_0 \cap V_i}$$

as desired. □

Lemma 5.2.9 (Standard position for retractions). *Suppose Y is a d-dimensional variety which is a closed retraction of an open subscheme $U \subset \mathbb{A}^n$. We also suppose that 0 is in Y (with respect to the inclusion of Y in $\mathbb{A}^n$). Then we may shrink U and choose coordinates on U so that Y smooth and is the zero locus of polynomials $f_1, \ldots, f_{n-d}$ with*

$$f_i = x_i + P_i$$

where the x_i's are the coordinate functions on $\mathbb{A}^n$ and P_i is a polynomial in the x_j's, each of whose terms are of degree at least 2.

Further, we may alter i and p defining the retraction so that the morphism ip : $U \to Y \to U$ is given by

$$(x_1, \ldots, x_n) \mapsto (M_1 + Q_1, \ldots, M_n + Q_n)$$

where

$$M_i = \begin{cases} 0 & \text{if } 1 \le i \le n-d \\ x_i & \text{if } n-d < i \le n \end{cases}$$

and Q_i is a rational function in the variables x_i, regular on U, such that $\frac{\partial}{\partial x_j} Q_i \Big|_0 = 0$ for all i, j.

Proof. For purposes of skimmability, we have placed this proof at the end of the section. □

5.3 Adic Convergence of Taylor Series

The basic strategy for factorization will be to produce closer and closer approximations to a particular factorization. In order to carry this out, it is necessary to discuss notions of convergence and approximations in the adic setting, paralleling the discussion of [HHK09, Sect. 2].

Suppose F_0 is a field complete with respect to a discrete valuation v with uniformizer t, and let $|a| = e^{-v(a)}$ be a corresponding norm. Let $A = F_0[x_1, \ldots, x_N]$, $\mathfrak{m}$

the maximal ideal at 0, $A_{\mathfrak{m}}$ the local ring at 0 and $\widehat{A} = F_0[[x_1,\dots,x_N]]$ the complete local ring at 0. For $I = (i_1,\dots,i_N) \in \mathbb{N}^N$, we let $|I| = \sum_j i_j$. Define for $r \in \mathbb{R}$, $r > 0$

$$\widehat{A}_r = \left\{ \sum_I a_I x^I \;\middle|\; \lim_{|I|\to\infty} |a_I| r^{|I|} = 0 \right\}$$

and for $f = \sum a_I x^I \in \widehat{A}_r$, we set

$$|f|_r = \sup_I |a_I| r^{|I|}.$$

We give $\mathbb{A}^n(F_0)$ a norm via the supremum of the coordinates

$$|(a_1,\dots,a_N)| = \max_i \{|a_i|\}$$

and we let $D(a,r)$ be the closed disk of radius r about $a \in \mathbb{A}^n(F_0)$ with respect to the induced metric. We note that since the values of the metric are discrete, this disk is in fact both open and closed in the t-adic topology.

We note the following elementary lemma:

Lemma 5.3.1. *Suppose $a \in D(0,r)$, and $f,g \in \widehat{A}_r$. Then:*

1. $f+g, fg \in \widehat{A}_r$.
2. $|f+g|_r \le \max\{|f|_r, |g|_r\}$.
3. *For every real number $M > 0$, the group*

$$\{f \in \widehat{A}_r \mid |f|_r < M\} \subset \widehat{A}_r$$

is complete with respect to the filtered collection of subgroups $\mathfrak{m}^i \cap \widehat{A}_r$.

4. $|f|_r$ *is finite.*
5. $|fg|_r \le |f|_r |g|_r$.
6. *if $r' < r$, then $|f|_{r'} \le \max\{|f(0)|, \frac{r'}{r}|f|_r\}$.*
7. *$f(a)$ is well defined (i.e. is a convergent series).*
8. *$|f(a)| \le |f|_r$, and if $f(0) = 0$ then $|f(a)| \le |f|_r |a| r^{-1}$.*

Lemma 5.3.2. *Suppose f is in $A_{\mathfrak{m}}$. Then for all $\varepsilon \ge |f(0)|$ with $\varepsilon > 0$, there exists $r > 0$ such that $f \in \widehat{A}_r$ and $|f|_r < \varepsilon$. Further, for any $\delta > 0$ we may choose $r < \delta$.*

Proof. Write $f = g/h$, $g,h \in A$ with $h \notin \mathfrak{m}$. Since $A/\mathfrak{m}$ is a field, we may find $h' \in A$ with $hh' - 1 = -b \in \mathfrak{m}$. Therefore, in $\widehat{A}$, we have $f = gh'(\sum b^i)$. Since g, h', b are polynomials, they are in A_r for any r. Further, by Lemma 5.3.1(6), we may reduce r so that $|gh'|_r \le |f(0)|$, and since $b(0) = 0$, we may also ensure $|b|_r < 1$. In doing this, note that we may also ensure that $r < \delta$. We note that by Lemma 5.3.1(5), $|b^i|_r < 1$. Now, by Lemma 5.3.1(3), it follows that $|\sum b^i|_r < 1$. Therefore, $|f|_r = |gh' \sum b^i|_r < \varepsilon$ as desired. □

Lemma 5.3.3. *The t-adic topology on $\mathbb{A}^N(F_0)$ is finer than the Zariski topology.*

Proof. It suffices to show that if $p \in \mathbb{A}^N(F_0)$ and f is a polynomial not vanishing on p, we may find a disk about p on which f is nonvanishing. Without loss of generality, we may apply a translation and assume that $p = 0$. Let $g = f - f(0)$. By Lemma 5.3.2, since $g(0) = 0$, we may find an $r > 0$ such that $f \in \widehat{A}_r$ and such that $|g|_r < |f(0)|$ (using $\varepsilon = |f(0)|$). In particular, if $a \in \mathbb{A}^N(F_0)$ with $|a| < r$, we have $|g(a)| \leq |g|_r < |f(0)|$ by Lemma 5.3.1(8). Therefore, for such an a, $f(a) = g(a) + f(0) \neq 0$. Therefore, f does not vanish on a disk of radius r about the origin as desired. □

Proposition 5.3.4 (Linear approximations and error term). *Suppose $f \in \widehat{A}_r$ for $r \leq 1$. Write*

$$f = c_0 + L + P, \text{ where } P(\mathbf{x}) = \sum_{|\nu| \geq 2} c_\nu x^\nu,$$

and L is a linear form with coefficients in F_0 and all $c_\nu \in F_0$. Suppose $|L+P|_r \leq 1$. Let $0 < \varepsilon \leq |t|r^2$, and suppose $a, h \in \mathbb{A}^N(F_0)$ with $|h|, |a| \leq \varepsilon$. Then

$$|f(a+h) - f(a) - L(h)| \leq |t||h|.$$

Proof. This proof is a very slight modification of Lemma 2.2 in [HHK09]. Choose a real number s so that we may write $|h| = \varepsilon|t|^s$. We may rearrange the quantity of interest as:

$$f(a+h) - f(a) - L(h) = \sum_{|\nu| \geq 2} c_\nu \left((a+h)^\nu - a^\nu \right).$$

Since the absolute value is nonarchimedean, it suffices to show that for every term $m = c_\nu x^\nu$ with $|\nu| \geq 2$ we have

$$|m(a+h) - m(a)| \leq \varepsilon |t|^{s+1}.$$

For a given ν with $|\nu| \geq 2$, view the expression $(x+x')^\nu - x^\nu$ as a homogeneous element of degree $j = |\nu|$ in the polynomial ring $F_0[x_1, \ldots, x_N, x'_1, \ldots, x'_N]$. Since the terms of degree j in $x_1, \ldots, x_N$ cancel, the result is a sum of terms of the form $\lambda\ell$ where λ is an integer and ℓ is a monomial in the variables x, x' with total degree d in $x_1, \ldots, x_N$ and total degree d' in $x'_1, \ldots, x'_N$, such that $d + d' = j$ and $d < j$. Hence $d' \geq 1$. Consequently, for each term of this form,

$$|\lambda\ell(a,h)| \leq |\ell(a,h)| \leq \varepsilon^d (\varepsilon|t|^s)^{d'} = \varepsilon^j |t|^{sd'} \leq \varepsilon^j |t|^s.$$

Since $(a+h)^\nu - a^\nu$ is a sum of such terms, and the norm is nonarchimedean, we conclude $|(a+h)^\nu - a^\nu| \leq \varepsilon^j |t|^s$.

Since $m = c_\nu x^\nu$, it follows that

$$|m(a+h) - m(a)| \leq |c_\nu| \varepsilon^j |t|^s \leq r^{-j} \varepsilon^j |t|^s.$$

Now $\varepsilon \leq |t|r^2$, so $\varepsilon^{j-1} \leq |t|^{j-1} r^{2j-2}$. Since $|t| < 1$, $r \leq 1$, and $j \geq 2$, we have

$$\varepsilon^{j-1} \leq |t|^{j-1} r^{j+j-2} \leq |t| r^j.$$

Rearranging this gives the inequality $(\varepsilon/r)^j \leq \varepsilon|t|$ and so $(\varepsilon/r)^j|t|^s \leq \varepsilon|t|^{s+1}$. Therefore

$$|m(a+h)-m(a)| \leq r^{-j}\varepsilon^j|t|^s \leq \varepsilon|t|^{s+1} = |t||h|,$$

as desired. $\square$

Lemma 5.3.5 (Local bijectivity / inverse function theorem). *Suppose $f: U \to V$ is a morphism between Zariski-open subschemes of $\mathbb{A}^d_{F_0}$ containing the origin and such that $f(0)=0$. Suppose further, that after writing the coordinates of f as power series in $\widehat{A}$, we have $f=(f_1,\dots,f_d)$ with $f_i = x_i + Q_i$ and Q_i consisting of terms of degree at least 2. Then we may find t-adic neighborhoods $U' \subset U(F_0)$ and $V' \subset V(F_0)$ of 0 such that f maps U' bijectively onto V'. Further, we may assume that U' and V' are disks about the origin of equal radii.*

Proof. By Lemma 5.3.2, since $f(0)=0$, we may find $0<r\leq 1$ such that $f \in \widehat{A}_r$ and $|f|_r \leq 1$. Choose $\varepsilon \leq |t|r^2$ as in the statement of Proposition 5.3.4 and such that $D_0(\varepsilon) \subset V(F_0)$ and $D_0(\varepsilon) \subset U(F_0)$. Let $V' = D_0(\varepsilon) \subset V(F_0)$ and $U' = D_0(\varepsilon) \subset U(F_0)$. We claim that for $b \in U'$, we have $|f(b)| \leq \varepsilon$ and so $f(b) \in V'$. To see this, we note that $Q_i \in \widehat{A}_r$ and $|Q_i|_r \leq 1$, and hence we may apply Proposition 5.3.4 (with 0 linear and constant term) to see that $|Q_i(b)| \leq |t||b| < |b| = \max\{|b_i|\}$. By the nonarchimedean property, this gives

$$\begin{aligned}|f(b)| = \max\{|f_i(b)|\} = \max\{|b_i + Q_i(b)|\} \leq \max\{|b_i|, |Q_i(b)|\}\\ = \max\{|b_j|\} = |b|.\end{aligned}$$

We consider first surjectivity. Note that both U' and V' are both closed and open. Since they are closed in a complete metric space, they contain all limits of their Cauchy sequences. Let $a \in V'$, and let $b_0 = 0$. We will inductively construct elements $b_i \in U'$ such that $|f(b_i)-a| \leq \varepsilon|t|^i$. In particular, since $|a| \leq \varepsilon$, we have $|f(b_0)-a| = |a| \leq \varepsilon$. Assuming we have constructed b_{i-1}, we let $h = a - f(b_{i-1})$, and note $|h| \leq \varepsilon|t|^{i-1}$ by hypothesis, and $|b_{i-1}| \leq \varepsilon$ since $b_{i-1} \in U'$. Therefore, by Proposition 5.3.4, we have

$$|f(b_{i-1}+h) - f(b_{i-1}) - h| \leq |t|\,|h| \leq \varepsilon|t|^i.$$

By setting $b_i = b_{i-1}+h$, we find that, since $f(b_{i-1})+h = a$, we have

$$|f(b_i)-a| = |f(b_{i-1}+h)-a| = |f(b_{i-1}+h) - f(b_{i-1}) - h| \leq |t|\,|h| \leq \varepsilon|t|^i$$

as desired. Since b_i is a Cauchy sequence, using the completeness of U', we may set $b = \lim b_i \in U'$ and we find by continuity that $f(b) = a$ as desired.

Next, we consider injectivity. Suppose $a,b \in U'$, let $h = b-a$ and suppose $h \neq 0$. We need to show that $f(a) \neq f(b)$. Since the valuation is nonarchimedean, we have $a,h \leq \varepsilon$. Let $E = f(a+h) - f(a) - h$. Then we find $|E| \leq |h||t|$ by Proposition 5.3.4. But this means in particular that $|E+h| = |h|$ by the nonarchimedean triangle inequality. Therefore

$$|f(b) - f(a)| = |f(a+h) - f(a)| = |E + h| = |h| \neq 0$$

so $f(b) \neq f(a)$ as desired. $\square$

Lemma 5.3.6. *Suppose that Y is a d-dimensional variety which is a closed retraction of an open subscheme $U \subset \mathbb{A}^n$ in the standard form of Lemma 5.2.9 with respect to morphisms i, p. Then we may find a t-adic neighborhood V' of $0 \in Y$ (regarding Y as a subscheme of U via i) such that the composition $V' \to \mathbb{A}^n(F_0) \to \mathbb{A}^d(F_0)$ is bijective onto a t-adic disk, where the last map is given by projection onto the last d coordinates.*

Proof. As in Lemma 5.2.9, we suppose that Y is the zero locus of polynomials $f_1, \ldots, f_{n-d}$ with

$$f_i = x_i + P_i$$

where P_i is a polynomial in the x_j's each of whose terms are of degree at least 2. Using Lemma 5.3.2, we may choose $0 < r \leq 1$ such that $f_i \in \widehat{A}_r$ and $|f_i|_r \leq 1$ for each of the finitely many functions f_i. Choose $\varepsilon \leq |t|r^2$ as in Proposition 5.3.4. Let $g : U \to \mathbb{A}^d$ the projection onto the last d coordinates. Let $U' \in \mathbb{A}^d(F_0)$ be the disk about the origin of radius ε. Let V' be the intersection of $g^{-1}U'$ with $Y(F_0)$.

Suppose $a \in V'$ and $b \in U'$ with $a \neq b$ and $g(a) = g(b)$. We claim that $b \notin V'$. In particular, this would imply that $g|_{V'}$ is injective. To see that b is not in V', first let $h = b - a$. If $g(a) = g(b)$, then by definition of g, the last d coordinates of a and b must match. Since $a \neq b$, we therefore know that $x_i(h) \neq 0$ for some $i = 1, \ldots, n-d$ where x_i is the ith coordinate function on $\mathbb{A}^d$. We may therefore choose i such that $|x_i(h)|$ has the largest possible value, and in particular, we then would have $|x_i(h)| = |h|$. But, estimating $|f_i(b) - f_i(a)| = |f_i(a+h) - f_i(a)|$ using Proposition 5.3.4, we find

$$|f_i(a+h) - f_i(a) - x_i(h)| \leq |t||h|.$$

We claim that $|f_i(a+h) - f_i(a)| \geq |h|$ and in particular that $f_i(a) \neq f_i(b)$. To see this must hold, assume by contradiction that $|f_i(a+h) - f_i(a)| < |h|$. In this case, we have

$$|f_i(a+h) - f_i(a) - x_i(h)| = |x_i(h)|$$

since $|x_i(h)| = |h|$. Therefore we have $|h| \leq |t||h|$ which is a contradiction since $|t| < 1$. Therefore, $f_i(b) \neq f_i(a)$. Since V' lies in the zero locus of the functions f_i, we have $f_i(a) = 0 \neq f_i(b)$, and so $b \notin V'$ as claimed. Therefore, $g|_{V'}$ is injective.

By construction, $g|_{V'}$ has image entirely in the ball of radius ε in $\mathbb{A}^d(F_0)$ about the origin. We claim that it in fact surjects onto this ball (possibly after shrinking ε). For this, let $a \in U'$, and consider its image $b = g(a) \in \mathbb{A}^d(F_0)$. Using the form for the retraction in Lemma 5.2.9, we may apply Lemma 5.3.5 to the composition (shrinking ε if necessary)

$$\begin{tikzcd} \mathbb{A}^d \cap U \arrow[r] & U \arrow[r, "p"] & Y \arrow[r] \arrow[rr, bend left, "g|_Y"] & U \arrow[r, "g"'] & \mathbb{A}^d \end{tikzcd}$$

By Lemma 5.3.5, we may find an inverse image b' of b in $\mathbb{A}^d$ of norm less than ε. Consequently, by definition, the image of b' in Y must actually live in V', and this is an inverse image for a as desired. □

Corollary 5.3.7. *In the notation of the previous lemma, we may choose t-adic neighborhoods of the origin $U' \in \mathbb{A}^d$ and $V' \in Y$ such that the composition $U' \to U \to Y$ takes U' bijectively to V' and the composition $V' \to Y \to U \to \mathbb{A}^n \to \mathbb{A}^d$ takes V' bijectively to U'.*

Proof. By Proposition 5.2.9 and Lemma 5.3.5, we may find $U' \subset \mathbb{A}^d$, $V' \subset Y$ so that the composition $U' \to V' \to U'$ is bijective. By Lemma 5.3.6, we may find $V'' \subset V'$ such that $V'' \to U'$ in bijective onto a t-adic disk $U'' \subset U'$. But now again the composition $U'' \to U''$ is bijective, and since $V'' \to U''$ is also bijective, we find $U'' \to V''$ is bijective as well. □

5.4 Factorization

Theorem 5.4.1. *Under Hypothesis 5.1.7, let $f\colon \mathbb{A}^d_{F_0} \times \mathbb{A}^d_{F_0} \dashrightarrow \mathbb{A}^d_{F_0}$ be an F_0-rational map that is defined on a Zariski-open set $U \subseteq \mathbb{A}^d_{F_0} \times \mathbb{A}^d_{F_0}$ containing the origin $(0,0)$. Suppose further that we may write:*

$$f = (f_1, \dots, f_d) \text{ and } f_i \in \widehat{k}[x_1, y_1 \dots, x_d y_d]_{\mathfrak{m}} \text{ where } f_i = x_i + y_i + \sum_{|(\nu,\rho)| \geq 2} c_{\nu,\rho,i} x^\nu y^\rho.$$

Then there is a real number $\varepsilon > 0$ such that for all $a \in \mathbb{A}^d(F_0)$ with $|a| \leq \varepsilon$, there exist $v \in \mathfrak{V}^d$ and $w \in \mathfrak{W}^d$ such that $(v,w) \in U(F_0)$ and $f(v,w) = a$.

Proof. The proof of this theorem is exactly as for Theorem 2.5 in [HHK09], wherein in the first paragraph, the problem is reduced to exactly the hypotheses which we assume. □

Theorem 5.4.2. *Assume Hypothesis 5.1.7. Let $m : Y \times Y \to Y$ be a rational F-morphism defined at $(0,0)$, and suppose that $m(y,0) = y = m(0,y)$ where it is defined. Suppose that Y is a closed retraction of an open subscheme of $\mathbb{A}^n$. Then there exists $\varepsilon > 0$ such that for $y \in Y(F_0) \subset \mathbb{A}^n(F_0)$, $|y| \leq \varepsilon$, there exist $y_i \in Y(F_i)$, $i = 1,2$ such that $y = m(y_1, y_2)$.*

Proof. We consider as in Corollary 5.3.7, t-adic neighborhoods of 0 $U' \subset \mathbb{A}^d(F_0)$ and $V' \subset Y(F_0)$ such that we have bijections $U' \to V'$ and $V' \to U'$ defined by algebraic rational morphisms $p' : \mathbb{A}^d \dashrightarrow Y$ and $i' : Y \dashrightarrow \mathbb{A}^d$. We consider

$$\begin{tikzcd} V' \times V' \arrow[r, "m|_{V' \times V'}"] & V' \arrow[d, "i'"] \\ U' \times U' \arrow[u, "p'"] \arrow[r] & U' \end{tikzcd}$$

By hypothesis, the composition in the bottom $U' \times U' \to U'$ is given as the restriction of an algebraic rational morphism $\mu : \mathbb{A}^d \times \mathbb{A}^d \to \mathbb{A}^d$. By Corollary 5.3.7, it is sufficient to show that μ is surjective when restricted to a sufficiently small t-adic neighborhood.

We first shrink V', U' if necessary to make them contained in Zariski neighborhoods V, U as in Lemma 5.2.9. Now, we note that the rational map $\mu|_{\mathbb{A}^d \times \{0\}}$ is just ip, since $m|_{Y \times \{0\}} = id_Y$. By Lemma 5.2.9, we find

$$m|_{\mathbb{A}^d \times \{0\}}(x_1, \ldots, x_d) = (x_1 + Q_1, \ldots, x_d + Q_d)$$

where Q_i is a rational function in the variables x_i, regular on U, such that $\frac{\partial}{\partial x_j} Q_i \Big|_0 = 0$ for all i, j. But now we are done, using Theorem 5.4.1. □

Theorem 5.4.3 (Factorization for retract rational groups). *Under Hypothesis 5.1.7, assume that $F = F(\mathbb{P}^1_T)$, $F_1 = F_{\mathbb{A}^1_k}$, $F_2 = F_\infty$, and $F_0 = F_\wp$, where $\wp$ is the unique branch at ∞. Let G be a retract rational connected linear algebraic group defined over F. Then for any $g_0 \in G(F_0)$ there exist $g_i \in G(F_i)$, $i = 1, 2$, such that $g_1 g_2 = g_0$. That is to say, factorization holds for G with respect to $\mathbb{P}^1_T$ (see Definition 4.1.1).*

Proof. Using Lemma 5.2.6, we may find an open subscheme $Y \subset G$ that is a retraction of an open subscheme U of affine space. In particular, Y must contain an F-rational point $y \in Y(F)$, and after replacing Y by $y^{-1}Y$ if necessary, we may assume Y contains the identity element of G. Using 5.4.2, where m is the multiplication map, we find that there exists $\varepsilon > 0$ such that factorization holds for $g_0 \in G(F_0)$ provided that $|g_0| < \varepsilon$. Fix such an epsilon, and suppose $g_0 \in G(F_0)$ is an arbitrary element. Since G is retract rational, it follows that $G(F)$ is Zariski dense in $G(F_0)$. Therefore, we have the existence of an element $g' \in G(F)$ such that ${g'}^{-1} g_0 \in Y$. Since Y is a retraction of affine space, it follows that $Y(F_2)$ is t-adically dense in $Y(F_0)$. Therefore, we may find $g'' \in Y(F_2)$ such that $|{g'}^{-1} g_0 {g''}^{-1}| < \varepsilon$. Writing ${g'}^{-1} g_0 {g''}^{-1} = g_1 g_2$ where $g_i \in G(F_i)$, we conclude that $g_0 = (g' g_1)(g_2 g'')$. Since $g' g_1 \in G(F_1)$ and $g_2 g'' \in G(F_2)$, we are done. □

By Lemma 5.1.5 and the comments just following, we conclude that Theorem 5.1.1 holds.

5.5 *Proof of Lemma 5.2.9*

Lemma 5.5.1. *Suppose $f = g/h$ for $g, h \in k[x_1, \ldots, x_n]$ with $h(0) \neq 0$, $g(0) = 0$, and $(\partial f / \partial x_i)|_0 = 0$ for all i. Then if R is a k-algebra with $h(0) \in R^*$ and containing an element $\varepsilon \in R$, $\varepsilon^2 = 0$ then $f(\varepsilon v) = 0$ for $v \in k^n$.*

Proof. Since $g(0) = 0$, we may write $g = L + Q$ where L is a linear polynomial, and Q is a sum of homogeneous terms of degree at least 2. Now we simply note that

$$\frac{\partial f}{\partial x_i} = \frac{h(\partial L/\partial x_i + \partial Q/\partial x_i) - (L+Q)(\partial h/\partial x_i)}{h^2}.$$

In particular, since $h(0)$ is not zero, $(\partial f/\partial x_i)|_0 = 0$ implies that $h(0)(\partial L/\partial x_i(0)) = 0$, which implies that all the coefficients of the linear form L are 0 and so $L = 0$. Since $h(0) \neq 0$, it follows that $h(\varepsilon v)$ is a unit, and we therefore may note that $f(\varepsilon v) = Q(\varepsilon v)/h(\varepsilon v)$ is well defined and $\varepsilon^2 = 0$ implies $Q(\varepsilon v) = 0$, showing that $f(\varepsilon v) = 0$ as desired. □

We now proceed with the proof of Lemma 5.2.9. By Lemma 5.2.8, we may assume that Y is smooth. Choose $f_1, \dots, f_r$ which are regular on a neighborhood of $0 \in U$ and which cut out Y. Writing $f_i = g_i/h_i$, for g_i and h_i with no common factors, we see that since the h_i don't vanish at 0, after shrinking U so that the h_i don't vanish on U, we may ensure that the h_i are units, and hence Y is cut out by the g_i. Therefore, we may assume (after replacing f_i by g_i and shrinking U) that the f_i are polynomials. Next, we write

$$f_i = L_i + P_i$$

where L_i is a linear polynomial and P_i has degree at least 2. Note that f_i has no constant term since it must vanish at 0. Since Y is smooth of dimension d, by the Jacobian criterion, the L_is (which we may identify with the gradient of f_i at 0), span a $n-d$ dimensional space. After relabelling, we may assume that $L_1, \dots, L_{n-d}$ give a basis for this space. Let $\widetilde{Y}$ be the zero locus of $f_1, \dots, f_{n-d}$. Since $Y \subset \widetilde{Y}$ we have the codimension of $\widetilde{Y}$ at 0, $\mathrm{codim}_0(\widetilde{Y}) \leq \mathrm{codim}(Y) = n-d$. By construction, the Jacobian matrix of the defining equations for $\widetilde{Y}$ at 0 has rank $n-d$, and so by [Eis, p. 402], $n-d \leq \mathrm{codim}(\widetilde{Y})$. But then

$$n-d \leq \mathrm{codim}_0(\widetilde{Y}) \leq \mathrm{codim}(Y) = n-d$$

so $\mathrm{codim}_0(\widetilde{Y}) = n-d$ and also by the Jacobian criterion, we conclude that $\widetilde{Y}$ is smooth at 0. We may therefore, after shrinking U assume that $\widetilde{Y}$ is smooth, irreducible, and of the same dimension as Y. But $Y \subset \widetilde{Y}$ therefore implies $Y = \widetilde{Y}$, and in particular we may assume $r = n-d$, and the L_i are independent.

After choosing a new basis for $\mathbb{A}^n$, it is clear that we may assume $L_i = x_i$ while preserving our hypotheses.

Finally, consider the morphism $\gamma = ip : U \to U$ (where i and p are as in the definition of the retraction), and write $\gamma(\mathbf{x}) = (\gamma_1(\mathbf{x}), \dots, \gamma_n(\mathbf{x}))$, where each γ_i is a regular function on U. Since $\gamma_i(0) = 0$, we may write $\gamma_i = M_i + Q_i$ for the linear function

$$M_i = \sum \frac{\partial}{\partial x_i} \gamma_i \bigg|_{\mathbf{x}=0} x_i$$

and have all the partial derivatives of the Q_i vanishing. Let $\mathbb{T} = \mathrm{Spec}\, k[\varepsilon]/(\varepsilon^2)$, and consider a $\mathbb{T}$-valued point $\tau : \mathbb{T} \to U$ given by $\mathbf{a}\varepsilon = (a_1\varepsilon, \dots, a_n\varepsilon) \in \mathbb{A}^n(k[\varepsilon]/(\varepsilon^2))$. We note that τ maps $\mathbb{T}$ into Y if and only if $f_i(\mathbf{a}\varepsilon) = 0$ for each i. But we have (by Lemma 5.5.1)

$$f_i(\mathbf{a}\varepsilon) = L_i(\mathbf{a}\varepsilon) = \varepsilon L_i(\mathbf{a}).$$

In particular, this occurs exactly when $a_i = 0$ for $1 \le i \le n-d$. Since $\gamma(\mathbf{a}\varepsilon) \in Y$, we therefore have $M_i = 0$ for $1 \le i \le n-d$. Since $\gamma|_Y = \mathrm{id}_Y$, looking on $\mathbb{T}$-valued points of Y under γ, we find $M_i = M_i' + x_i$ for $n-d < i \le n$ where M_i' is a linear function of $x_1, \ldots, x_{n-d}$. Consider the linear function $\mathbb{A}^n \to \mathbb{A}^n$ given by

$$\phi : (x_1, \ldots x_n) \mapsto (y_1, \ldots, y_n)$$

where

$$y_i = \begin{cases} x_i & \text{if } 1 \le i \le n-d \\ x_i - M_i & n-d < i \le n \end{cases}$$

Define rational maps $i' = \phi \circ i : Y \dashrightarrow \mathbb{A}^n$ and $p' = p \circ \phi^{-1} : \mathbb{A}^n \dashrightarrow Y$. We then have $p' \circ i' = p \circ \phi^{-1} \phi i = pi = id_Y$ as rational maps, and therefore define a rational retraction. By Lemma 5.2.6 we may shrink U and Y to make this a closed retraction. Note also that $i'p' = \phi i p \phi^{-1} = \phi \gamma \phi^{-1}$.

As before, let $\tau : \mathbb{T} \to U$ be given by $\mathbf{a}\varepsilon = (a_1\varepsilon, \ldots, a_n\varepsilon) \in \mathbb{A}^n(k[\varepsilon]/(\varepsilon^2))$, where $\mathbf{a} \in \mathbb{A}^n(k)$. We consider the morphism $i'p' : U \to Y \to U$, which we write as

$$(x_1, \ldots, x_n) \mapsto (N_1 + P_1, \ldots, N_n + P_n)$$

with N_i linear and the first derivatives of the P_i vanishing at the origin. Computing using Lemma 5.5.1 applied to functions P_i, we then find

$$i'p'(\tau) = \varepsilon(N_1(\mathbf{a}), \ldots, N_n(\mathbf{a}))$$

and also, using the linearity of ϕ and the fact that $i'p' = \phi\gamma\phi^{-1} = \phi \circ (M+Q) \circ \phi^{-1}$,

$$i'p'(\tau) = \varepsilon\phi(M_1(\phi(\mathbf{a}), \ldots, M_n(\phi^{-1}(\mathbf{a}))) = \varepsilon(0, \ldots, 0, a_{n-d+1}, \ldots, a_n),$$

and so

$$N_i = \begin{cases} 0 \ \text{if } 1 \le i \le n-d \\ x_i \ \text{if } n-d < i \le n \end{cases}$$

Therefore, upon replacing p, i by p', i', we obtain the desired conclusion.

Acknowledgements The author is grateful to David Harbater, Julia Hartmann, and the anonymous referee for numerous helpful comments and corrections in the preparation of this manuscript.

References

[ASS] S.A. Amitsur, D.J. Saltman, and G.B. Seligman, editors. *Algebraists' homage: papers in ring theory and related topics*, volume 13 of *Contemporary Mathematics*, 1982. American Mathematical Society, Providence, RI.

[Bor] A. Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[CTPS] J.-L. Colliot-Thélène, R. Parimala, and V. Suresh. Patching and local-global principles for homogeneous spaces over function fields of p-adic curves, to appear in *Commentarii Math. Helv.*

[DI] F. DeMeyer and E. Ingraham. *Separable algebras over commutative rings*. Springer-Verlag, Berlin, 1971.

[Eis] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Gra] J.W. Gray. *Formal category theory: adjointness for* 2*-categories*. Lecture Notes in Mathematics, Vol. 391. Springer-Verlag, Berlin, 1974.

[Gro62] A. Grothendieck. *Fondements de la géométrie algébrique [Extraits du Séminaire Bourbaki, 1957–1962]*. Secrétariat mathématique, Paris, 1962.

[EGA] A. Grothendieck. Éléments de géométrie algébrique. 3–1: *Inst. Hautes Études Sci. Publ. Math.*, 11:167, 1961; 4–1: *Inst. Hautes Études Sci. Publ. Math.*, 20:259, 1964; 4–4: *Inst. Hautes Études Sci. Publ. Math.*, 32:321, 1967.

[HH] D. Harbater and J. Hartmann. Patching over fields. To appear in *Israel J. Math.*, arxiv:0710.1392.

[HHK] D. Harbater, J. Hartmann, and D. Krashen. Patching subfields of division algebras. to appear in *Trans. Am. Math. Soc.*, preprint available at arxiv:0904.1594.

[HHK09] ———. Applications of patching to quadratic forms and central simple algebras. *Invent. Math.*, 178:231–264, 2009.

[Hov] M. Hovey. *Model categories*, volume 63 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1999.

[Ill] L. Illusie. Frobenius et dégénérescence de Hodge. In *Introduction à la théorie de Hodge*, volume 3 of *Panor. Synthèses*, pages 113–168. Soc. Math. France, Paris, 1996.

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol. *The book of involutions*. American Mathematical Society, Providence, RI, 1998.

[ML] S. Mac Lane. *Categories for the working mathematician*. Springer-Verlag, New York, second edition, 1998.

[Sal] D.J. Saltman. Retract rational fields and cyclic Galois extensions. *Israel J. Math.*, 47(2–3):165–215, 1984.

[Ser] J-P. Serre. *Local fields*. Springer-Verlag, New York, 1979.

Deformation Theory and Rational Points on Rationally Connected Varieties

Max Lieblich

Summary We give an account of some recent work on the existence of rational points on varieties over function fields, starting with basic material on deformation theory and the bend-and-break theorem. We emphasize the connection with the geometry of moduli spaces and include a sketch of the irreducibility of $\mathscr{M}_g$ as a model. All details are relegated to the references.

1 Introduction

The question we address in these notes is the following. Fix once and for all an algebraically closed field k. In all sections but Sect. 2, we assume that k has characteristic 0.

Question 1.1. *Suppose $f : X \to S$ is a proper morphism to a smooth surface. What geometric properties of f ensure that it has a rational section?*

Lest this seem like a strange question, let us remind the reader of two theorems along these lines when the base has lower dimension.

Theorem 1.2 (Hilbert). *If $f : Z \to \operatorname{Spec} k$ is a morphism of finite type, then f has a section.*

This is the Nullstellensatz: any maximal ideal in a finite-type k-algebra has residue field k. Increasing the dimension of the base, we have the following more recent result.

Max Lieblich
Padelford Hall, University of Washington, Seattle, WA 98195, USA
e-mail: lieblich@math.washington.edu

2010 Mathematics subject classification. Primary: 14D06. Secondary: 14G05.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_5,

Theorem 1.3 (Graber–Harris–Starr). *If $f: Y \to C$ is a proper morphism to a curve whose geometric generic fiber is rationally connected, then f has a section.*

From an arithmetic point of view, this theorem says that any geometrically rationally connected variety over a finite extension of $k(t)$ has a rational point. Of course, it is easy to see that there are proper varieties over $k(t)$ that lack rational points. (*Example*. Let E be an elliptic curve over k. For any nonzero element of $\mathrm{H}^1(\operatorname{Spec} k(t), \mathbf{Z}/n\mathbf{Z}^{\oplus 2})$, there is an étale form of $E \otimes k(t)$ that lacks a section.)

What about higher-dimensional base fields? To what extent does the cohomological complexity of the base constrain the existence of sections? It is not enough for the geometric fibers of f to be rationally connected. For example, the conic over $k(s,t)$ given in homogeneous coordinates by $X^2 + tY^2 + sZ^2 = 0$ has no points over $k(s,t)$. Our goal in these notes is ultimately to explain some of the ideas behind recent work of de Jong and Starr that imposes some additional conditions on the fibers of f to ensure that f does have a rational section when S is a surface. These conditions are roughly analogous to the condition that the fibers be "rationally simply connected," but we will not explain this in any detail.

In fact, we will not be able to explain much at all! The primary purpose of these notes is to put the work of de Jong and Starr in context, and to introduce the reader to some basic ideas and techniques related to the interaction between the geometry of moduli spaces and the existence of rational points on varieties over function fields. In Sect. 2, we will recall some of the basic results on rational curves and deformation theory, including Mori's bend-and-break and the notion of rational connectedness. Having seen the usefulness of deforming and degenerating moving curves, we will formalize it in Sect. 3 by introducing Kontsevich spaces. The geometry of these spaces rules the domain of rational points over function fields. As two examples, we give a sketch of the Graber–Harris–Starr theorem and the irreducibility of the moduli space of smooth curves of genus g. The latter gives the archetypical example of a moduli problem that one can attack by attaching a boundary parameterizing degenerate objects whose degeneracies give an inductive structure to the moduli problem (in this case, inductive in the genus). Finally, in Sect. 4, we describe aspects of the de Jong–Starr theory of porcupines, showing how a similar inductive structure yields irreducibility results for Kontsevich spaces of stable sections. We then explain how these types of results can be used to reduce questions about fibrations over surfaces to questions about fibrations over curves, thus allowing de Jong and Starr to bootstrap from the Graber–Harris–Starr theorem to give results about rational sections over surfaces. Gille's paper "Serre's Conjecture II: A Survey" in this volume explains how de Jong, He, and Starr used these ideas to prove Serre's Conjecture II on torsors over surfaces.

We assume that the audience does not consist of expert algebraic geometers, so we have tried to make most of the document understandable to beginners (going so far as to include a couple of sporadic exercises in Sect. 2). Even so, the level is highly uneven and a few digressions are only suitable for more experienced readers. The books and articles in the bibliography are a good place to start for a reader interested in learning more about this area.

2 Deformations of Maps and Rational Connectivity

In this section, we allow k to have arbitrary characteristic. Let us begin with a question.

Question 2.1. *Suppose Y is a smooth variety over k. How can we produce simple curves in Y?*

Here is an idea: choose any irreducible curve $D \subset Y$ and "move D around" until it breaks into two components. If this is done properly, one should expect that the two components are simpler than D. In fact, a careful analysis of how this process works shows that the limit will break off the simplest kind of curve – a rational curve.

The basic result underpinning this technique is the following theorem.

Theorem 2.2. *Let Y be a proper smooth variety over k, C a proper smooth curve over k, $y \in Y$ a point, and $c \in C$ a point. Suppose T is a (possibly affine) curve over k, and that there is a morphism $\varphi : T \times C \to Y$ such that for each $t \in T$, the fiber φ_t sends c to y. If there exist two points t_1 and t_2 in T such that $\varphi_{t_1}(C) \neq \varphi_{t_2}(C)$, then there is a rational curve R in Y which passes through y, a morphism from a curve $\gamma : D \to Y$ whose image contains y, and an algebraic equivalence between $\varphi_{t_1}(C)$ and $R + \gamma_* D$.*

In other words, as C moves fixing a point ("bends"), it breaks off a (rational) component in the limit. If the variety Y is projective and γ is nonconstant, then we see that both $\gamma_* D$ and R have smaller degree than C, so that in this case C breaks into "simpler" curves. The theorem is phrased in a strange way because we want to include the case in which γ is a constant map (so that $\varphi_{t_1}(C)$ is equivalent to R).

Exercise 2.3. A simple example of this phenomenon (in which the exceptional fiber of a blowup "replaces" the fiber of the family to which it attaches) is given by the scaling rational map $\mathbf{P}^1 \times \mathbf{P}^1 \dashrightarrow \mathbf{P}^1$; in coordinates, $[X : Y] \times [S : T] \mapsto [XS : YT]$. Find the points of indeterminacy and show that the morphism $\gamma : D \to Y$ in Theorem 2.2 is constant. (The proof of Theorem 2.2 will clarify the meaning of this exercise.)

Proof of Theorem 2.2. We may suppose that T is a smooth curve; let T' be the smooth projective completion of T. It is well known that there is a sequence of blowups in smooth points on the projective surface $T' \times C$ such that the rational map φ extends to a regular morphism from the blowup to Y. It is enough to see that we need at least one blowup centered on $T' \times \{c\}$ to extend the morphism. Suppose to the contrary that φ is itself regular in a neighborhood of $T' \times \{c\}$. By assumption, φ contracts the curve $T' \times \{c\}$ to the point y in Y. By the rigidity lemma [12, Proposition 6.1], φ then has to contract all of the fibers in a neighborhood of c, and it easily follows from this that all of the morphisms φ_t are the same. □

This theorem would not be especially useful were it not for the fact that we can tell when such positive-dimensional families of maps exist. First, recall the following fundamental result of Grothendieck.

Proposition 2.4 (Grothendieck). *If Y is projective, the functor* $\mathrm{Hom}(C,Y)$ *which sends a k-scheme U to the set of k-morphisms $U \times C \to Y$ is representable by a scheme (which we will also write as* $\mathrm{Hom}(C,Y)$*) with quasiprojective connected components. Given points $c \in C$ and $y \in Y$, there is a closed subscheme* $\mathrm{Hom}_{c \mapsto y}(C,Y)$ *parameterizing morphisms $\varphi : C \to Y$ such that $\varphi(c) = y$.*

More generally, if $\mathscr{C} \to S$ is a proper flat family of curves and $Y \to S$ is a projective scheme, then one can construct an S-scheme $\mathrm{Hom}_S(\mathscr{C},Y)$ parameterizing families of homomorphisms. In either case, to prove the proposition, one first identifies a morphism with its graph, which is a closed subscheme of $C \times Y$. This turns $\mathrm{Hom}(C,Y)$ into a closed subscheme of the Hilbert scheme parameterizing closed subschemes of a projective scheme, which Grothendieck had already constructed and shown has quasiprojective connected components [6].

To find a family $T \times C \to Y$ as in Theorem 2.2, we need only map a curve T to the Hom-scheme $\mathrm{Hom}_{c \mapsto y}(C,Y)$.

Corollary 2.5. *Suppose $C \subset Y$ is a curve, and fix a point $c \in C$. If* $\mathrm{Hom}_{c \mapsto c}(C,Y)$ *is positive dimensional, then there is a rational curve $R \subset Y$ passing through c, a curve D with a morphism $\gamma : D \to Y$ and an algebraic equivalence $C \equiv R + \gamma_* D$.*

How can we tell if $\mathrm{Hom}_{c \mapsto y}(C,Y)$ is positive dimensional? Let us start with an easier question: how can we tell if $\mathrm{Hom}(C,Y)$ is positive dimensional? One thing we can do is to calculate the tangent space to the scheme at a point $\varphi : C \to Y$. The calculation is one of the gems of algebraic geometry.

Write $S = \operatorname{Spec} k[\varepsilon]/(\varepsilon^2)$. It is a standard fact that the tangent space to a k-scheme Q at a point $q : \operatorname{Spec} k \to Q$ is identified with the set of maps $S \to Q$ such that the composition with the natural closed immersion $\operatorname{Spec} k \hookrightarrow S$ (given by setting ε equal to 0) is q. For the scheme $Q = \mathrm{Hom}(C,Y)$, the tangent space at a morphism $\varphi : C \to Y$ is thus described by families of maps $S \times C \to Y$ reducing to φ when $\varepsilon = 0$. These are basic objects of deformation theory: first-order infinitesimal deformations of φ.

Definition 2.6. An *infinitesimal deformation* of a morphism $\varphi : C \to Y$ is an S-morphism $\tilde{\varphi} : C \times S \to Y \times S$ whose base change via the natural morphism $\operatorname{Spec} k \to S$ is equal to φ.

There is always an infinitesimal deformation of any morphism φ: the trivial deformation given by base change with respect to structure morphism $S \to \operatorname{Spec} k$. This is precisely the 0 element of the tangent space $T_\varphi \mathrm{Hom}(C,Y)$. (*Exercise*. The tangent space has a linear structure. Find a functorial description in terms of maps.)

Using Čech cohomology, we can describe precisely what the infinitesimal deformations of φ are.

Proposition 2.7. *There is a natural bijection between infinitesimal deformations of φ and* $\mathrm{H}^0(C, \varphi^* T_Y)$*, where T_Y denotes the tangent sheaf of Y.*

Proof. Suppose for a moment that all of the schemes are affine, so that $C = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$ with A and B two k-algebras. The morphism φ then corresponds to a k-algebra homomorphism $\gamma : B \to A$, and an infinitesimal deformation of φ corresponds to a $k[\varepsilon]$-algebra homomorphism $B[\varepsilon] \to A[\varepsilon]$ which equals γ modulo ε. A routine calculation identifies such extensions with B-linear derivations $B \to A$. By the universal property of the module of differentials, such derivations are identified with B-linear module homomorphisms $\Omega_B \to A$, and these are the same as A-linear module homomorphisms $\Omega_B \otimes A \to A$. Dualizing, such maps are elements of the tangent module $T_B \otimes A$. Covering C with affine schemes which map into affine open subschemes of Y, we can apply the preceding argument to give local sections of $\varphi^* T_Y$; these glue together to give a global section, as desired. □

Now, even if we can show that the tangent space $T_\varphi \operatorname{Hom}(C,Y)$ is positive dimensional, this does not mean that the scheme is positive dimensional. To settle the issue, we would like to be able to compute all the jets at a point and not merely the tangent space. In other words, we would like to describe the structure of the complete local ring $\widehat{\mathscr{O}}_{\operatorname{Hom}(C,Y),\varphi}$. This requires a broadening of our deformation theory.

Write $S_n = \operatorname{Spec} k[x]/(x^{n+1})$. Given a k-morphism $\varphi : C \times S_{n-1} \to Y$ (which is the same as an S_{n-1}-morphism $C \times S_{n-1} \to Y \times S_{n-1}$), we can try to understand its deformations to a morphism $C \times S_n \to Y$. Write $\varphi_0 : C \to Y$ for the restriction of φ to the closed subscheme arising from the closed immersion $\operatorname{Spec} k \hookrightarrow S_{n-1}$. An analysis similar to that carried out above shows that for any affine $\operatorname{Spec} A \subset C$ such that $\varphi(\operatorname{Spec} A)$ lands in an affine open $\operatorname{Spec} B$ of Y, there is an extension of φ to $C \times S_n$, and that extensions are parameterized by (are a principal homogeneous space under) $\mathrm{H}^0(\operatorname{Spec} A, \varphi_0^* T_Y)$. Let $\{U_i\}_{i=1}^m$ be such an affine open covering of C. Given $i \neq j$, choosing deformations of φ_{U_i} yields two sections of $\varphi_0^* T_Y$ over $U_i \cap U_j$. It is an amusing exercise to show that this is a 1-cocycle with coefficients in $\varphi_0^* T_Y$. In fact, we have the following proposition.

Proposition 2.8. *Given a morphism $\varphi : C \times S_{n-1} \to Y$ as above:*

1. *There is an extension of φ to a morphism $\tilde{\varphi} : C \times S_n \to Y$ if and only if the cohomology class $ob \in \mathrm{H}^1(C, \varphi_0^* T_Y)$ associated to the cocycle constructed above vanishes.*
2. *If $ob = 0$, then the set of deformations of φ to $\tilde{\varphi} : C \times S_n \to Y$ is a principal homogeneous space under the group $\mathrm{H}^0(C, \varphi_0^* T_Y)$.*

Proof. The proof is left to the reader as an exercise. □

In other words, the vector bundle $\varphi_0^* T_Y$ governs the infinitesimal deformation theory of the morphism $\varphi_0 : C \to Y$. A more careful study of the properties of the deformation theory yields the following result, due to Schlessinger (implicit in the proof of Theorem 2.11 of [13] and made explicit using obstruction theory in Proposition 2.A.11 of [7]). Write $d_i = \dim_k \mathrm{H}^i(C, \varphi_0^* T_Y)$ for $i = 0, 1$.

Proposition 2.9. *The complete local ring of* $\operatorname{Hom}(C,Y)$ *at* $[\varphi_0]$ *is isomorphic to a quotient of* $k[[x_1, \dots, x_{d_0}]]$ *by at most three elements.*

The proof is a formal consequence of a suitably functorial generalization of Proposition 2.8. Thus, for example, if $\mathrm{H}^1(C,\varphi_0^*T_Y)=0$ then $\mathrm{Hom}(C,Y)$ is smooth at $[\varphi_0]$.

Now what about the subscheme $\mathrm{Hom}_{c\mapsto y}(C,Y)$? It turns out that we can easily modify the deformation theory to account for the fixed points. The restriction map $\mathrm{H}^0(C,\varphi_0^*T_Y)\to\mathrm{H}^0(c,\varphi_0^*T_Y|_c)$ expresses the restriction of infinitesimal deformations to c, and we seek those whose restriction to c is trivial. Arguing as in the proof of Proposition 2.8 yields the following.

Proposition 2.10. *Given a point $[\varphi]\in\mathrm{Hom}_{c\mapsto y}(C,Y)(S_{n-1})$ as above:*

1. *There is a class $ob\in\mathrm{H}^1(C,\varphi_0^*T_Y(-c))$ which vanishes if and only if φ extends to $C\times S_n$.*
2. *If $ob=0$, then the set of deformations is a principal homogeneous space under the group $\mathrm{H}^0(C,\varphi_0^*T_Y(-c))$.*
3. *Writing $d_i=\dim\mathrm{H}^i(C,\varphi_0^*T_Y(-c))$, the complete local ring of $\mathrm{Hom}_{c\mapsto y}(C,Y)$ at $[\varphi_0]$ is isomorphic to a quotient of $k[[x_1,\dots,x_{d_0}]]$ by at most d_1-relations. In particular, $\dim_{\varphi_0}\mathrm{Hom}_{c\mapsto y}(C,Y)\geq\chi(\varphi_0^*T_Y(-c))$.*

The astonishing result of combining Proposition 2.10 and Theorem 2.2 is the following numerical criterion for the existence of a rational curve through y contributing to the numerical equivalence class of C.

Corollary 2.11. *Suppose C, Y, c, y, and φ_0 are as above with C smooth. If*

$$-\deg\varphi_0^*K_Y>g(C)\dim Y,$$

then there is a rational curve passing through y.

Proof. First, if $\varphi_0(C)$ is a rational curve then the corollary is verified. Thus, we will assume that $\varphi_0(C)\subset Y$ is a (possibly singular!) curve whose geometric genus is positive. (In particular, C itself has positive genus.)

Riemann-Roch tells us that

$$\chi(C,\varphi_0^*T_Y(-c))=\deg\varphi_0^*T_Y(-c)+\dim Y(1-g(C))=-\deg\varphi_0^*K_Y-g(C)\dim Y.$$

On the other hand, we know by Proposition 2.10(3) that $\dim_{\varphi_0}\mathrm{Hom}_{c\mapsto y}(C,Y)\geq\chi(C,\varphi_0^*T_Y(-c))$. The result thus follows from Theorem 2.2 if we can show that a positive-dimensional family of morphisms $C\to Y$ sending c to y containing φ_0 as a fiber must have image of dimension at least 2. Suppose to the contrary that T is a smooth curve and $\varphi:C\times T\to Y$ is a morphism such that $\varphi(\{c\}\times T)=y$ and $\varphi(C\times T)$ is a curve $\overline{C}\subset Y$. Replacing $\overline{C}$ by its normalization (T being itself normal), we may thus assume that Y is a smooth proper curve of positive genus and $C\times T\to Y$ is a family of surjective morphisms sending c to y. But now the tangent space to $\mathrm{Hom}_{c\mapsto y}(C,Y)$ at φ_0 has dimension $\dim\mathrm{H}^0(C,\varphi_0^*T_Y(-c))=0$ because $\deg\omega_Y\geq 0$. In other words, the family corresponds to a map $T\to\mathrm{Hom}_{c\mapsto y}(C,Y)$ to a discrete space and thus to a constant family of maps, contradicting our assumption. □

What happens if we already know that C is a rational curve? Can we move C until it breaks into a simpler curve (e.g., one of lower degree)? The phenomenon described in Exercise 2.3 shows that trying to simplify C by pinning down a single point is an exercise in futility. Mori's insight was instead to fix *two* points of C. For the sake of expository simplicity, we will take an even easier way out and fix three points. (Of course, the more points one can fix, the better the chances of breaking off a simpler component in the deformation. The cost of this ease is that to deform a curve while fixing a large number of points, the curve must start out with a fairly high degree.)

Fix three distinct points y_0, y_1, and y_∞ of Y.

Proposition 2.12. *Suppose T is a smooth curve and $f : T \times \mathbf{P}^1 \to Y$ is a morphism such that $f(T \times \{i\}) = y_i$ for $i = 0, 1, \infty$. If there are t_1 and t_2 such that $f_{t_1} \neq f_{t_2}$, then there are two nonempty curves R and D in Y with rational irreducible components, with R passing through y_0, and an algebraic equivalence $f_{t_1}(\mathbf{P}^1) \equiv R + D$.*

Proof. Just as in the proof of Theorem 2.2, let T' be the smooth projective closure of T. We claim that the rational map $T' \times \mathbf{P}^1 \dashrightarrow Y$ induced by f must have a point of indeterminacy on at least one section $T \times \{i\}$. If not then the argument of Theorem 2.2 shows that $f_{t_1} = f_{t_2}$, contradicting the assumption. Without loss of generality, we may assume that there is some $t \in T'$ such that f only extends after blowing up (possibly several times) at $t \times \{0\}$ (and infinitely near points). Write $X \to T' \times \mathbf{P}^1$ for the blowup and (abusing notation) $f : X \to Y$ for the extension. The three points $0, 1, \infty$ of $\mathbf{P}^1$ extend to sections which we will call $[0], [1], [\infty]$ of X over T'. The fiber X_t is a union of rational curves, and to prove the proposition it suffices to show that at least two of them map finitely to Y. Suppose to the contrary that there is a unique irreducible component $\Xi \subset X_t$ such that $f(\Xi) = f(X_t)$. Since we are assuming that f is not regular along $\mathbf{P}^1_t$, we know that Ξ must be in the exceptional locus of $X \to \mathbf{P}^1 \times T'$. But then there is a connected subscheme of $X_t \setminus \Xi$ intersecting at least two of the sections $[0], [1], [\infty]$. Thus, if $X_t \setminus \Xi$ has 0-dimensional image, then $f([i])$ and $f([j])$ must intersect for some $i \neq j$, and this contradicts our assumption that $f([i]) = y_i$. We thus conclude that at least two components of X_t map nontrivially to X, yielding the desired algebraic equivalence. $\square$

Corollary 2.13. *If $f : \mathbf{P}^1 \to Y$ is a generically injective morphism such that*

$$-\deg f^* K_Y > 3 \dim Y,$$

then there is a rational curve $R \subset Y$ passing through $f(0)$, a curve $D \subset Y$, and an algebraic equivalence $f(\mathbf{P}^1) \equiv R + D$. In particular, if $-K_Y$ is ample and there is a rational curve $Z \subset Y$ through a point y, then there is a rational curve R through y such that $0 < -K_Y \cdot R \leq 3 \dim Y$.

Proof. First, note that the local dimension of Hom-space with three fixed points at any point (in a neighborhood of any fixed morphism) is bounded below by $\chi(\mathbf{P}^1, f^* T_Y(-[0] - [1] - [\infty])) = -\deg f^* K_Y - 3 \dim Y$. We claim that if this dimension is positive, then the restriction of the universal family to any smooth curve

$T \subset \mathrm{Hom}(\mathbf{P}^1, Y; 0+1+\infty)$ satisfies the hypothesis of Proposition 2.12. Indeed, this works as in the proof of Corollary 2.11. We state an appropriate exercise for the reader in training.

Exercise 2.14. Show that any morphism $\Phi : \mathbf{P}^1 \times T \to Y$ with T a smooth curve such that

1. $\Phi([i]) = y_i$ for $i = 0, 1, \infty$, and
2. there is a geometric point $t \to T$ such that the fiber Φ_t is generically injective

has two-dimensional image. In other words, there are t_1 and t_2 in T such that $f_{t_1} \neq f_{t_2}$. (*Hint*. The scheme of automorphisms of $\mathbf{P}^1$ that fix 0, 1, and ∞ is trivial.)

For the final statement, note that for any curve (closed subscheme of dimension 1) $E \subset Y$, the intersection $E \cdot (-K_Y)$ is positive. Thus, if $Z = D + R$ then $0 < R \cdot (-K_Y) < Z \cdot (-K_Y)$, and we can always find such an R if $Z \cdot (-K_Y) > 3 \dim Y$. □

Putting Corollaries 2.11 and 2.13 together yields the following result. Recall that a smooth proper variety Y is *Fano* if $-K_Y$ is an ample divisor.

Proposition 2.15. *Suppose Y is Fano and $y \in Y$ is a point. If there is a curve C and a morphism $f : C \to Y$ passing through y such that $-\deg f^* K_Y > g(C) \dim Y$, then there is a rational curve R in Y passing through y such that $-K_Y \cdot R \leq 3 \dim Y$.*

This seems to imply that Fano varieties should be covered by rational curves. We briefly recall a basic definition.

Definition 2.16. A variety Y is

1. *uniruled* if a general point $y \in Y$ is contained in the image of a morphism $\mathbf{P}^1 \to Y$.
2. *rationally connected* if for all points y_0 and y_1 in Y there is a morphism $f : \mathbf{P}^1 \to Y$ such that $f(i) = y_i$ for $i = 0, 1$.

This definition of rational connectedness is equivalent to various other conditions: it suffices to check that for a single fixed uncountable algebraically closed over field κ/k, a general pair of κ-valued points is connected by rational curve, and this is equivalent to the statement that there is a finite-type k-scheme M and a morphism $M \times \mathbf{P}^1 \to Y$ such that the morphism $M \to Y \times Y$ induced by evaluation at 0 and 1 is dominant. Moreover, a proper smooth variety Y is rationally connected if and only if it is rationally chain connected, which means that any two points are connected by a (nodal) chain of rational curves in Y. As usual, these ideas are more subtle in positive characteristic due to the existence of nontrivial inseparable morphisms.

Proposition 2.15 might lead the reader to think that Fano varieties are uniruled. However, there is a subtle point: one must have a curve mapping to Y which deforms in a family of size depending upon its genus. How can one arrange for this? Mori observed that this is much easier in characteristic p and that the numerical bound in Proposition 2.15 suffices to lift this to characteristic 0.

Theorem 2.17 (Mori [11]). *Fano varieties over k are uniruled.*

Idea of proof. First, suppose k has positive characteristic p. Choose a point $y \in Y$ and any nonconstant curve $f : C \to Y$ passing through y. Since Y is Fano, $-\deg f^*K_Y > 0$, but of course it could be smaller than $g(C)\dim Y$. It is here that the great advantage of characteristic p – the Frobenius morphism – comes to the rescue. Composing f with the relative Frobenius $F : C^{(\mathrm{F})} \to C$ (so that all morphisms are over k!) yields a new morphism $f_1 : C^{(\mathrm{F})} \to Y$ from a curve of the same genus such that $-\deg f_1^*K_Y = p(-\deg f^*K_Y)$. In particular, composing with sufficiently many copies of F, we may assume that $-\deg f^*K_Y$ is as large as we like. This fits f into the regime of Proposition 2.15, which then produces a rational curve $R \subset Y$ containing y such that $R \cdot (-K_Y) \leq 3\dim Y$.

Now comes the delightful surprise. Since Y is of finite type over k, there is a finitely generated subring $A \subset k$ and a smooth proper A-scheme $\mathscr{Y} \to \operatorname{Spec} A$ with a section $\sigma : \operatorname{Spec} A \to \mathscr{Y}$ whose base change with respect to the geometric generic point $\operatorname{Spec} k \to \operatorname{Spec} A$ is isomorphic to Y with the section y and such that $\omega^\vee_{\mathscr{Y}/A}$ is A-ample. The relative Hom-space $\operatorname{Hom}^\sigma_A(\mathbf{P}^1, \mathscr{Y})^{3\dim Y}$ parameterizing nonconstant morphisms $f : \mathbf{P}^1 \to \mathscr{Y}$ with images containing σ such that $f^*\omega^\vee_{\mathscr{Y}/A}$ has degree at most $3\dim Y$ on each fiber is known to be of finite type over A: thinking of the graphs of the morphisms, one sees that this is a locally closed subscheme of the Hilbert scheme of $\mathscr{Y} \times \mathbf{P}^1$ and is contained in the locus with a bounded degree with respect to the natural polarization on $\mathscr{Y} \times \mathbf{P}^1$. Since every closed point of $\operatorname{Spec} A$ has residue field of positive characteristic, the previous paragraph shows that the scheme-theoretic image of $\pi : \operatorname{Hom}^\sigma_A(\mathbf{P}^1, \mathscr{Y})^{3\dim Y} \to \operatorname{Spec} A$ contains every closed point. But π is of finite type, hence has constructible image by Chevalley's theorem, and therefore the image must contain the generic point. This says precisely that there is a rational curve on Y through y (over k), as desired.

For further details the reader could consult numerous sources, among them [2, 8, 10]. □

With more elbow grease, one can prove the following amazing theorem.

Theorem 2.18 (Campana [1], Kollár–Miyaoka–Mori [9]). *A smooth projective Fano variety is rationally connected.*

The characterization of infinitesimal deformations in terms of linear algebra is the first pillar of deformation theory. Let us now touch on the second pillar – integrating infinitesimal deformations over complete local base rings.

3 Deformations of Curves, Stable Maps, the Graber–Harris–Starr Theorem, and Irreducibility of $\mathscr{M}_g$

In this section, we discuss a more systematic approach to the ways in which curves can break when they are moving. This will lead us to stable curves and the Kontsevich moduli space of stable maps. We also review some classical moduli problems and discuss how the method of degeneration to the boundary yields numerous results on the structure of moduli spaces. As we will see in Sect. 4, the techniques of de Jong and Starr fit into the classical framework in which moduli problems come with an inductive structure provided by the boundary.

In Sect. 2, we described the deformation theory of morphisms and how it can be used to break a curve apart. In this section, we spend some time describing the deformation theory of varieties and how this can be used to smooth a singular curve in a variety. The easiest way to construct a degenerating family of varieties is to blow up a trivial family. The resulting family will be surprising useful in what follows.

Degeneration 3.1. Given a fixed smooth curve C, we can blow up $\mathbf{P}^1 \times C$ in finitely many points. This yields a family of curves, of which the generic fiber is smooth, and for which special fibers are nodal unions of a curve isomorphic to the general fiber and some rational components. We can obviously iterate this construction, to produce chains of rational curves attached to C in a fiber, with a family smoothing this to a copy of C. (This is a simple example of the famous "deformation to the normal cone.")

Let $T = \operatorname{Spec} k[[t]]$ and write $T_n = \operatorname{Spec} k[[t]]/(t^{n+1})$. The blowup construction above yields proper flat families $\mathscr{C} \to T$ whose geometric generic fiber is isomorphic to the base change of C and whose closed fiber $\mathscr{C}_0$ is isomorphic to a nodal union of C and a finite number of chains of rational curves. Given a morphism $\varphi_0 : \mathscr{C}_0 \to Y$ such that $\mathrm{H}^1(\mathscr{C}_0, \varphi_0^* T_Y) = 0$, the machinery described in the previous section yields a sequence of extensions of φ_0 to morphisms $\mathscr{C} \times_T T_n$. Can we somehow integrate these infinitesimal extensions to yield a morphism from the proper smooth curve C?

Proposition 3.2. *Base change yields a bijection between the set* $\hom_T(\mathscr{C}, Y \times T)$ *and the set* $\varprojlim \hom_{T_n}(\mathscr{C} \times_T T_n, Y \times T_n)$ *of compatible systems of infinitesimal morphisms.*

Proof. As discussed in Sect. 2, the functor $\mathrm{Hom}_T(\mathscr{C}, Y \times T)$ is representable by a scheme H locally of finite type over T. The proposition is thus equivalent to the claim that the natural map induced by restriction $H(T) \to \varprojlim \mathrm{Hom}(\mathscr{C} \times_T T_n, Y \times T_n)$ is a bijection. But this is equivalent to the fact that if A is a local ring, the natural map $\mathrm{Hom}_{\mathrm{local}}(A, k[[t]]) \to \varprojlim \mathrm{Hom}(A, k[t]/(t^n))$ is a bijection, where the first is the set of local homomorphisms of local rings. Bijectivity of this map follows from the fact that $k[[t]]$ is t-adically complete. $\square$

As a consequence of the proposition, we see that a cohomological calculation on $\mathscr{C}_0$ ultimately yields a smooth curve in Y with the same homology class as $\varphi_0(\mathscr{C}_0)$. If we start with a large supply of curves on which the tangent bundle of Y is positive, then these kinds of arguments produce for us many smooth curves in Y; later, we will apply this technique to produce sections of a proper flat morphism $Y \to C$. Let us formalize these processes.

Definition 3.3. A *stable map of genus* g to Y is a morphism $f : C \to Y$ such that:

1. C is a reduced connected proper curve of arithmetic genus g with at worst nodes as singularities.
2. Any rational component of C which is contracted by f contains at least three singular points of C, while any genus 1 component of C contracted by f contains at least one singular point of f.

The second condition of Definition 3.3 is equivalent to the statement that the morphism f has finite automorphism group. As a special case, when Y is a single point, we recover the usual Deligne–Mumford notion of a stable curve of genus g (and here the second condition is equivalent to finiteness of the automorphism group of C).

The basic result on stable maps is the following, which is a special case of Theorem 1 of Fulton and Pandharipande [4].

Theorem 3.4. *Given a homology class β on Y, there is a projective moduli space $\overline{\mathscr{M}}_{g,0}(Y,\beta)$ parameterizing stable maps $f : C \to Y$ of genus g such that the pushforward of the fundamental class $f_*(C)$ is equal to β.*

When we say that β is a "homology class," the reader can choose to work with Chow theory (modulo algebraic equivalence) or with integral or ℓ-adic cohomology. The original work was done over $\mathbf{C}$, so it is customary to fix $\beta \in \mathrm{H}_2(Y,\mathbf{Z})$.

Remark 3.5. When we say "moduli space," we are purposely leaving things slightly vague. The reader comfortable with stacks should read this as "Deligne–Mumford stack" and should replace "projective" with "proper with projective coarse moduli space." In this case, an isomorphism between two objects $C \to Y$ and $C' \to Y$ is an isomorphism $C \to C'$ commuting with the morphisms to Y. Readers unfamiliar with the theory of stacks will not lose anything essential, and should think we are working with coarse moduli spaces as in [4]. In this case, the points of $\overline{\mathscr{M}}_{g,o}(Y,\beta)$ parameterize isomorphism classes of stable maps $C \to Y$.

Using modern techniques, the proof of this theorem is not especially difficult (although projectivity is a bit more subtle than existence). Existence follows relatively easily from the existence of the Deligne–Mumford moduli space $\overline{\mathscr{M}}_g$ of stable curves of genus g; the existence of the latter is somewhat less trivial. In fact, it was in Deligne and Mumford's paper [3] on the irreducibility of $\mathscr{M}_g$ that the concept of an algebraic stack was first codified. One especially streamlined way to see that $\overline{\mathscr{M}}_g$ exists as an algebraic stack is to use Artin's representability theorem, which reduces the algebraicity to properties of the natural deformation theory of the moduli problem, something that is transparent for families of curves.

One especially amusing example of a Kontsevich space is the space $\overline{\mathscr{M}}_{g,0}(C,[C])$, where C is a fixed smooth curve of genus g and $[C]$ is the fundamental class of C in $\mathrm{H}_2(C,\mathbf{Z})$. What does this parameterize? A stable map $f : D \to C$ with homology class $f_*([D]) = [C]$ has the following properties:

1. There is a unique irreducible component $C' \subset D$ which maps isomorphically to C.
2. The union of the remaining components (if there are any) is a nodal union of curves with total arithmetic genus 0 such that each component contains at least three singular points.

Exercise 3.6. In the above situation, the inclusion $C' \subset D$ is an isomorphism.

In other words, $\overline{\mathscr{M}}_{g,0}(C,[C])$ has only one point. (Two different isomorphisms $C' \to C$ differ by an automorphism of C' and thus give rise to the same point in the moduli space.)

On the other hand, consider the space $\overline{\mathscr{M}}_{g,0}(C,e[C])$ for some integer $e > 1$, and let us restrict our attention to the case $C = \mathbf{P}^1$. Now, we can make interesting elements in the space.

Construction 3.7. Given e copies of $\mathbf{P}^1$, choose $e+g-1$ points p_i in $\mathbf{P}^1$. For each i, choose two indices $j \neq j'$ and (nodally) glue the points p_i on the j and j' copies of $\mathbf{P}^1$; do this in such a way that the resulting curve is connected. This yields a flat stable map $C \to \mathbf{P}^1$ of genus g whose irreducible components are all isomorphic to $\mathbf{P}^1$.

Remark 3.8. It is a remarkable fact that there is actually a unique irreducible component of $\overline{\mathscr{M}}_{g,0}(\mathbf{P}^1,e[\mathbf{P}^1])$ containing those points parameterizing stable maps which are flat. (Note that even in this irreducible component, the limit points need not be flat.) We will call this component F.

For large enough e, which is all that is needed here, one can prove the uniqueness of F rather easily as follows. Let F° denote the locus parameterizing flat stable maps $\sigma : C \to \mathbf{P}^1$ of genus g with C smooth. The forgetful functor gives a morphism $\Phi : F^\circ \to \mathscr{M}_g$ to the stack of stable curves of genus g, which we claim is smooth for large enough values of e. Since Φ has connected geometric fibers (Grassmannian bundles over Pic^e_C), it will follow that F° is itself irreducible (by Theorem 3.10). To see that Φ is smooth, note that morphisms σ correspond to invertible sheaves $\mathscr{L}$ on C of degree e along with a pair of generating sections $\mathscr{O}_C^{\oplus 2} \twoheadrightarrow \mathscr{L}$. Given an infinitesimal deformation of C over $k[\varepsilon]$, the invertible sheaf $\mathscr{L}$ lifts (as the obstruction to doing so lies in $\mathrm{H}^2(C,\mathscr{O}) = 0$), and the obstruction to lifting the generating sections lies in $\mathrm{H}^1(C,\mathscr{L})^{\oplus 2}$, which vanishes as long as $e > 2g-2$.

Now, let $D \to \mathbf{P}^1$ be a flat stable map of genus g with D nodal. By an argument identical to that following Proposition 3.11 (treating D as a lci $\mathbf{P}^1$-scheme), one can show that $D \to \mathbf{P}^1$ deforms to a map $D' \to \mathbf{P}^1$ with D' smooth. It follows that any flat stable map is in the closure of F°, showing that there is thus a unique irreducible component containing F°, as desired.

The geometry of the Kontsevich spaces (in particular, the uniqueness of the component F in Remark 3.8) leads to the existence of sections for rationally connected fibrations over curves.

Theorem 3.9 (Graber–Harris–Starr). *If $f : Y \to B$ is a proper morphism to a curve with rationally connected geometric generic fiber, then f has a section.*

Idea of proof. We may (and will) assume that Y is smooth and projective. First suppose $C = \mathbf{P}^1$. Given a proper flat morphism $f : Y \to \mathbf{P}^1$, a smooth irreducible curve $C \subset Y$ of genus g which is (finite) flat of degree e over $\mathbf{P}^1$ yields a point $[C] \in \overline{\mathscr{M}}_{g,0}(\mathbf{P}^1, e[\mathbf{P}^1])$. Can we deform C until it breaks up into sections of f?

Suppose there is a family of smooth curves $\mathscr{C} \to T$ with a morphism $\Phi : \mathscr{C} \to Y$ such that:

1. For all $s \in T$, the morphism $f \circ \Phi_s : \mathscr{C}_s \to \mathbf{P}^1$ is finite (flat).
2. There is a point $t \in T$ such that Φ_t is the given multisection $C \to Y$.

Suppose furthermore that the composed map $f \circ \Phi : \mathscr{C} \to \mathbf{P}^1$ induces a dominant morphism $T \to F$ (where F is as in Remark 3.8). We know that there is a k-point of F parameterizing a curve that is a union of sections over $\mathbf{P}^1$ as in Construction 3.7. Thus, we can find

1. a discrete valuation ring R with fraction field K and residue field κ,
2. a proper flat family of curves $\mathscr{D} \to \operatorname{Spec} R$, and
3. morphisms $p : \operatorname{Spec} K \to T$, $\rho : \mathscr{D}_K \to Y$, $\chi : \mathscr{D} \to \mathbf{P}^1_R$

such that there is a commutative diagram

$$\begin{tikzcd} \mathscr{D}_K \arrow[dr, "\rho"] \arrow[dd, "\cong"'] & \\ & Y \\ \mathscr{C} \times_T \operatorname{Spec} K \arrow[ur, "\Phi|_{\mathscr{C} \times_T \operatorname{Spec} K}"'] & \end{tikzcd}$$

and χ restricted to the closed point of R is one of the curves given by Construction 3.7. Let $\eta \in \mathscr{D}$ be the generic point of one of the irreducible components of $\mathscr{D}_\kappa$. Consider the proper morphism $g : Y \times_{\mathbf{P}^1} \operatorname{Spec} \mathscr{O}_{\mathscr{D},\eta} \to \operatorname{Spec} \mathscr{O}_{\mathscr{D},\eta}$. By construction there is a section of g over the generic point of $\operatorname{Spec} \mathscr{O}_{\mathscr{D},\eta}$, so by the valuative criterion of properness there is a section of g. Evaluating g at η (and extending to a section again using the valuative criterion of properness) yields a morphism $\mathbf{P}^1_\kappa \to Y_\kappa$ giving a section of $Y_\kappa \to \mathbf{P}^1_\kappa$. Since the base field is algebraically closed, it follows from standard limiting and specialization arguments (write κ as a direct limit of finite-type k-algebras, etc.) that the existence of a section over κ implies the existence of a section over k.

The strategy employed by Graber, Harris, and Starr is thus to find a multisection $C \subset Y$ whose deformations inside Y dominate $F \subset \mathscr{M}_{g,0}(\mathbf{P}^1, e[\mathbf{P}^1])$. Now, a random curve C will *not* have enough deformations in Y to dominate F. But we can make curves of genus g that admit larger deformation spaces when we know that the general fibers of f are rationally connected. Here is how: given $C \subset Y$, choose points $c_1, \ldots, c_n$ which lie in general (smooth rationally connected) fibers $Y_1, \ldots, Y_n$. Since the Y_i are rationally connected, there are many rational curves R_i on Y_i through c_i (in fact, the rational curves generate the tangent space to Y_i at c_i) such that the tangent bundle T_{Y_i} is ample when restricted to R_i. Given such curves $R_1,\dots,R_n$, we can form the nodal union $C' = C \cup R_1 \cup \cdots \cup R_n$, which gives a stable map to Y. Since each R_i is rational, C' still has genus g. Moreover, one can show that given m, for sufficiently large n we have that the normal sheaf $\mathscr{N}_{f'}$ to the map $f' : C' \to Y$ is generated by global sections taking any prescribed values on m smooth points $q_1,\dots,q_m$ of C', and that $\mathrm{H}^1(C', \mathscr{N}_{f'}(-q_1 - \cdots - q_m)) = 0$. The latter group is the group of obstructions to deforming C' as a Y-scheme; combining both calculations, we see that $C' \to Y$ deforms to a stable map $C'' \to Y$ with C'' smooth and finite of degree e over $\mathbf{P}^1$. Moreover, this map has the property that its deformations will induce arbitrary deformations (in Y) of m fixed points.

Now, if there happens to be such a deformation $C'' \to Y$ which is ramified over $\mathbf{P}^1$ at $2e+2g-2$ points (so that the ramification is simple – only two sheets come together at each point), then this high degree of deformability shows that the deformations of C'' in Y are dominant over the component $F \subset \mathscr{M}_{g,0}(\mathbf{P}^1, e[\mathbf{P}^1])$, allowing us to conclude as in the second paragraph above. Producing such a curve in Y that is only mildly ramified over $\mathbf{P}^1$ is beyond the scope of this survey and the reader is referred to Sect. 3 of Graber et al. [5] for the details.

This proves Theorem 3.9 when the base curve is $\mathbf{P}^1$. As observed by de Jong, generalizing the result to other base curves B is a triviality using the technique of Weil restriction: choose a finite generically étale morphism $\pi : B \to \mathbf{P}^1$ and consider the variety $\pi_* Y$ whose functor of points sends $T \to \mathbf{P}^1$ to $\mathrm{Hom}_B(T \times_{\mathbf{P}^1} B, Y)$. One checks that $\pi_* Y$ is indeed a variety (e.g., it is a proper algebraic space with a finite cover by a projective scheme) with a proper morphism $\pi_* Y \to \mathbf{P}^1$. The description of the functor of points shows that for a general point $p \in \mathbf{P}^1$ with preimages $\{q \in B\}$, the fiber of $\pi_* Y$ over p is isomorphic to $\prod Y_q$. Thus, $\pi_* Y \to \mathbf{P}^1$ has rationally connected geometric generic fiber. Since $\pi_* Y(\mathbf{P}^1) = Y(B)$, the result follows. $\square$

The short form of the proof. Attach vertical rational curves to a multisection so that it deforms enough to break into a union of sections (and possibly a few vertical components). This combines the techniques of deforming off of the boundary (smoothing the singular curve) and degenerating to the boundary (following the moving curve to the nice part of the boundary of $\overline{\mathscr{M}}_{g,0}(\mathbf{P}^1, e[\mathbf{P}^1])$ which consists of singular curves containing sections). Continuing along these lines, one can in fact see that there are many sections of the morphism, with any nonempty open subscheme of Y containing infinitely many sections [8, Theorem IV.6.10].

As we have seen, "degenerating to the boundary" is a way of carrying complex information into a simpler situation (and therefore achieving greater understanding using the surplus). As another illustration of this principle, we conclude this section by describing the mapping space to a point: the moduli space $\mathscr{M}_g$ of curves of genus g. In particular, we will sketch the basic idea of Deligne and Mumford's proof that $\mathscr{M}_g$ is geometrically irreducible. The proof is an archetype: one compactifies the moduli space by enlarging the moduli problem, and the boundary then endows the moduli problem with an inductive structure in which the interiors of "lower" problems appear as boundary strata of "higher" problems, allowing a transfer of information up the chain and (in many cases) resulting in an irreducibility proof. This kind of inductive structure is ubiquitous in the study of moduli and will appear in the next section when we discuss de Jong and Starr's theory of porcupines.

Theorem 3.10 (Deligne–Mumford). *The space $\mathscr{M}_g$ parameterizing smooth curves of genus g is geometrically irreducible.*

Note that as stated this is not a theorem about the space of stable curves, only about the space of smooth curves. In fact, the space of stable curves was introduced to compactify the space of smooth curves in such a way that the argument we sketch here (using the inductive structure of the compactification) would be possible. Here is how it works. Assume that $g > 1$:

Step 1. Embed $\mathscr{M}_g$ as an open subspace of the space $\overline{\mathscr{M}}_g$ of stable curves of genus g.

Step 2. Show that the embedding from step 1 is dense, and never an isomorphism. We can accomplish both of these things by studying the deformation theory of singular stable curves. For example, a nodal union E of a curve of genus $g-1$ with a curve of genus 1 will be a stable curve of genus g. We can smooth such a nodal union by using infinitesimal deformation theory: the formal smoothing of a node works just as in the blowup picture in Degeneration 3.1. On the other hand, the infinitesimal deformation theory of the curve E maps to the infinitesimal deformation theory of a node. One checks using abstract nonsense that this map is formally smooth. This says that a formal smoothing of the node can be extended to a formal smoothing of E. More generally, one can make this argument for any stable curve. Thus, there are singular stable curves, and any singular stable curve can be deformed to a smooth one. This shows that the inclusion is dense and never an isomorphism, as desired.

It is worth making this more precise, as it gives another illustration of basic deformation theory. For the sake of simplicity, we will study deformations over the bases S_n used in Sect. 2.

Proposition 3.11. *Let $X \to S_{n-1}$ be a flat morphism of finite type with X_0 a curve with at worst nodal singularities. Then*

1. *There is no obstruction to deforming X to a flat scheme over S_n.*
2. *The space of deformations is a principal homogeneous space under the group* $\mathrm{Ext}^1(\Omega_{X_0}, \mathscr{O}_{X_0})$. *Moreover, this description is functorial in local immersions on X.*

Given a stable curve C with nodal locus N, applying the proposition to C and the localization of C at N, and noting (via the spectral sequence connecting local to global Ext) that $\mathrm{Ext}^1(\Omega_C, \mathscr{O}_C)$ is concentrated on N, gives the statement on surjectivity and formal smoothness of the restriction map on infinitesimal deformation theories. More precisely, writing $\mathscr{F}_{C,N}$ for the restriction of a coherent sheaf $\mathscr{F}$

on C to the semilocal ring $\mathscr{O}_{C,N}$, the spectral sequence and vanishing of H^2 give a surjection (as an edge map)

$$\mathrm{Ext}^1(\Omega_C, \mathscr{O}_C) \to \mathrm{H}^0(C, \mathscr{E}xt^1(\Omega_C, \mathscr{O}_C)) = \mathrm{Ext}^1(\Omega_{C,N}, \mathscr{O}_{C,N})$$

which one checks corresponds to the natural restriction map, which in turn corresponds to the restriction of infinitesimal deformation theories. The rest (smoothing the node and following this by a smoothing of the curve C) uses the second pillar: results similar to those of Proposition 3.2 for the integration of infinitesimal deformations of curves (instead of morphisms).

Step 3. Show that the space $\overline{\mathscr{M}}_g$ is proper (in fact, projective). This is the famous stable reduction theorem.

Step 4. Show that the space $\overline{\mathscr{M}}_g$ is normal (in fact, has finite quotient similarities). This is a formal consequence of the fact that the infinitesimal deformation theory of a curve is formally smooth; a proper understanding of this point uses the theory of stacks.

Step 5. To show that a normal variety is irreducible, it suffices to show that it is connected. In other words, to show that $\mathscr{M}_g$ is irreducible, it is enough to show that given two points a and b of $\mathscr{M}_g$, there is a connected curve C in $\overline{\mathscr{M}}_g$ which contains a and b.

Step 6. To produce such a path, we proceed as follows. The point a parameterizes a smooth curve D of genus g. Using a stable reduction theorem, we can degenerate D to a nodal union D_0 of curves of lower genera; this degeneration connects D to D_0 by a curve in $\overline{\mathscr{M}}_g$. We can do a similar thing for the curve D' parameterized by b, yielding another singular curve D'_0. On the other hand, by induction we know that the moduli spaces $\mathscr{M}_h$ with $h < g$ are irreducible. Taking enough care with the degenerations, we can use this inductive fact to prove that there is a curve in $\overline{\mathscr{M}}_g$ connecting D_0 to D'_0.

Step 7. We are done! (Obviously, there are many technical details that are left out of this sketch. In particular, we did not explain how to do the degenerations properly to ensure that the limits are connected by a curve in a simple way.) We follow the same basic pattern as in the Graber–Harris–Starr theorem: we combined degenerating to the boundary with deformation off of the boundary to connect together points in the open moduli problem that was originally of interest to us.

In Sect. 4, we will see another technique for putting an inductive structure on a moduli problem. While the problem in question is a moduli problem of stable maps, the inductive structure on the problem is actually more reminiscent of what happens for the moduli of vector bundles on algebraic surfaces: the structural results described (irreducibility, rational connectivity) only hold asymptotically in a discrete parameter (in contrast to the irreducibility of $\mathscr{M}_g$ for any genus g). For moduli problems of this type, the inductive structure involves an increasing understanding of the problem as one ascends the chain of moduli spaces, and not merely a transfer of perfect information from lower problems to higher ones.

4 Moduli of Porcupines and Rational Sections of Rationally Simply Connected Fibrations over Surfaces

In this section, we fix a smooth projective surface S over k. Our goal is to understand when there exists a rational section to a morphism $f : X \to S$ whose fibers are sufficiently rationally connected. As explained in Sect. 1, there are many rationally connected fibrations over S which lack rational sections. If we suppose for a moment that X and S are CW complexes with S two dimensional, then a consideration of the long exact sequence in homotopy associated to a fibration shows that if the fibers of f are simply connected, then there is no topological obstruction to lifting the largest cells of S into X. This is not meant to give any kind of an argument in the classical complex topology; for example, the dimensions are wrong. Instead, this is meant to inspire us to think of what it should mean for the fibers of f to be simply connected in some algebraic sense. Ultimately, de Jong and Starr came up with a careful list of hypotheses that seem to express simple connectivity in the context of rational curves.

To motivate the definition, let us consider an approach to finding sections to f. Let $C \subset S$ be a general smooth curve. (Here "general" can be taken to mean that the fiber of f over C still has smooth total space and rationally connected geometric generic fiber.) By the Graber–Harris–Starr theorem, the restriction f_C has many sections. In fact, there is a moduli space $\Sigma(X_C/C) \to \operatorname{Spec} k$ parameterizing sections. Moreover, this moduli space varies nicely as C varies. (Of course, $\Sigma(X_C/C)$ can be complicated – it can have many connected components, etc. – but we still get a reasonable family of such moduli spaces as the curve C moves in S.) The question is: how can we properly formulate what it would mean to make a family of sections of f over a variable curve C?

There is a well-known resolution of this type of question which illustrates the power of Grothendieck's theory of generic points. Suppose the curve C is a member of a very ample linear system on S. We can choose two members C_1 and C_2 of the linear system $|C|$ which are smooth and intersect transversely in the locus of S over which f is smooth. The total space $\tilde{S}$ of the pencil spanned by C_1 and C_2 will be the blowup of S in the intersection $C_1 \cap C_2$. Since $\tilde{S}$ and S are birational, to find a rational section of f it is enough to find a rational section of the pullback of X to $\tilde{S}$. On the other hand, there is a natural proper flat generically smooth morphism $\tilde{S} \to \mathbf{P}^1$. Thus, we may assume that our original base surface S fibers are a family of curves over $\mathbf{P}^1$; this expresses our surface as the total space of a moving family of curves.

Now, what does it mean to paste together sections of the fibration over these curves? Such a compatible family of sections should be precisely a section of the fibration $X \to S$ over the generic member of the family parameterized by $\mathbf{P}^1$. In other words, it should be a section of the restriction of f to the generic fiber of $\tilde{S} \to \mathbf{P}^1$. This generic fiber is a proper smooth geometrically connected curve C over the field $k(t)$.

To summarize: we can solve our original problem if we can solve the analogous problem for fibrations $f : X \to C$ with proper smooth rationally simply connected fibers over curves, but now over the base field $k(t)$. Associated to the fibration f is a moduli space $\Sigma \to \operatorname{Spec} k(t)$ parameterizing sections. If we knew that suitable components of Σ were rationally connected, then we could apply the Graber–Harris–Starr theorem to conclude a section exists. This is precisely what de Jong and Starr do. What is perhaps more interesting, they deduce the rational connectivity of certain spaces of sections from a condition on the generic fiber of f which is analogous (by a loose topological analogy) to the path connectedness of spaces of paths between two points (where now a space of paths is to be interpreted as a space of rational curves, and path connectedness is to be interpreted as rational connectedness).

With this introduction, we are now ready to put some conditions on f which will allow us to make all of this (more) rigorous. We will suppose the following. (de Jong and Starr allow more general hypotheses, but nothing essential about their argument is changed by using the stricter hypotheses we have chosen here.)

Hypothesis 1. The morphism $f : X \to C$ is a proper flat morphism of smooth geometrically connected varieties over $k(t)$. Following Jason Starr's notes [14], we will write Y for the geometric generic fiber of f (so Y is a variety over $K = \overline{k(C)}$).

Hypothesis 2. There is an invertible sheaf $\mathscr{L}$ on X which is ample and globally generated.

Hypothesis 3. The restriction $\mathscr{L}|_Y$ is very ample.

Hypotheses 2 and 3 together say that $\mathscr{L}$ defines a morphism to a projective space and that this morphism restricted to a general fiber is finite. There may be "horizontal" collapsing induced by the map, but no curve in a general fiber is collapsed.

To state the rest of the hypotheses, we first need to develop a small amount of theory. For the moment, let us work with the geometric generic fiber; thus, we restrict our attention to the variety Y over the field K. Since $\mathscr{L}$ is very ample on Y, we can imagine Y embedded in some $\mathbf{P}^N$ in such a way that $\mathscr{L}$ is the restriction of $\mathscr{O}(1)$. Any curve $D \subset Y$ has a degree (via the induced embedding in $\mathbf{P}^N$). The curves of degree 1 in Y are precisely the lines in $\mathbf{P}^N$ which lie in Y. For historical reasons (and to harmonize our notation with that of Starr), we will denote the space of pairs (L, p) with L a line in Y and p a point of L by $\overline{\mathscr{M}}_{0,1}(Y/K, 1)$. Since lines cannot degenerate, the space is actually projective. There is a natural morphism $\mathrm{ev} : \overline{\mathscr{M}}_{0,1}(Y/K, 1) \to Y$ which is defined by sending a pair (L, p) to the point $p \in Y$.

Recall the following definition.

Definition 4.1. A closed subscheme $Z \subset W$ of a smooth variety is *free* if the restriction $T_W|_Z$ is globally generated.

Following de Jong and Starr, given a natural number n, a *chain of n-free lines* is a sequence of triples (L_i, p_i, q_i) with each L_i a free line in Y and p_i and q_i two points of L_i, such that for each i we have that $q_{i-1} = p_i$, with this intersection point being a node of the total curve given by the union of the L_i. It is easy to see that there is a quasiprojective K-scheme $F_2(Y/K, n)$ parameterizing chains of n-free lines, with

p_1 and q_n marked on the total curve. This again comes with an evaluation morphism $\mathrm{ev} : F_2(Y/K,n) \to Y \times Y$ given by evaluating maps at p_1 and q_n.

Using these two evaluation morphisms, we can state the next two hypotheses:

Hypothesis 4. The evaluation morphism $\overline{\mathscr{M}}_{0,1}(Y/K,1) \to Y$ is surjective, the geometric generic fiber is irreducible and rationally connected, and the fibers over codimension one points of Y are only allowed to be mildly singular (in a fashion which de Jong and Starr make precise).

Hypothesis 5. For some natural number n, the evaluation morphism $F_2(Y/K,n) \to Y \times Y$ is dominant, and the geometric generic fiber is isomorphic to an open subscheme of a projective rationally connected scheme.

To state the final hypothesis, I need to remind you of one more geometric object. A *scroll* in a projective space $\mathbf{P}^N$ is a smooth surface $R \subset \mathbf{P}^N$ together with a smooth morphism $R \to \mathbf{P}^1$ whose fibers are lines.

Hypothesis 6. There is a very twisting scroll in Y. This is a special type of scroll $R \subset Y$ which comes with a section, the whole package required to satisfy some cohomological conditions. In particular, R should be free in $\mathbf{P}^1 \times Y$ (in the sense of Definition 4.1). (There is more, and the meaning is very clearly explained in the lecture notes of Starr [14].)

As Starr points out, all of these hypotheses are necessary for the veracity of the theorem which we will ultimately state. The reader should know that these hypotheses are algebraic analogues of natural topological conditions: Hypothesis 4 says that the space of paths through point is path connected (a trivial hypothesis in usual topological settings), while Hypothesis 5 says that the space of paths connecting two points is itself path connected (which is equivalent to being simply connected in the usual topological settings). The fact that Hypothesis 6 has no reasonable (nontautological) topological analogue gives an indication of the complexity of the algebraic situation.

Before I can state the theorem, I need to introduce one more object: the Abel map on the space of stable sections. Using the invertible sheaf $\mathscr{L}$, we can define a degree for any stable map $D \to X$: we simply compute the degree of the preimage of $\mathscr{L}$ on D.

Definition 4.2. Given $f : X \to C$ as above, a *stable section of degree e* is a stable map $\varphi : D \to X$ of degree e together with a section $\sigma : C \to D$ of the induced morphism $f \circ \varphi$ such that $D \setminus \sigma(C)$ maps entirely into a finite closed subscheme of C.

It is relatively easy to see that stable sections of degree e form a projective moduli space, which we will denote $\Sigma^e(X/C/k(t))$. Colloquially, we get $D \to X$ by taking a section of f and attaching some vertical components in the fibers of f. The horizontal component is referred to as the "handle" of the stable map. Among the stable sections of f of degree e are those which are actually sections $C \to X$ whose degree is e. The sections form an open subscheme which we will denote $S^e(X/C/k(t))$. Note that $S^e(X/C/k(t))$ is nonempty by Theorem 3.9.

Pulling back $\mathscr{L}$ defines a morphism $S^e(X/C/k(t)) \to \mathrm{Pic}^e_{C/k(t)}$. It turns out that this morphism extends to all of $\Sigma^e(X/C/k(t))$. (While the handle of a stable section has lower degree, the vertical components make up the difference.) This morphism

$$\alpha : \Sigma^e(X/C/k(t)) \to \mathrm{Pic}^e_{C/k(t)}$$

is called the *Abel map* associated to $(X, \mathscr{L}, f)$. Since abelian varieties contain no nontrivial rational curves, any statement we make about rational connectivity of spaces of sections will have to be about fibers of the morphism α.

We are now in a position to state a theorem, and see how it implies the existence of rational sections for fibrations over algebraic surfaces.

Theorem 4.3 (de Jong–Starr). *Suppose the triple $(X, \mathscr{L}, f)$ satisfies Hypotheses 1–6. For all sufficiently large e, there is a geometrically irreducible component Z_e of $\Sigma^e(X/C/k(t))$ such that:*

1. *A general point of Z_e corresponds to a free section of f.*
2. *The restriction of the Abel map $\alpha|_{Z_e} : Z_e \to \mathrm{Pic}^e_{C/k(t)}$ is surjective with rationally connected irreducible geometric generic fiber.*

As we will see below, there is a fairly explicit description of the irreducible component Z_e using porcupines. But before we give the (mildest) indication of how one proves such a theorem, let me show you how to deduce the existence of rational sections from this theorem.

Proposition 4.4 (de Jong–Starr). *Suppose $f : X \to S$ is a proper morphism of smooth k-varieties with S a smooth projective connected surface and $\mathscr{L}$ is an invertible sheaf on X. Suppose there is an open subscheme $U \subset S$ which is the complement of finitely many closed points such that $f|_U$ is smooth and $\mathscr{L}|_U$ is ample and globally generated relative to $f|_U$. Finally, suppose the geometric generic fiber of f and the invertible sheaf $\mathscr{L}$ restricted to the geometric fiber satisfy Hypotheses 3–6. Then there is a rational section of f.*

Proof. As in the beginning of the section, choosing a pencil of sufficiently ample divisors on S reduces us to the situation we have been studying: we have a proper smooth morphism $f : X \to C$ with C a proper smooth curve over $k(t)$ with a rational point p. In particular, for any natural number e, there is a divisor $e[p]$ of degree e on C, so that $\mathrm{Pic}^e(C)$ is nonempty. On the other hand, by Theorem 4.3, for all sufficiently large e, the general fiber of the Abel map $Z_e \to \mathrm{Pic}^e_{C/k(t)}$ is irreducible and rationally connected. By the Graber–Harris–Starr theorem, we thus see that a general $k(t)$-point of $\mathrm{Pic}^e_{C/k(t)}$ will lift to a point of Z_e. Taking the handle of the stable section corresponding to this point gives a section of f, and therefore a rational section of the original morphism $X \to S$, as desired. There is one technical point: we do not know that there is such a thing as a general $k(t)$-point of $\mathrm{Pic}^e_{C/k(t)}$! However, it turns out that there is a relatively standard (but technical) trick to overcome this difficulty. It relies on the following lemma.

Lemma 4.5. *Suppose k is an algebraically closed field of characteristic 0. Suppose* $\mathrm{Spec}\,A$ *is an affine $k[[s]]$-scheme with geometrically integral generic fiber such that there is a point* $\xi \in \mathrm{Spec}(A \otimes_R k) \subset \mathrm{Spec}\,A$ *for which the local ring A_ξ is a dvr with uniformizer s. Write $R = k[[s]]$ and $K = k((s))$.*

If $W \to \mathrm{Spec}\,A$ is a proper scheme such that $W \otimes_R \overline{K}$ admits a rational section over $\mathrm{Spec}\,A \otimes_R \overline{K}$*, then $W \times_{\mathrm{Spec}\,A} \xi \to \xi$ has a rational point.*

Before proving the lemma let us first see how this applies. We return to the global situation with C the generic fiber of a morphism $S \to \mathbf{P}^1$, $\mathrm{Pic}^e_{C/k(t)}$ the generic fiber of the relative Picard family $\mathrm{Pic}^e_{S/\mathbf{P}^1}$, and $\alpha : \widetilde{Z}_e \to \mathrm{Pic}^e_{S/\mathbf{P}^1}$ the Abel map (so that Z_e is the generic fiber of $\widetilde{Z}_e$ over $\mathbf{P}^1$). (For our purposes, $\widetilde{Z}_e$ can be any extension of Z_e to a proper $\mathbf{P}^1$-scheme over which α extends.) By assumption, the geometric generic fiber of α is rationally connected, which implies that there is a dense open subscheme $O \subset \mathrm{Pic}^e_{S/\mathbf{P}^1}$ over which the fibers of α are rationally connected. In particular, a curve in $\mathrm{Pic}^e_{S/\mathbf{P}^1}$ moving in a sufficiently large family will have a general deformation intersecting O.

Given a section $\sigma : \mathbf{P}^1 \to \mathrm{Pic}^e_{S/\mathbf{P}^1}$, we can think of the image as a component of a complete intersection of hyperplane sections of $\mathrm{Pic}^e_{S/\mathbf{P}^1}$ in some projective embedding, whereupon we see that there is a family of curves whose general member is smooth and intersects O. Choose an affine open subscheme $\mathrm{Spec}\,A$ of the total space of this family of curves which contains the generic point of $\mathbf{P}^1$ (viewed as a component of the special fiber of the family). The map $\mathrm{Spec}\,A \to \mathrm{Pic}^e_{S/\mathbf{P}^1}$ gives a map $\mathrm{Spec}\,A \to \mathbf{P}^1$, so we can pull back the morphism $X \to S$ to get a family of morphisms to fibered surfaces $\mathscr{X} \to \mathscr{S} \to \mathrm{Spec}\,A$ parameterized by $k[[t]]$. By the assumption on the generic fiber of $\mathrm{Spec}\,A$ over $k[[t]]$, the associated scheme of stable sections $\Sigma^e(\mathscr{X}/\mathscr{S}/A)$ has a point over $\overline{K}$. By Lemma 4.5, it has a point over $\mathbf{P}^1$, whose restriction to the generic point $\mathrm{Spec}\,k(t)$ gives rise to a stable section of X/C. Taking the handle gives the desired result.

It remains to prove Lemma 4.5.

Proof of Lemma 4.5. We know that the algebraic closure of $K = k((s))$ is the union of the extensions $k((s^{1/N}))$. Thus, if W has a rational section over $A \otimes_R \overline{K}$, then it has one over $A \otimes_R k((s^{1/N}))$ for some N. The point ξ lifts to a point of $\mathrm{Spec}\,A \otimes_R k[[s^{1/N}]]$ for which $s^{1/N}$ is a uniformizer. By the valuative criterion of properness, the generic point of the section of $W \otimes_R k[[s^{1/N}]] \to \mathrm{Spec}\,A \otimes_R k[[s^{1/N}]]$ extends to give a section over ξ, as desired. □

This completes the proof of Proposition 4.4. The reader is referred to the proof of Corollary 9.1 of Starr [14] for more details. □

One fact which makes this theorem especially interesting is the following.

Proposition 4.6 (de Jong–He–Starr). *Suppose Y is a smooth connected projective k-scheme which is a homogeneous space for a linear algebraic group scheme G. If there is an ample generator $\mathscr{L}$ for* $\mathrm{Pic}(Y)$*, then the pair $(Y, \mathscr{L})$ satisfies Hypotheses 3–6. Thus, if $f : X \to S$ is a proper smooth morphism to a smooth projective* *surface whose generic fiber is such a homogeneous space, and if $\mathscr{L}$ is an invertible sheaf on X whose restriction to the geometric generic fiber is ample generator for the Picard group, then f has a rational section.*

Combining this proposition with work of de Jong and Starr on "discriminant avoidance" gives a proof of Serre's conjecture II on the triviality of torsors under connected, simply connected, semisimple linear algebraic groups over function fields of surfaces. This connection is described in "Serre's Conjecture II: A Survey."

I will now give a very mild indication of the techniques that go into proving some of these results. This is by no means meant to be detailed or complete. The reader is referred to the exhaustive notes of Starr, and the paper by de Jong, He, and Starr recently posted to the archive [14, 15]. In particular, we will usually flagrantly ignore technical hypotheses (often with parenthetical remarks). No proofs will be found anywhere. *Every idea described here is due to de Jong and Starr. I claim no originality except in the order of presentation and the decision to omit several important pieces of the argument*!

The idea of the proof of Theorem 4.3 uses an idea going back to O'Grady's study of the moduli spaces of sheaves on a surface. Here is the general principle: suppose we have defined a sequence of quasicompact moduli spaces M_e over the algebraic closure $\overline{k(t)}$, indexed by the natural numbers. Suppose, furthermore, that we have a geometric construction which associates to each irreducible component of M_e an irreducible component of M_{e+1} in a way compatible with the Galois action. Write $\xi(e)$ for the (Galois) set of irreducible components of M_e; by abuse of notation, we will write $\Phi : \xi(e) \to \xi(e+1)$ for each of the Galois-equivariant maps induced by the geometric construction in question. If we know that Φ is surjective and that any two elements of $\xi(e)$ are eventually brought together by some iterate of Φ, then we know that for sufficiently large indices e, the set $\xi(e)$ consists of a single Galois-invariant element, that is, that M_e is geometrically irreducible.

To produce the spaces M_e, we will take the unique components containing certain special loci of stable sections, called *porcupines*. These are "free enough" sections of f glued to lines in fibers. Let us make this precise.

Definition 4.7. A section $\sigma : C \to X$ is (g)-free if for some $d \geq \max\{2g, 1\}$ and every effective Cartier divisor D in C of degree d, we have that

$$\mathrm{H}^1(C, \sigma^* N_{\sigma(C)/X}(-D)) = 0.$$

Definition 4.8. A point $x \in X$ is *peaceful* if:

1. x is a smooth point of the morphism f.
2. Given a line L in $f^{-1}(f(x))$ through x, any infinitesimal deformation of x is contained an infinitesimal deformation of L.

Definition 4.9. A *porcupine* (of genus g) is a stable section $C' \to X$ of genus g such that the associated section $C \to C' \to X$ is (g)-free and all of the irreducible components of $\{C' \setminus C\}^-$ are lines in fibers of f whose attachment points to the section are peaceful points of X.

The vertical lines attached to the (g)-free section are called *quills*.

Since a porcupine fibers by lines over C, it is natural to consider those scrolls in X which contain a given porcupine.

Definition 4.10. A porcupine is *penned by a scroll* R if it is contained in R.

Porcupines form an open subscheme $P^e(X/C/k(t))$ of the scheme of stable sections. We will write $P^{e,\delta}(X/C/k(t))$ for the space of porcupines of degree e which have exactly δ quills and $P^{e,\geq\delta}(X/C/k(t))$ for the space of porcupines with at least δ quills. It turns out that $P^{e,\geq 1}(X/C/k(t))$ is a snc divisor in $P^e(X/C/k(t))$, and the spaces $P^{e,\delta}(X/C/k(t))$ give the natural locally closed stratification of the smooth space $P^e(X/C/k(t))$ coming from the divisor. In particular, each $P^{e,\delta}(X/C/k(t))$ is a locally closed smooth subscheme with an open neighborhood in $\Sigma^e(X/C/\overline{k(t)})$ that is smooth, and therefore any irreducible component of $P^{e,\delta}(X/C/k(t))\otimes\overline{k(t)}$ is contained in a unique irreducible component of $\Sigma^e(X/C/k(t))\otimes\overline{k(t)}$. Forgetting quills defines a smooth dominant morphism $P^{e,\delta}(X/C/k(t))\to P^{e-\delta}(X/C/k(t))$ with geometrically irreducible fibers. (See [14, 15] for proofs of these statements.)

Of course, the preceding paragraph would be nonsense if we did not know that porcupines exist, but in fact they do: there is a (g)-free section of $f\otimes\overline{k(t)}$ which intersects the peaceful locus of X. Thus, there is a natural number e_0 such that $P^{e_0,0}(X/C/k(t))$ is nonempty. We can now define our sequence of spaces.

Sequence 4.11 (M_e). For $e\geq e_0$, we let M_e be the union of those irreducible components of $\Sigma^e(X/C/k(t))$ containing the smooth locus $P^{e,e-e_0}(X/C/k(t))$.

In particular, M_{e_0} is the closure of $P^{e_0,0}(X/C/k(t))$ in $\Sigma^{e_0}(X/C/k(t))$, which is the set of components generically parameterizing a (g)-free section. We do not claim that M_{e_0} is geometrically irreducible. (This is a slightly different presentation of the results of Starr [14] and Starr et al. [15], where they work with a sequence of irreducible components over $\overline{k(t)}$ and show that eventually they are Galois-stable.)

Let $\xi(e)$ be the set of irreducible components of $M_e\otimes\overline{k(t)}$. This is a finite discrete set with continuous $\mathrm{Gal}(\overline{k(t)}/k(t))$-action. Define a map $\Phi:\xi(e)\to\xi(e+1)$ as follows.

Map 4.12 ($\Phi:\xi(e)\to\xi(e+1)$). Given a component Z_e of $M_e\otimes\overline{k(t)}$ corresponding to an element $[Z_e]\in\xi(e)$, choose a porcupine C' parameterized by Z_e. Fix a general peaceful point c in the handle D and attach a line L in $f^{-1}f(c)$ to C' at c. This defines a new porcupine C'' of degree $e+1$ with $e-e_0+1$ quills, which thus lies in a unique irreducible component Z_{e+1} of M_{e+1} (as it is a smooth point).

Lemma 4.13. *The map Φ is well defined and Galois equivariant.*

Sketch of proof. The peaceful point of attachment moves in an irreducible family (as the peaceful locus is open), and the space of lines in fibers through a general point is irreducible by Hypothesis 4 and smooth over the attachment point (by the definition of peaceful), so that different versions of this construction (as we vary the porcupine C' and the newly attached line) move in an irreducible family and thus will not leave the component Z_{e+1}. For the same reasons, the construction is Galois equivariant. $\square$

We claim that Φ is a contracting map, in the following sense.

Theorem 4.14. *Given $a, b \in \xi(e)$, there is a natural number m such that $\Phi^{\circ m}(a) = \Phi^{\circ m}(b)$.*

Before discussing Theorem 4.14, let us see an immediate consequence.

Corollary 4.15. *For all sufficiently large e, the space M_e is geometrically irreducible.*

Proof. Indeed, since $\xi(e_0)$ is finite, there is an iterate $\Phi^{\circ M}$ such that $\Phi^{\circ M}(\xi(e_0))$ is a Galois-invariant singleton, that is, corresponds to a geometrically irreducible component. On the other hand, Φ is surjective by the construction of M_e, so for all $e \geq e_0 + M$ we see that $\xi(e)$ is a singleton, which shows that M_e is geometrically integral for all $e \geq e_0 + M$. □

The proof of Theorem 4.14 is somewhat subtle. The idea is to choose general points of a and b and show that porcupines formed by attaching sufficiently many quills (corresponding to sufficiently large iterates $\Phi^{\circ m}(a)$ and $\Phi^{\circ m}(b)$) are connected by a chain of rational curves. However, rational curves can only connect points in a common fiber of the Abel map. We proceed in two steps: we first show (over $\overline{k(t)}$) that the Abel map is dominant with irreducible fibers on each irreducible component, and then we show that two porcupines with the same Abel image are connected by a chain of rational curves with nodes in the smooth locus of the space of stable sections.

Proposition 4.16. *For sufficiently large e, the Abel map*

$$\alpha : M_e \otimes \overline{k(t)} \to \mathrm{Pic}^e_{C/k(t)} \otimes \overline{k(t)}$$

has the property that the restriction of α to each irreducible component of $M_e \otimes \overline{k(t)}$ is dominant with geometrically irreducible generic fiber.

Idea of proof. There is a beautiful trick here: fix a component Z_e of $M_e \otimes \overline{k(t)}$. Since the porcupines are smooth points of Z_e, to show that $\alpha|_{Z_e}$ is dominant with geometrically irreducible generic fiber, it suffices to prove the statement for the locus of porcupines $W \subset Z_e$. It is now relatively easy to analyze the Abel map: taking the body and quill attachment points gives a map $W \to Z_{e_0} \times \mathrm{Sym}^{e-e_0}(C)$, where Z_{e_0} is now a smooth scheme parameterizing free sections (the image of Z_e in $M_{e_0} \otimes \overline{k(t)}$ under the natural rational map). This is smooth and dominant with geometrically irreducible fibers by Hypothesis 4 and the definition of peaceful.

The Abel map factors through the product

$$\begin{array}{ccc} Z_{e_0} \times \mathrm{Sym}^{e-e_0} C \longrightarrow Z_{e_0} \times \mathrm{Pic}^{e-e_0}_{C\otimes\overline{k(t)}/\overline{k(t)}} & & \\ \big\downarrow & & \\ \mathrm{Pic}^{e_0}_{C\otimes\overline{k(t)}/\overline{k(t)}} \times \mathrm{Pic}^{e-e_0}_{C\otimes\overline{k(t)}/\overline{k(t)}} & \longrightarrow & \mathrm{Pic}^{e}_{C\otimes\overline{k(t)}/\overline{k(t)}}, \end{array}$$

where the first map is the divisor class map and the last is the tensor product of invertible sheaves. For large enough e, the divisor class map is smooth and surjective.

Fix $s \in Z_{e_0}$ with Abel image $L \in \mathrm{Pic}^{e_0}_{C\otimes\overline{k(t)}/\overline{k(t)}}(\overline{k(t)})$. Translating by elements of Pic^{e-e_0} covers Pic^e, so the composition of the latter two maps is surjective. On the other hand, fixing $L \in \mathrm{Pic}^{e}_{C\otimes\overline{k(t)}/\overline{k(t)}}(\overline{k(t)})$ and $s \in Z_{e_0}$, there is a unique $L' \in \mathrm{Pic}^{e-e_0}_{C\otimes\overline{k(t)}/\overline{k(t)}}(\overline{k(t)})$ such that $L' + \alpha(s) = L$, namely $L - \alpha(s)$! This shows that the fibers of the composition are in bijection with Z_{e_0}, hence geometrically irreducible.

Combining the statements shows that the Abel map on W is dominant with geometrically irreducible generic fiber, as desired. □

Corollary 4.17. *For sufficiently large e, a general point of any irreducible component of $M_e \otimes \overline{k(t)}$ maps to a general point of* $\mathrm{Pic}^e_{C/k(t)} \otimes \overline{k(t)}$.

Thus, to show that M_e is eventually irreducible, it suffices to look for chains of rational curves connecting porcupines with the same Abel images. The key to carrying this out is contained in the following two results.

Fix a scroll R in X, and suppose $C'_a \to X$ and $C'_b \to X$ are two porcupines of degree e penned by R.

Lemma 4.18. *The Abel images $\alpha(C'_a)$ and $\alpha(C'_b)$ are equal in* $\mathrm{Pic}^e_{C/k(t)}$ *if and only if C'_a and C'_b are linearly equivalent as divisors in R. If the images are equal, then there is a chain of rational curves in $\Sigma^e(X/C/k(t))$ connecting C'_a to C'_b whose nodes lie in the smooth locus.*

Remark 4.19. The reader will note that the chain of curves need not stay in the locus of porcupines. This is why the results mentioned here do not show that the locus of porcupines has rationally connected Abel fibers.

How can we make the divisor classes of C'_a and C'_b equal? By adding quills!

Proposition 4.20. *Suppose D and D' are two general porcupines with the same Abel image. For every sufficiently large natural number e, there is a sequence of porcupines $D_1, D_2, \ldots, D_{n-1}$ of degree e and a sequence of scrolls $R_1, \ldots, R_n$ such that:*

1. *The Abel images of the D_i are all the same.*
2. *D and D_1 are both penned in R_1.*
3. *For $i = 2, \ldots, n-1$, D_{i-1} and D_i are penned in R_i.*
4. *D_{n-1} and D' are penned in R_n.*

Combining this with the lemma, we see that given two general porcupines D and D', up to adding quills to each, we can connect them by a chain of rational curves lying in a single irreducible component of $\Sigma^e(X/C/k(t))$ with nodes at smooth points. This completes the proof of Theorem 4.14.

To complete the proof of Theorem 4.3(2) (that general fibers of the Abel map are rationally connected), we thus need to see how to connect a general point of M_e to a general porcupine with the same Abel image. It is here that one must use the existence of a very twisting scroll in X. In fact, this part of the argument is quite difficult, as one sees must be the case: it requires understanding a general point of the mysterious component M_e, when all we know about is a part of its boundary – the locus of porcupines.

The work of de Jong and Starr is a tour de force of algebraic geometry, and yet it barely scratches the surface of the concept of rational simple connectivity. What is the most general form of the condition? Is there a theorem on the existence of rational sections for fibrations with higher Picard numbers? (What about higher-dimensional bases? Will we soon be reading about connecting "general Dimetrodons" by rational curves?) The recent theorems on rational sections of fibrations are a sign that we have hit a rich seam at the intersection of arithmetic, geometry, topology, and deformation theory. Much digging remains to be done!

Acknowledgements I am grateful to Aise Johan de Jong and Jason Starr for discussing their ideas with me, and to the referee and Jean-Louis Colliot-Thélène for helpful comments and corrections.

References

1. F. Campana. Une version géométrique généralisée du théorème du produit de Nadel. *Bull. Soc. Math. France*, 119(4):479–493, 1991
2. O. Debarre. *Higher-dimensional algebraic geometry*. Universitext. Springer, New York, 2001
3. P. Deligne, D. Mumford. The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.*, 36:75–109, 1969
4. W. Fulton, R. Pandharipande. Notes on stable maps and quantum cohomology. In *Algebraic geometry – Santa Cruz 1995, vol. 62: Proceedings of the Symposium on Pure Mathematics*, pp. 45–96. American Mathematical Society, Providence, RI, 1997
5. T. Graber, J. Harris, J. Starr. Families of rationally connected varieties. *J. Am. Math. Soc.*, 16(1):57–67 (electronic), 2003
6. A. Grothendieck. Techniques de construction et théorèmes d'existence en géométrie algébrique. IV. Les schémas de Hilbert. In *Séminaire Bourbaki*, vol. 6, pages Exp. No. 221, 249–276. Socit Mathmatique de France, Paris, 1995
7. D. Huybrechts, M. Lehn. *The geometry of moduli spaces of sheaves*. Aspects of Mathematics, E31. Friedrick Vieweg & Sohn, Braunschweig, 1997
8. J. Kollár. *Rational curves on algebraic varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete 3, vol. 32. Springer, Berlin, 1996
9. J. Kollár, Y. Miyaoka, S. Mori. Rational curves on Fano varieties. In *Classification of irregular varieties (Trento, 1990), vol. 1515: Lecture Notes in Mathematics*, pp. 100–105. Springer, Berlin, 1992
10. J. Kollár, S. Mori. *Birational geometry of algebraic varieties, vol. 134: Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1998 (translated from the 1998 Japanese original)
11. S. Mori. Projective manifolds with ample tangent bundles. *Ann. Math. (2)*, 110(3):593–606, 1979
12. D. Mumford, J. Fogarty, F. Kirwan. *Geometric invariant theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete (2), 3rd ed., vol. 34. Springer, Berlin, 1994
13. M. Schlessinger. Functors of Artin rings. *Trans. Am. Math. Soc.*, 130:208–222, 1968
14. J. Starr. Rational points of rationally simply connected varieties, 2009 (preprint)
15. J. Starr, A.J. de Jong, X. He. Families of rationally simply connected varieties over surfaces and torsors for semisimple groups, 2009. arXiv:0809.5224

Recent Progress on the Kato Conjecture

Shuji Saito

Summary This is a survey paper on recent works in progress by Jannsen, Kerz, and the author on the Kato conjecture on the cohomological Hasse principle.

This is a survey paper on recent works [17, 19] and a work in progress [19] by Jannsen, Kerz, and the author on the Kato conjecture on the cohomological Hasse principle. In [17, 19], general approaches are proposed to solve the conjecture for schemes over a finite field assuming resolution of singularities. Based on the idea in [19], a new approach is proposed in [24] to solve the conjecture for schemes over a finite field or the ring of integers in a local field, restricted to the prime-to-characteristic part. A key ingredient in [24], which replaces resolution of singularities, is a recently announced result on refined alterations due to Gabber (see [16]). We will give an outline of the proof. As an application, it implies a finiteness result on higher Chow groups of arithmetic schemes using the Bloch–Kato conjecture whose proof has been announced by Rost and Voevodsky ([31, 35], see also [14, 36–38]).

1 Statements of the Kato Conjectures

We start with a review on the following fundamental fact in number theory. Let k be a global field, namely either a finite extension of $\mathbb{Q}$ or a function field in one

Shuji Saito
Graduate School of Mathematical Sciences, University of Tokyo, 3-8-1 Komaba,
Tokyo 153-8914, Japan
e-mail: sshuji@ms.u-tokyo.ac.jp

2010 Mathematics subject classification. 14F20, 14F42, 14G17, 14G26, 11R34.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_6,

variable over a finite field. For simplicity, we assume that $\mathrm{char}(k) > 0$ or k is totally imaginary. Let P be the set of all finite places of k, and denote by k_v the completion of k at $v \in P$. For a field L, let $\mathrm{Br}(L)$ be its Brauer group, and identify the Galois cohomology group $H^1(L, \mathbb{Q}/\mathbb{Z})$ with the group of continuous characters on the absolute Galois group of L with values in $\mathbb{Q}/\mathbb{Z}$:

1. For $v \in P$, there is a natural isomorphism
$$\mathrm{Br}(k_v) \xrightarrow[\alpha_v]{\simeq} H^1(F_v, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\beta_v]{\simeq} \mathbb{Q}/\mathbb{Z},$$
where F_v be the residue field of v and α_v is the residue map and β_v is the evaluation of characters at the Frobenius element.
2. There is an exact sequence
$$0 \to \mathrm{Br}(k) \to \bigoplus_{v\in P} H^1(F_v, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z} \to 0,$$
where the first map is the composite of the restriction maps and α_v and the second map is the sum of β_v. The injectivity of the first map is the so-called *Hasse principle* for central simples algebras of k, which is a celebrated theorem of Hasse–Brauer–Noether.

Kato [21] proposed a fascinating framework of conjectures that generalizes the above facts to higher-dimensional arithmetic schemes. To review these conjectures, we introduce some notation. Let L be a field with $p = \mathrm{char}(L)$. Let n be an integer $n > 0$ and write $n = mp^r$ with $(p,m) = 1$. We define the following Galois cohomology groups:

$$H^i(L, \mathbb{Z}/n\mathbb{Z}(j)) = H^i(L, \mu_m^{\otimes j}) \oplus H^{i-j}(L, W_r\Omega^i_{L,\log}), \tag{1}$$

where μ_m is the Galois module of nth roots of unity and $W_r\Omega^i_{L,\log}$ is the logarithmic part of the de Rham-Witt sheaf $W_r\Omega^i_L$ [15, I, (5.7)]. Note that there is a canonical identification $H^2(L, \mathbb{Z}/n\mathbb{Z}(1)) = Br(L)[n]$, where $[n]$ denotes the n-torsion part.

Now, let X be a scheme of finite type over $\mathbb{F}_p$ or the integer ring of a number field or a ($\mathfrak{p}$-adic) local field. Kato introduced the following complex $KC_\bullet(X, \mathbb{Z}/n\mathbb{Z})$ which we call the *Kato complex*:

$$\begin{aligned} \cdots \to \bigoplus_{x\in X_{(a)}} H^{a+1}(x, \mathbb{Z}/n\mathbb{Z}(a)) \to \bigoplus_{x\in X_{(a-1)}} H^a(x, \mathbb{Z}/n\mathbb{Z}(a-1)) \to \cdots \\ \cdots \to \bigoplus_{x\in X_{(1)}} H^2(x, \mathbb{Z}/n\mathbb{Z}(1)) \to \bigoplus_{x\in X_{(0)}} H^1(x, \mathbb{Z}/n\mathbb{Z}), \end{aligned} \tag{2}$$

where $X_{(a)} = \{x \in X \mid \dim \overline{\{x\}} = a\}$ and the term $\oplus_{x\in X_{(a)}}$ is put in degree a. We will also use the complexes:

$$KC_\bullet(X, \mathbb{Q}/\mathbb{Z}) = \varinjlim_n KC_\bullet(X, \mathbb{Z}/n\mathbb{Z}) \quad \text{and} \quad KC_\bullet(X, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = \varinjlim_n KC_\bullet(X, \mathbb{Z}/\ell^n\mathbb{Z}),$$

where ℓ is a prime. Their homology groups

$$KH_a(X,\Lambda) := H_a(KC_\bullet(X,\Lambda)) \quad (\Lambda = \mathbb{Z}/n\mathbb{Z},\, \mathbb{Q}/\mathbb{Z},\, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \tag{3}$$

are called the *Kato homology* of X with coefficient Λ. (It is indeed a homology theory in the sense of Definition 3.1.)

Now let X be a projective smooth connected curve over a finite field $\mathbb{F}_q$ with the function field $k = \mathbb{F}_q(X)$, or $X = \mathrm{Spec}(\mathscr{O}_k)$ for the integer ring $\mathscr{O}_k$ of a number field or a local field. Then the Kato complex $KC_\bullet(X,\mathbb{Q}/\mathbb{Z})$ is identified with the following complex:

$$Br(k) \longrightarrow \bigoplus_{x\in X_{(0)}} H^1(x,\mathbb{Q}/\mathbb{Z}).$$

Hence the above facts (1) and (2) are equivalent to the following:

$$KH_1(X,\mathbb{Q}/\mathbb{Z}) = 0 \quad \text{and} \quad KH_0(X,\mathbb{Q}/\mathbb{Z}) = \begin{cases} 0 & \text{if } k \text{ is local,} \\ \mathbb{Q}/\mathbb{Z} & \text{if } k \text{ is global.} \end{cases}$$

Kato [21] proposed the following vast generalizations of these facts.

Conjecture 1.1. *Let X be a connected proper smooth variety over a finite field $\mathbb{F}_q$. Then*

$$KH_a(X,\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\cong} \begin{cases} 0 & \textit{if } a \neq 0, \\ \mathbb{Z}/n\mathbb{Z} & \textit{if } a = 0. \end{cases}$$

Conjecture 1.2. *Let X be a connected regular scheme proper and flat over* $\mathrm{Spec}(\mathscr{O}_k)$ *where $\mathscr{O}_k$ is the integer ring of a number field k. Assume*

$$\textit{either } n \textit{ is odd or } k \textit{ is totally imaginary.} \tag{$*$}$$

Then

$$KH_a(X,\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\cong} \begin{cases} 0 & \textit{if } a \neq 0, \\ \mathbb{Z}/n\mathbb{Z} & \textit{if } a = 0. \end{cases}$$

We note that the assumption $(*)$ may be removed by modifying $KH_a(X,\mathbb{Q}/\mathbb{Z})$ (see Conjecture C on page 482 of Jannsen and Saito [18]).

Conjecture 1.3. *Let X be a regular scheme proper and flat over* $\mathrm{Spec}(\mathscr{O}_k)$ *where $\mathscr{O}_k$ is the integer ring of a local field k. Then*

$$KH_a(X,\mathbb{Z}/n\mathbb{Z}) = 0 \quad \textit{for } a \geq 0.$$

2 Known Results and Announcement of New Results

As was already noticed, the Kato conjectures in case $\dim(X) = 1$ rephrase the classical fundamental facts on the Brauer group of a global field and a local field.

Kato [21] proved Conjectures 1.1–1.3 in case $\dim(X) = 2$. He deduced it from higher class field theory for X proved in [23,29]. For X of dimension 2, the vanishing of $KH_2(X, \mathbb{Z}/n\mathbb{Z})$ in Conjecture 1.1 had been earlier established in [8] (prime-to-p part), and completed by Gros [13] for the p-part.

We note that it is easy to show the isomorphism for $a = 0$ in the conjectures (see (7) in Sect. 3). So we are only concerned with the isomorphisms for $a > 0$. The first result after [21] is the following.

Theorem 2.1 (Saito [30]). *Let X be a smooth projective 3-fold over a finite field F. Then $KH_3(X, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = 0$ for any prime $\ell \neq \mathrm{char}(F)$.*

This result was immediately generalized to the following.

Theorem 2.2 (Colliot-Thélène [7], Suwa [33]). *Let X be a smooth projective variety over a finite field F. Then*

$$KH_a(X, \mathbb{Q}/\mathbb{Z}) = 0 \quad \text{for } 0 < a \leq 3.$$

Colliot-Thélène [7] handled the prime-to-p part, where $p = \mathrm{char}(F)$, and Suwa [33] later adapted the technique of Colliot-Thélène [7] to handle the p-part. A tool in [30] is a class field theory of surfaces over local fields, while the technique in [7] is global and different from that in [30].

The arithmetic version of the above theorem was established in the following.

Theorem 2.3 (Jannsen–Saito [18]). *Let X be a regular projective flat scheme over $S = \mathrm{Spec}(\mathscr{O}_k)$ where k is a number field or a $\mathfrak{p}$-adic field. Assume that k is totally imaginary if k is a number field. Fix a prime p. Assume that for any closed point $v \in S$, the reduced part of $X_v = X \times_S v$ is a simple normal crossing divisor on X and that X_v is reduced if $v|p$. Then we have*

$$KH_a(X, \mathbb{Q}_p/\mathbb{Z}_p) = 0 \quad \text{for } 0 < a \leq 3.$$

Recently, general approaches to Conjecture 1.1 were proposed assuming resolution of singularities.

Theorem 2.4 (Jannsen [17], Jannsen–Saito [19]). *Let X be a projective smooth variety of dimension d over a finite field F. Let $t \geq 1$ be an integer. Then we have*

$$KH_a(X, \mathbb{Q}/\mathbb{Z}) = 0 \quad \text{for } 0 < a \leq t$$

if either $t \leq 4$ or $(\mathbf{RS})_d$, *or* $(\mathbf{RES})_{t-2}$ *(see below) holds.*

$(\mathbf{RS})_d$ For any X integral and proper of dimension $\leq d$ over F, there exists a proper birational morphism $\pi : X' \to X$ such that X' is smooth over F. For any U smooth of dimension $\leq d$ over F, there is an open immersion $U \hookrightarrow X$ such that X is projective smooth over F with $X - U$ a simple normal crossing divisor on X.

$(\mathbf{RES})_t$ For any smooth projective variety X over F, any simple normal crossing divisor Y on X with $U = X - Y$, and any integral closed subscheme $W \subset X$ of dimension $\leq t$ such that $W \cap U$ is regular, there exists a projective smooth X'

over F and a birational proper map $\pi : X' \to X$ such that $\pi^{-1}(U) \simeq U$, and that $Y' = X' - \pi^{-1}(U)$ is a simple normal crossing divisor on X', and that the proper transform of W in X' is regular and intersects transversally with Y'.

We note that a proof of $(\mathbf{RES})_2$ is given in [9] based on an idea of Hironaka, which enables us to obtain the unconditional vanishing of the Kato homology with $\mathbb{Q}/\mathbb{Z}$-coefficients in degree $a \le 4$.

Finally, the above approach has been improved to remove the assumptions $(\mathbf{RS})_d$ and $(\mathbf{RES})_t$ on resolution of singularities, at least if we are restricted to the prime-to-char(F) part.

Theorem 2.5 (Kerz–Saito [24]). *Let X be a projective smooth variety over a finite field F. For a prime $\ell \neq \mathrm{char}(F)$, we have $KH_a(X, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = 0$ for $a > 0$.*

A key to the proof is the following refinement of de Jong's alteration theorem due to Gabber (see [16]).

Theorem 2.6 (Gabber). *Let F be a perfect field and X be a variety over F. Let $W \subset X$ be a proper closed subscheme. Let ℓ be a prime different from $\mathrm{char}(F)$. Then there exists a projective morphism $\pi : X' \to X$ such that:*

- *X' is smooth over F and the reduced part of $\pi^{-1}(W)$ is a simple normal crossing divisor on X.*
- *π is generically finite of degree prime to ℓ.*

The same technique proves the following arithmetic version as well.

Theorem 2.7 (Kerz–Saito [24]). *Let X be a regular projective flat scheme over a henselian discrete valuation ring with finite residue field F. Then, for a prime $\ell \neq \mathrm{char}(F)$, we have $KH_a(X, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = 0$ for $a \ge 0$.*

Finally we remark that one can prove the above results with $\mathbb{Z}/\ell^n\mathbb{Z}$-coefficients instead of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$-coefficients by using the Bloch–Kato conjecture: For a prime ℓ and a field L, we have the symbol map

$$h^t_{L,\ell} : K^M_t(L)/\ell \to H^t(L, \mathbb{Z}/\ell\mathbb{Z}(t)),$$

where $K^M_t(L)$ denotes the Milnor K-group of L. It is conjectured that $h^t_{L,\ell}$ is surjective. The conjecture is called the *Bloch–Kato conjecture* in case $l \neq \mathrm{char}(L)$. For a scheme X, we introduce the following condition:

$(\mathbf{BK})^t_{X,\ell}$ For every field L finitely generated over a residue field of X, $h^t_{L,\ell}$ is surjective.

The surjectivity of $h^t_{L,\ell}$ is known if $t = 1$ (Kummer theory) or $t = 2$ (Merkurjev–Suslin [26]) or $\ell = \mathrm{char}(L)$ (Bloch–Gabber–Kato [5]) or $\ell = 2$ (Voevodsky [34]). It is conjectured (the Bloch–Kato conjecture) that $h^t_{L,\ell}$ is always an isomorphism for every field L. Recently, a complete proof of the conjecture has been announced by Rost and Voevodsky ([31, 35], see also [14, 36–38]).

Theorem 2.8 (see [19, Sect. 5]). *Let X and ℓ be as in either of Theorem 2.5 or of Theorem 2.7. Assume $(\mathbf{BK})^t_{X,\ell}$ holds. Then we have $KH_a(X, \mathbb{Z}/\ell^n\mathbb{Z}) = 0$ for $0 < a \le t$.*

3 Outline of Proof of Theorem 2.5

In this section, we give an outline of the proof of Theorem 2.5. We fix a finite field F with $p = \mathrm{char}(F)$ and work in the category $\mathscr{C}$ of schemes separated of finite type over F. We first recall the following.

Definition 3.1. Let $\mathscr{C}_*$ be the category with the same objects as $\mathscr{C}$, but morphisms are just the proper maps in $\mathscr{C}$. Let *Mod* be the category of modules. A homology theory $H = \{H_a\}_{a\in\mathbb{Z}}$ on $\mathscr{C}$ is a sequence of covariant functors:

$$H_a(-) : \mathscr{C}_* \to Mod$$

satisfying the following conditions:

1. For each open immersion $j : V \hookrightarrow X$ in $\mathscr{C}$, there is a map $j^* : H_a(X) \to H_a(V)$, associated to j in a functorial way.
2. If $i : Y \hookrightarrow X$ is a closed immersion in X, with open complement $j : V \hookrightarrow X$, there is a long exact sequence (called the *localization sequence*)

$$\cdots \xrightarrow{\partial} H_a(Y) \xrightarrow{i_*} H_a(X) \xrightarrow{j^*} H_a(V) \xrightarrow{\partial} H_{a-1}(Y) \longrightarrow \cdots .$$

   (The maps ∂ are called the *connecting morphisms*.) This sequence is functorial with respect to proper maps or open immersions, in an obvious way.

   It is an easy exercise to check that the Kato homology (3)

$$KH(-,\Lambda) = \{KH_a(-,\Lambda)\}_{a\in\mathbb{Z}}$$

provides us with a homology theory on $\mathscr{C}$.

Given a homology theory H on $\mathscr{C}$, we have the spectral sequence of homological type associated to every $X \in Ob(\mathscr{C})$, called the *niveau spectral sequence* (cf. [6]):

$$E^1_{a,b}(X) = \bigoplus_{x\in X_{(a)}} H_{a+b}(x) \;\Rightarrow\; H_{a+b}(X) \quad \text{with } H_a(x) = \lim V \subseteq \overline{\{x\}} H_a(V). \tag{4}$$

Here, the limit is over all open nonempty subschemes $V \subseteq \overline{\{x\}}$. This spectral sequence is covariant with respect to proper morphisms in $\mathscr{C}$ and contravariant with respect to open immersions. The functoriality of the spectral sequence is a direct consequence of that of the homology theory H.

In what follows, we assume $\Lambda = \mathbb{Z}/n\mathbb{Z}$ with n prime to p or $\Lambda = \mathbb{Q}_\ell/\mathbb{Z}_\ell$ with $\ell \neq p$.

Step 1: Kato Homology and Étale Homology

We now consider the étale homology on $\mathscr{C}$ given by

$$H_a(X,\Lambda) := H^{-a}(X_{\text{ét}}, Rf^!\Lambda) \quad \text{for } f : X \to \mathrm{Spec}(F) \text{ in } \mathscr{C}.$$

Here $Rf^!$ is the right adjoint of $Rf_!$ defined in [2, XVIII, (3.1.4)]. This is a homology theory in the sense of Definition 3.1. For X smooth of pure dimension d over F, we have (cf. [6] and [18, Theorem 2.14])

$$H_a^{\text{ét}}(X,\Lambda) = H_{\text{ét}}^{2d-a}(X,\Lambda(d))\,, \tag{5}$$

where, for an integer $r > 0$, $\Lambda(r)$ is the Tate twist by the étale sheaf of roots of unity.

We then look at the spectral sequence (4) arising from this homology theory. The first step of the proof is the following lemma.

Lemma 3.2. *For $X \in Ob(\mathscr{C})$, we have $E^1_{a,b}(X) = 0$ if $b < -1$ and there is a natural isomorphism of complexes*

$$KC_\bullet(X,\Lambda) \simeq E^1_{\bullet,-1}(X),$$

where the right-hand side denotes the complex

$$\cdots \to E^1_{a,-1}(X) \xrightarrow{d^1} E^1_{a-1,-1}(X) \xrightarrow{d^1} \cdots \xrightarrow{d^1} E^1_{1,-1}(X) \xrightarrow{d^1} E^1_{0,-1}(X).$$

In particular, we have a natural isomorphism

$$KH_a(X,\Lambda) \simeq E^2_{a,-1}(X).$$

The first assertion follows easily from the fact $\mathrm{cd}(F) = 1$ and the second from [20, Theorem 1.1.1].

By the above lemma, we get the edge homomorphism

$$\varepsilon_X^a \;:\; H_{a-1}(X,\Lambda) \to KH_a(X,\Lambda) = E^2_{a,-1}(X), \tag{6}$$

which is an isomorphism for $a = 0$ by the first assertion of the lemma. For X connected smooth projective of dimension d over F, it gives rise to canonical isomorphisms

$$KH_0(X,\Lambda) \simeq H_{-1}(X,\Lambda) \simeq H^{2d+1}(X_{\text{ét}},\Lambda(d)) \simeq H^1(F,\Lambda) \simeq \Lambda\,, \tag{7}$$

where the second isomorphism is due to (5) and the third is the trace map and the last is the natural isomorphism in (1).

Step 2: Log Pairs and Graphication

Let the assumptions be as above. Let $\mathscr{S} \subset \mathscr{C}$ be the subcategory of irreducible smooth projective schemes over $\mathrm{Spec}(F)$.

Definition 3.3. A *log pair* is a couple $\Phi = (X,Y)$ where $X \in Ob(\mathscr{S})$, and $Y = \emptyset$ or Y is a divisor with simple normal crossings on X. We call $U = X - Y$ the complement of Φ and denote sometimes $\Phi = (X,Y;U)$.

Let $\Phi = (X,Y)$ be a log pair and let $Y_1,\dots,Y_N$ be the irreducible components of Y. For an integer $a \geq 1$ write

$$Y^{(a)} = \coprod_{1\leq i_i<\cdots<i_a\leq N} Y_{i_1,\dots,i_a} \quad (Y_{i_1,\dots,i_a} = Y_{i_1}\cap\cdots\cap Y_{i_a}). \tag{8}$$

We also denote $Y^{(0)} = X$. For $1 \leq \nu \leq a$ the proper morphism

$$\delta_\nu : Y^{(a)} \to Y^{(a-1)} \tag{9}$$

is induced by the inclusions $Y_{i_1,\dots,i_a} \hookrightarrow Y_{i_1,\dots,\hat{i_\nu},\dots,i_a}$.

Definition 3.4. The *graph complex* of a log pair $\Phi = (X,Y)$ is the complex:

$$G_\bullet(\Phi,\Lambda) \ : \ \Lambda^{\pi_0(Y^{(d)})} \xrightarrow{\partial} \Lambda^{\pi_0(Y^{(d-1)})} \xrightarrow{\partial} \cdots \to \Lambda^{\pi_0(Y^{(1)})} \xrightarrow{\partial} \Lambda^{\pi_0(X)},$$

where $\pi_0(Y^{(a)})$ is the set of connected components of $Y^{(a)}$ and $\Lambda^{\pi_0(Y^{(a)})}$ is put in degree a. Here $\partial : \Lambda^{\pi_0(Y^{(a)})} \to \Lambda^{\pi_0(Y^{(a-1)})}$ is defined as

$$\partial = \sum_{\nu=1}^{a} (-1)^\nu \partial_\nu \ , \tag{10}$$

$$\partial_\nu : \Lambda^{\pi_0(Y^{(a)})} \to \Lambda^{\pi_0(Y^{(a-1)})}, \quad (a_i)_{i\in\pi_0(Y^{(a)})} \to \left(\sum_{\delta_\nu(i)=j} a_i\right)_{j\in\pi_0(Y^{(a-1)})},$$

where $\delta_\nu : \pi_0(Y^{(a)}) \to \pi_0(Y^{(a-1)})$ is induced by the map (9).

Now a key construction [19, (3.2)] is to define a natural map of complexes

$$\gamma_\Phi : KC_\bullet(U,\Lambda) \to G_\bullet(\Phi,\Lambda) \quad \text{for } \Phi = (X,Y;U)$$

that induces the natural homomorphism

$$\gamma_\Phi^a : KH_a(U,\Lambda) \to GH_a(\Phi,\Lambda) := H_a(G_\bullet(\Phi,\Lambda)), \tag{11}$$

which we call the *graphication of the Kato homology*. To control γ_Φ^a, we use

$$\gamma\varepsilon_\Phi^a \ : \ H_{a-1}(U,\Lambda) \to GH_a(\Phi,\Lambda) \tag{12}$$

which is defined as the composite of γ_Φ^a with ε_U^a (cf. (6)). We note that the right-hand side of (12) is nonzero only if $0 \leq a \leq d = \dim(X)$ while the left-hand side could be nonzero for any a with $0 \leq a \leq 2d+1$.

Definition 3.5. A log pair $\Phi = (X,Y)$ is *clean in degree q* for a nonnegative integer $q \leq \dim(X)$ if $\gamma\varepsilon_\Phi^a$ is injective for $a = q$ and surjective for $a = q+1$.

Now the following theorem [19, Lemmas 3.3 and 3.4] is crucial.

Theorem 3.6. *Take* $\Lambda = \mathbb{Q}_\ell/\mathbb{Z}_\ell$. *Let* $\Phi = (X,Y;U)$ *be an ample log pair, which means by definition that one of the irreducible components of* Y *is an ample divisor on* X. *Then* Φ *is clean in degree* q *for all* $q \leq \dim(X)$.

The proof of the above theorem hinges on the affine Lefschetz theorem and the Weil conjecture proved by Deligne [10].

The above theorem implies that for an ample log pair Φ and for any integer a with $0 \leq a \leq \dim(X)$, γ^a_Φ is surjective, and an isomorphism if ε^a_U is surjective. This is already a big step in the proof of Theorem 2.5.

We will need a variant of the above construction.

Definition 3.7. The *reduced graph complex* of a log pair $\Phi = (X,Y)$ is the complex:

$$G_\bullet(\hat{\Phi},\Lambda)\ :\ \Lambda^{\pi_0(Y^{(d)})} \xrightarrow{\partial} \Lambda^{\pi_0(Y^{(d-1)})} \xrightarrow{\partial} \cdots \to \Lambda^{\pi_0(Y^{(1)})},$$

where $\Lambda^{\pi_0(Y^{(a)})}$ is put in degree a. We have evident maps of complexes

$$\Lambda^{\pi_0(X)}[0] \to G_\bullet(\Phi,\Lambda) \xrightarrow{\iota} G_\bullet(\hat{\Phi},\Lambda)$$

that induce an isomorphism

$$\iota : GH_a(\Phi,\Lambda) \xrightarrow{\cong} GH_a(\hat{\Phi},\Lambda) \quad \text{for } a \neq 1, \tag{13}$$

and an exact sequence

$$0 \to GH_1(\Phi,\Lambda)) \xrightarrow{\iota} GH_1(\hat{\Phi},\Lambda) \to \Lambda \to 0. \tag{14}$$

In the same way as above, one may also define the natural homomorphism [24]

$$\gamma^a_{\hat{\Phi}} : KH_{a-1}(Y,\Lambda) \to GH_a(\hat{\Phi},\Lambda) \tag{15}$$

which fits into the commutative diagram

$$\begin{tikzcd} KH_a(U,\Lambda) \arrow[r, "\partial"] \arrow[d, "\gamma^a_\Phi"] & KH_{a-1}(Y,\Lambda) \arrow[d, "\gamma^a_{\hat{\Phi}}"] \\ GH_a(\Phi,\Lambda) \arrow[r, "\iota"] & GH_a(\hat{\Phi},\Lambda) \end{tikzcd}$$

where ∂ is the boundary map for the Kato homolgy.

Step 3: Pullback Map for Kato Homology

Another key ingredient to the proof of Theorem 2.5 is the construction of the pullback map for Kato homology, which is stated in the following form.

Lemma 3.8. *For any dominant morphism $f : X \to Y$, where X, $Y \in Ob(\mathscr{C})$ are integral smooth of the same dimension over F, we have the pullback maps for all q:*

$$f^* : H_q(Y,\Lambda) \to H_q(X,\Lambda) \quad \textit{and} \quad f^* : KH_q(Y,\Lambda) \to KH_q(X,\Lambda),$$

which satisfy the following conditions:

- *For a dominant morphism $g : Y \to Z$ with Z integral smooth over F of the same dimension, we have $(g \cdot f)^* = f^* \cdot g^*$.*
- *The following diagram is commutative (cf. (6))*

$$\begin{array}{ccc} H_{q-1}(Y,\Lambda) & \xrightarrow{\varepsilon_Y^q} & KH_q(Y,\Lambda) \\ \Big\downarrow f^* & & \Big\downarrow f^* \\ H_{q-1}(X,\Lambda) & \xrightarrow{\varepsilon_X^q} & KH_q(X,\Lambda) \end{array}$$

- *If f is proper, the composite map*

$$KH_q(Y,\Lambda) \xrightarrow{f^*} KH_q(X,\Lambda) \xrightarrow{f_*} KH_q(Y,\Lambda)$$

  is the multiplication by the degree $[F(X) : F(Y)]$ of the extension of the function fields.

In [24] the above lemma is shown based on the intersection theory on cycle modules due to Rost [28]. (The theory was originally developed over a field but it may be extended to a more general base.)

Step 4: The Condition $(\mathbf{LG})_q$

Let $q \geq 1$ be an integer. For a log pair $\Phi = (X,Y;U)$ consider the condition:

$(\mathbf{LG})_q$ The composite map

$$\partial\varepsilon_\Phi^a : H_{a-1}(U,\Lambda) \xrightarrow{\varepsilon_U^a} KH_a(U,\Lambda) \xrightarrow{\partial} KH_{a-1}(Y,\Lambda)$$

is injective for $a = q$ and surjective for $a = q+1$.

Lemma 3.9. *Let $q \geq 1$ be an integer. Let $\Phi = (X,Y;U)$ be a log pair that satisfies the condition $(\mathbf{LG})_q$. Let $j^* : KH_q(X,\Lambda) \to KH_q(U,\Lambda)$ be the pullback via $j : U \hookrightarrow X$ and $\varepsilon_U^q : H_{q-1}(U,\Lambda) \to KH_q(U,\Lambda)$ be as in (6). Then the map j^* is injective and* $\mathrm{Image}(j^*) \cap \mathrm{Image}(\varepsilon_U^q) = 0$.

Proof. First we claim that j^* is injective. Indeed we have the exact sequence

$$KH_{q+1}(U,\Lambda) \xrightarrow{\partial} KH_q(Y,\Lambda) \to KH_q(X,\Lambda) \xrightarrow{j^*} KH_q(U).$$

Since $\partial\varepsilon_U^{q+1}$ is surjective by the assumption, ∂ is surjective and the claim follows. By the above claim it suffices to show $\mathrm{Image}(j^*) \cap \mathrm{Image}(\varepsilon_U^q) = 0$. We have the exact sequence

$$KH_q(X,\Lambda) \xrightarrow{j^*} KH_q(U,\Lambda) \xrightarrow{\partial} KH_{q-1}(Y,\Lambda).$$

Let $\beta \in H_{q-1}(U,\Lambda)$ and assume $\alpha = \varepsilon_U^q(\beta) \in KH_q(U,\Lambda)$ lies in $\mathrm{Image}(j^*)$. It implies $\partial(\alpha) = \partial\varepsilon_U^q(\beta) = 0$. Since $\partial\varepsilon_U^q$ is injective by the assumption, this implies $\beta = 0$ so that $\alpha = 0$. □

For integers $q \geq 1$ and $d \geq 0$, consider the condition:

$\mathbf{KC}(q,d)$ $\quad KH_a(X,\Lambda) = 0$ for all $X \in Ob(\mathscr{S})$ with $\dim(X) \leq d$ and $0 < a \leq q$.

Lemma 3.10. *Take $\Lambda = \mathbb{Q}_\ell/\mathbb{Z}_\ell$. Fix integers d and q with $d \geq q \geq 1$, and assume $\mathbf{KC}(q,d-1)$. For any log pair $\Phi = (X,Y)$ with $d = \dim(X)$, there exists a log pair $\Phi' = (X,Y')$ with $Y \subset Y'$ such that Φ' satisfies the condition $(\mathbf{LG})_q$.*

Proof. It follows from Bertini's theorem [1, 27] that for any log pair $\Phi = (X,Y)$ with $\dim(X) = d$, one can take $Z \subset X$, a smooth section of a sufficiently ample line bundle on X, such that $\Phi' = (X, Y \cup Z)$ is an ample log pair so that it is clean in degree q for all $q \leq \dim(X)$ by Theorem 3.6. Hence, it suffices to show that if $\Phi = (X,Y;U)$ is clean in degree q, then it satisfies the condition $(\mathbf{LG})_q$. We consider the commutative diagram

$$\begin{tikzcd}
H_q(U,\Lambda) \arrow[r, "\varepsilon_U^{q+1}"] & KH_{q+1}(U,\Lambda) \arrow[r, "\partial"] \arrow[d, "\gamma_\Phi^{q+1}"] & KH_q(Y,\Lambda) \arrow[d, "\gamma_{\hat{\Phi}}^{q+1}"] \\
 & GH_{q+1}(\Phi,\Lambda) \arrow[r, "\simeq", "\iota"'] & GH_{q+1}(\hat{\Phi},\Lambda)
\end{tikzcd}$$

where ι is an isomorphism by (13), and $\gamma\varepsilon_\Phi^{q+1} = \gamma_\Phi^{q+1} \circ \varepsilon_U^{q+1}$ is surjective by the assumption. Moreover, $\gamma_{\hat{\Phi}}^{q+1}$ is an isomorphism. Indeed we have the spectral sequence (Mayer–Vietoris for homology of closed coverings):

$$E_{s,t}^1 = KH_t(Y^{(s)},\Lambda) \Rightarrow KH_{s+t-1}(Y,\Lambda) \quad \text{(cf. (8))}$$

where we put $E_{s,t}^1 = 0$ for $s \leq 0$, so that $\mathbf{KC}(q,d-1)$ implies $KH_t(Y^{(s)},\Lambda) = 0$ for $0 < t \leq q$ and $s > 0$. The assertion follows easily from this and (7). Now a diagram chase shows that $\partial\varepsilon_U^{q+1}$ is surjective.

Next we consider the commutative diagram

$$\begin{array}{ccccc} H_{q-1}(U,\Lambda) & \xrightarrow{\varepsilon_U^q} & KH_q(U,\Lambda) & \xrightarrow{\partial} & KH_{q-1}(Y,\Lambda) \\ & & \downarrow{\scriptstyle \gamma_\Phi^q} & & \downarrow{\scriptstyle \gamma_{\hat{\Phi}}^{q-1}} \\ & & GH_q(\Phi,\Lambda) & \xrightarrow[\iota]{\hookrightarrow} & GH_q(\hat{\Phi},\Lambda) \end{array}$$

where ι is injective by (13) and (14), and $\gamma\varepsilon_\Phi^q = \gamma_\Phi^q \circ \varepsilon_U^q$ is injective by the assumption. As before one can show by using $\mathbf{KC}(q,d-1)$ that $\gamma_{\hat{\Phi}}^{q-1}$ is an isomorphism. This shows $\partial\varepsilon_U^q$ is injective and the proof is complete. $\square$

Step 5: Gabber's Theorem Enters to End the Proof

We fix a prime $\ell \neq \mathrm{char}(F)$ and take $\Lambda = \mathbb{Q}_\ell/\mathbb{Z}_\ell$. We finish the proof of Theorem 2.5 by induction on $d = \dim(X) \geq 0$. The case $d = 0$ is trivial. Assume $d \geq 1$ and that $\mathbf{KC}(q,d-1)$ holds for $1 \leq q \leq d$. Let $X \in Ob(\mathscr{S})$ with $d = \dim(X)$. Let $\alpha \in KH_q(X,\Lambda)$. By recalling that

$$\varepsilon_X^q : H_{q-1}(X,\Lambda) \to KH_q(X,\Lambda) = E_{q,-1}^2(X)$$

is an edge homomorphism and by looking at the differentials

$$d_{q,-1}^r : E_{q,-1}^r(X) \to E_{q-r,r-2}^r(X),$$

we conclude that there exists a closed subscheme $W \subset X$ such that $\dim(W) \leq q-2$, and that putting $U = X - W$, the pullback $\alpha_{|U} \in KH_q(U,\Lambda)$ of α via $U \to X$ lies in the image of ε_U^q, namely there exists $\beta \in H_{q-1}(U,\Lambda)$ such that $\alpha_{|U} = \varepsilon_U^q(\beta)$. Take $\pi : X' \to X$ as in Theorem 2.6 and put $U' = \pi^{-1}(U)$ and $Y' = \pi^{-1}(W)_{red}$ which is a divisor with simple normal crossings on X'. By Lemma 3.10 there is a log pair $\Phi = (X', Y''; V)$ with $Y' \subset Y''$ which satisfies the condition $(\mathbf{LG})_q$. Thanks to Step 3, we have the commutative diagram

$$\begin{array}{ccccc} KH_q(X,\Lambda) & \xrightarrow{\pi^*} & KH_q(X',\Lambda) & & \\ \downarrow & & \downarrow & & \\ KH_q(U,\Lambda) & \xrightarrow{\pi^*} & KH_q(U',\Lambda) & \xrightarrow{j^*} & KH_q(V,\Lambda) \\ \uparrow{\scriptstyle \varepsilon_U^q} & & \uparrow{\scriptstyle \varepsilon_{U'}^q} & & \uparrow{\scriptstyle \varepsilon_V^q} \\ H_{q-1}(U,\Lambda) & \xrightarrow{\pi^*} & H_{q-1}(U',\Lambda) & \xrightarrow{j^*} & H_{q-1}(V,\Lambda) \end{array}$$

where $j : V \to U$ is the open immersion. Put $\alpha' = \pi^*(\alpha) \in KH_q(X',\Lambda)$ and $\beta' = \pi^*(\beta) \in H_{q-1}(U',\Lambda)$. Let $\alpha'_{|V} \in KH_q(V,\Lambda)$ (resp., $\beta'_{|V} \in H_{q-1}(V,\Lambda)$) be the pullback of α' (resp., β') via $V \hookrightarrow X'$ (resp., $V \hookrightarrow U'$). By the diagram, we get $\alpha'_{|V} = \varepsilon_V^q(\beta'_{|V}) \in KH_q(V,\Lambda)$. By Lemma 3.9, this implies $\alpha' = 0$. Since the composite

$$KH_q(X,\Lambda) \xrightarrow{\pi^*} KH_q(X',\Lambda) \xrightarrow{\pi_*} KH_q(X,\Lambda)$$

is the multiplication of the degree of π which is prime to ℓ, we get $\alpha = 0$. $\square$

4 Applications

Let X be a smooth scheme over a field F and let

$$H_M^q(X,\mathbb{Z}(r)) = CH^r(X,2r-q) = H_{2r-q}(z^r(X,\bullet)) \quad (q,r \geq 0)$$

be the motivic cohomology of X defined as Bloch's higher Chow group, where $z^r(X,\bullet)$ is Bloch's cycle complex [4]. Recall that $\mathrm{CH}^r(X,0)$ is the classical Chow group $\mathrm{CH}^r(X)$. A "folklore conjecture," generalizing the analogous conjecture of Bass on K-groups, is that in case F is finite, $H_M^q(X,\mathbb{Z}(r))$ should be finitely generated. Except the case of $r=1$ or $\dim(X)=1$ (Quillen), the only known case is that of $H_M^{2d}(X,\mathbb{Z}(d)) = \mathrm{CH}^d(X) = \mathrm{CH}_0(X)$, where $d = \dim(X)$. It is a consequence of higher-dimensional class field theory [3, 8, 22].

One way to approach the problem is to look at an étale cycle map constructed by Geisser and Levine [12]:

$$\rho^{r,q}_{X,\mathbb{Z}/n\mathbb{Z}} : \mathrm{CH}^r(X,q;\mathbb{Z}/n\mathbb{Z}) \to H^{2r-q}_{\text{ét}}(X,\mathbb{Z}/n\mathbb{Z}(r)). \tag{16}$$

Here,

$$\mathrm{CH}^r(X,q;\mathbb{Z}/n\mathbb{Z}) = H_q(z^r(X,\bullet)\otimes^{\mathbb{L}}\mathbb{Z}/n\mathbb{Z})$$

is the higher Chow group with finite coefficients which fits into an exact sequence

$$0 \to \mathrm{CH}^r(X,q)/n \to \mathrm{CH}^r(X,q;\mathbb{Z}/n\mathbb{Z}) \to \mathrm{CH}^r(X,q-1)[n] \to 0,$$

and $\mathbb{Z}/n\mathbb{Z}(r)$ is the complex of étale sheaves on X:

$$\mathbb{Z}/n\mathbb{Z}(r) = \mu_m^{\otimes r} \oplus W_\nu \Omega^r_{X,\log}[-r],$$

where $n = mp^r$ and $(p,m)=1$ with $p = \mathrm{char}(F)$ (cf. (1)). The same construction has been carried out for a regular scheme X of finite type over a Dedekind domain by Levine [25] (see also [11]), assuming that n is invertible on X.

We recall the following result due to Suslin–Voevodsky [32] and Geisser-Levine [12].

Theorem 4.1. *Let the assumption be as above (the case over a Dedekind domain is included). Assume* $\mathbf{(BK)}^t_{X,\ell}$ *for all* $t \geq 0$ *(cf. Sect. 1). Then* $\rho^{r,q}_{X,\mathbb{Z}/\ell^n\mathbb{Z}}$ *is an isomorphism for* $r \leq q$ *and injective for* $r = q+1$.

Now we turn our attention to $\rho^{r,q}_{X,\mathbb{Z}/n\mathbb{Z}}$ in case $r \geq d := \dim(X)$. We assume that X is a regular scheme over either a finite field F or a henselian discrete valuation ring with finite residue field F. In case $r > d$ it is easily shown (see [19, Lemma 6.2]) that $\rho^{r,q}_{X,\mathbb{Z}/\ell^n\mathbb{Z}}$ is an isomorphism assuming $\mathbf{(BK)}^{q+1}_{X,\ell}$. An interesting phenomenon emerges for $\rho^{r,q}_{X,\mathbb{Z}/\ell^n\mathbb{Z}}$ with $r = d$. $\mathbf{(BK)}^{q+1}_{X,\ell}$ implies a long exact sequence (see [19, Lemma 6.2]):

$$KH_{q+2}(X,\mathbb{Z}/\ell^n\mathbb{Z}) \to \mathrm{CH}^d(X,q;\mathbb{Z}/\ell^n\mathbb{Z}) \xrightarrow{\rho^{d,q}_{X,\mathbb{Z}/\ell^n\mathbb{Z}}} H^{2d-q}_{\text{ét}}(X,\mathbb{Z}/\ell^n\mathbb{Z}(d))$$
$$\to KH_{q+1}(X,\mathbb{Z}/\ell^n\mathbb{Z}) \to \mathrm{CH}^d(X,q-1;\mathbb{Z}/\ell^n\mathbb{Z}) \xrightarrow{\rho^{d,q-1}_{X,\mathbb{Z}/\ell^n\mathbb{Z}}} \cdots$$

Hence Theorem 2.8 implies the following.

Theorem 4.2 (Kerz and Saito [24]). *Let X be a regular projective scheme over either a finite field F or a henselian discrete valuation ring with finite residue field F. Let $q \geq 0$ be an integer and $n > 0$ be an integer prime to* $\mathrm{char}(F)$ *and assume* $\mathbf{(BK)}^{q+2}_{X,\ell}$ *for all primes ℓ dividing n. Let $d = \dim(X)$. Then*

$$\rho^{d,q}_{X,\mathbb{Z}/n\mathbb{Z}} : \mathrm{CH}^d(X,q;\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\cong} H^{2d-q}_{\acute{e}t}(X,\mathbb{Z}/n\mathbb{Z}(d)).$$

In particular, $\mathrm{CH}^d(X,q;\mathbb{Z}/n\mathbb{Z})$ *is finite.*

The above theorem implies the following affirmative result on the finiteness conjecture on motivic cohomology.

Corollary 4.3. *Let X be a quasiprojective scheme over either a finite field F or a henselian discrete valuation ring with finite residue field F. Let $n > 0$ be an integer prime to* $\mathrm{char}(F)$ *and assume* $\mathbf{(BK)}^t_{X,\ell}$ *for all primes ℓ dividing n and integers $t \geq 0$. Then* $\mathrm{CH}^r(X,q;\mathbb{Z}/n\mathbb{Z})$ *is finite for all* $r \geq \dim(X)$ *and* $q \geq 0$.

Proof. For simplicity, we only treat the case over a finite field F. We may assume $n = \ell^m$ for a prime $\ell \neq \mathrm{char}(F)$. We proceed by the induction on $\dim(X)$. First we remark that the localization sequence for higher Chow groups implies that for a dense open subscheme $U \subset X$, the finiteness of $\mathrm{CH}^r(X,q;\mathbb{Z}/n\mathbb{Z})$ for all $r \geq \dim(X)$ and q is equivalent to that of $\mathrm{CH}^r(U,q;\mathbb{Z}/n\mathbb{Z})$. Thus it suffices to show the assertion for any smooth variety U over F. If U is an open subscheme of a smooth projective variety X over F, the assertion holds for X by Theorem 4.2 and hence for U by the above remark. In general Gabbers's theorem 2.6 implies that there exist an open subscheme V of a smooth projective variety X over F, an open subscheme W of U, and a finite étale morphism $\pi : V \to W$ of degree prime to ℓ. We know that the assertion holds for V so that it holds for W by a standard norm argument. This completes the proof by the above remark. □

Finally, we note that the above corollary implies the following affirmative result on the Bass conjecture. Let $K'_i(X,\mathbb{Z}/n\mathbb{Z})$ be Quillen's higher K-groups with finite coefficients constructed from the category of coherent sheaves on X (which coincide with the algebraic K-groups with finite coefficients constructed from the category of vector bundles when X is regular).

Corollary 4.4. *Under the assumption of Corollary 4.3, $K'_i(X,\mathbb{Z}/n\mathbb{Z})$ is finite for $i \geq \dim(X)-2$.*

Proof. Theorem 4.1 implies that $\mathrm{CH}^r(X,q;\mathbb{Z}/n\mathbb{Z})$ is finite for $r \leq q+1$. Hence the assertion follows from the Atiyah–Hirzebruch spectral sequence (see [25] for its construction in the most general case):

$$E_2^{p,q} = \mathrm{CH}^{-q/2}(X,-p-q;\mathbb{Z}/n\mathbb{Z}) \Rightarrow K'_{-p-q}(X,\mathbb{Z}/n\mathbb{Z}).$$

(Note that $E_2^{p,q}$ may be nonzero only if $q \leq 0$ and $p+q \leq 0$.) □

References

1. A. Altman and S. Kleiman, *Bertini theorems for hypersurface sections containing a subscheme*, Commun. Algebra **7** (1979), 775–790
2. M. Artin, A. Grothendieck and J.-L. Verdier, eds., *Séminaire de Géomírie Algébrique du Bois Marie (1963–64) – SGA4*, Lecture Notes in Mathematics, vols. 269, 270, and 305, Springer, Berlin, 1972
3. S. Bloch, *Higher algebraic K-theory and class field theory for arithmetic surfaces*, Ann. Math. **114** (1981), 229–265
4. ———, *Algebraic cycles and higher algebraic K-theory*, Adv. Math. **61** (1986), 267–304
5. S. Bloch and K. Kato, *p-adic étale cohomology*, Publ. Math. IHES **63** (1986), 107–152
6. S. Bloch and A. Ogus, *Gersten's conjecture and the homology of schemes*, Ann. Sci. Ecole. Norm. Sup. 4 série **7** (1974), 181–202
7. J.-L. Colliot-Thélène, *On the reciprocity sequence in the higher class field theory of function fields*, in: Algebraic K-Theory and Algebraic Topology (Lake Louise, AB, 1991), (J.F. Jardine and V.P. Snaith, eds), Kluwer, Dordrecht, 1993, pp. 35–55
8. J.-L. Colliot-Thélène, J.-J. Sansuc and C. Soulé, *Torsion dans le groupe de Chow de codimension deux*, Duke Math. J. **50** (1983), 763–801
9. V. Cossart, U. Jannsen and S. Saito, *Canonical embedded and non-embedded resolution of singularities for excellent two-dimensional schemes*, arxiv:0905.2191 (2009)
10. P. Deligne, *La conjecture de Weil II*, Publ. Math. IHES **52** (1981), 313–428
11. T. Geisser, *Motivic cohomology over Dedekind rings*, Math. Z. **248** (2004), 773–794
12. T. Geisser and M. Levine, *The Bloch–Kato conjecture and a theorem of Suslin–Voevodsky*, J. Reine Angew. **530** (2001), 55–103
13. M. Gros, *Sur la partie p-primaire du groupe de Chow de codimension deux*, Commun. Algebra **13** (1985) 2407–2420
14. C. Haesemeyer and C. Weibel, *Norm varieties and the chain lemma (after Markus Rost)*, in: Algebraic Topology, Abel Symposia, vol. 4, Springer, Berlin, 2009, pp. 95–130
15. L. Illusie, *Complexe de de Rham-Witt et cohomologie cristalline*, Ann. Sci. Ecole. Norm. Sup. 4 série **12** (1979), 501–661
16. ———, *On Gabber's refined uniformization*, preprint available at http://www.math.u-psud.fr/illusie/ (2008)
17. U. Jannsen, *Hasse principles for higher-dimensional fields*, arxiv:0910.2803 (2009)
18. U. Jannsen and S. Saito, *Kato homology of arithmetic schemes and higher class field theory*, Doc. Math. Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 479–538

19. ———, *Kato conjecture and motivic cohomology over finite fields*, arxiv:0910.2815 (2009)
20. U. Jannsen, S. Saito and K. Sato, *Étale duality for constructible sheaves on arithmetic schemes*, arxiv:0910.3759 (2009)
21. K. Kato, *A Hasse principle for two dimensional global fields*, J. Reine Angew. Math. **366** (1986), 142–183
22. K. Kato and S. Saito, *Unramified class field theory of arithmetic surfaces*, Ann. Math. **118** (1985), 241–275
23. ———, *Global class field theory of arithmetic schemes*, Am. J. Math. **108** (1986), 297–360
24. M. Kerz and S. Saito, *Kato conjecture and motivic cohomology for arithmetic schemes* (in preparation)
25. M. Levine, *K-theory and motivic cohomology of schemes*, preprint (1999)
26. A.S. Merkurjev and A.A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Math. USSR Izvestiya **21** (1983), 307–340
27. B. Poonen, *Bertini theorems over finite fields*, Ann. Math. **160** (2004), 1099–1127
28. M. Rost, *Chow groups with coefficients*, Doc. Math. J. **1** (1996), 319–393
29. S. Saito, *Class field theory for curves over local fields*, J. Number Theory **21** (1985), 44–80
30. ———, *Cohomological Hasse principle for a threefold over a finite field*, in: Algebraic K-Theory and Algebraic Topology, NATO ASI Series, vol. 407, Kluwer, Dordrecht, 1994, pp. 229–241
31. A. Suslin and S. Joukhovitski, *Norm varieties*, J. Pure Appl. Algebra **206** (2006), 245–276
32. A. Suslin and V. Voevodsky, *Bloch–Kato conjecture and motivic cohomology with finite coefficients*, in: Cycles, Transfer, and Motivic Homology Theories, Annals of Mathematics Studies, vol. 143, Princeton University Press, Princeton, 2000
33. N. Suwa, *A note on Gersten's conjecture for logarithmic Hodge-Witt sheaves*, K-Theory **9** (1995), 245–271
34. V. Voevodsky, *Motivic cohomology with $\mathbb{Z}/2$-coefficients*, Publ. IHES **98** (2003), 1–57
35. ———, *On motivic cohomology with $\mathbb{Z}/l$-coefficients*, K-Theory Preprint Archives, http://www.math.uiuc.edu/K-theory/0639/ (2003)
36. ———, *Motivic Eilenberg–MacLane spaces*, K-Theory Preprint Archives, http://www.math.uiuc.edu/K-theory/0864/ (2007)
37. C. Weibel, *Axioms for the norm residue isomorphism*, in: K-Theory and Noncommutative Geometry, European Mathematical Society, Zürich, 2008, pp. 427–435
38. ———, *The norm residue isomorphism theorem*, J. Topol. **2** (2009), 346–372

Elliptic Curves and Iwasawa's $\mu = 0$ Conjecture

R. Sujatha

To Parimala on the occasion of her 60th birthday

Summary The μ-invariant is a fundamental invariant in Iwasawa theory and a long-standing conjecture of Iwasawa asserts that it is zero for number fields. This can be viewed as a statement on an arithmetic Iwasawa module associated to the trivial motive. In this chapter, we discuss what the analogous conjecture should be for elliptic curves.

1 Introduction

A fundamental problem in algebraic number theory concerns the study of the absolute Galois group of the field $\mathbb{Q}$ of rational numbers. Class field theory partially resolves this problem by explicitly describing the Galois groups of the maximal abelian extension of any number field. The study of various representations of the absolute Galois group of $\mathbb{Q}$ that occur naturally in arithmetic geometry affords another approach in attacking this problem. In this note, we shall outline yet another path, which has its origins in Iwasawa theory and describes the Galois groups of certain infinite extensions of p-adic Lie extensions of a number field. This chapter is largely expository in nature, with the exception of the last part of Sect. 4, where we give a different proof of Theorem 4.7 that fits with the approach in this paper (see [17, Lemma 1] for a simpler proof). Here is how the paper is organized. We start with a brief discussion of Iwasawa's celebrated $\mu = 0$ conjecture, and show how it may also be viewed as a conjecture for the trivial Tate motive. Thereafter, we

---

R. Sujatha
School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India
e-mail: sujatha@math.tifr.res.in

2010 Mathematics subject classification. 11R23, 11G05.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_7,

explain how Iwasawa's $\mu = 0$ conjecture proves the freeness of certain pro-p Galois groups of infinite p-adic Lie extensions of $\mathbb{Q}$. We then proceed to describe the analogue of this conjecture for the motive of an elliptic curve, whose formulation was carried out in a joint work with J. Coates a few years ago ("Conjecture A" in [3]). Finally, we discuss some recent results that prove Conjecture A in special cases.

Throughout, p will denote an odd prime and $\mathbb{Z}_p$ (resp., $\mathbb{Q}_p$), will denote the ring of p-adic integers (resp., the field of p-adic numbers). Given any number field F, we shall denote by F^{cyc} the cyclotomic $\mathbb{Z}_p$-extension of F. Recall that an extension $\mathscr{L}$ of F is said to be a p-adic Lie extension if the Galois group $\mathrm{Gal}(\mathscr{L}/\mathbb{Q})$ is a p-adic Lie group [12]. The cyclotomic extension F^{cyc} is a basic example of a p-adic Lie extension of F, and has been studied extensively for over a century, culminating in Iwasawa's seminal works [8,9]. For any finite set S of primes in a number field F, F_S denotes the maximal extension of F unramified outside S. We shall always assume that S contains the set S_p of primes in F that lie above p, and the archimedean primes. Given a field L, the p-cohomological dimension of the field will be denoted by $\mathrm{cd}_p(L)$. If G is a profinite group, the Iwasawa algebra of G is denoted by $\Lambda(G)$, and we recall that it is defined as

$$\Lambda(G) = \varprojlim_{U} \mathbb{Z}_p[G/U],$$

where U runs over all open normal subgroups of G, with the inverse limit being taken with respect to the natural surjections. For any number field F, we shall denote the Galois group $\mathrm{Gal}(F^{\mathrm{cyc}}/F)$ of the cyclotomic extension by Γ. Given a discrete module M over the Iwasawa algebra $\Lambda(G)$, we denote its compact Pontryagin dual by $M^{\vee}$. For any module M over the Iwasawa algebra $\Lambda(G)$, $M(p)$ denotes the p-primary torsion submodule of M.

2 Iwasawa's $\mu = 0$ Conjecture

In this section, we describe the celebrated $\mu = 0$ conjecture of Iwasawa. To do this, we first recall the structure theorem for finitely generated modules over the Iwasawa algebra $\Lambda(G)$, where G is any group isomorphic to $\mathbb{Z}_p$. In this case, there is an isomorphism of the Iwasawa algebra $\Lambda(G)$ with the power series ring $\mathbb{Z}_p[[T]]$ in one variable, with the property that, if γ is a fixed topological generator of G, the isomorphism maps the element $\gamma - 1$ to T. If M and N are finitely generated $\Lambda(G)$-modules, then M and N are said to be *pseudoisomorphic* if there is a $\Lambda(G)$-homomorphism $f: M \to N$ with finite kernel and cokernel. The following structure theorem was proved by Iwasawa and independently by Serre (cf. [1, Chap. VII, Sect. 4]):

Theorem 2.1. *Let M be a finitely generated module over $\Lambda(G)$. Then there is a pseudoisomorphism*

$$f: M \to \Lambda(G)^r \bigoplus \left(\bigoplus_{i=1}^{k} \Lambda(G)/\mathfrak{p}_i^{n_i} \right),$$

where the $\mathfrak{p}_i$s are prime ideals of height 1. Further, the set of prime ideals $\{\mathfrak{p}_i\}$ and the set of integers $\{n_i\}$ are unique up to a bijection of the indexing set.

The integer r is called the rank of M. The importance of this theorem lies in the fact that it enables us to define two key invariants for finitely generated torsion $\Lambda(G)$-modules. Let M be a finitely generated torsion $\Lambda(G)$-module so that it has rank zero. Write $\mathfrak{p}_{i_j}$ (with $1 \leq j \leq k$) for the set of prime ideals occurring in the structure theorem such that $\mathfrak{p}_{i_j} = p$. Then the μ-invariant of M is defined as

$$\mu(M) = \sum_j n_{i_j},$$

and the λ-invariant of M is defined as

$$\lambda(M) = \mathbb{Z}_p\text{-rank of } M/M(p),$$

where $M(p)$ denotes the p-primary torsion submodule of M. Note that if $\mu(M) = 0$, then M is a finitely generated $\mathbb{Z}_p$-module. Further, as the height 1 prime ideals of $\Lambda(G)$ are principal, the *characteristic ideal* of M denoted $\mathrm{ch}_G(M)$, and defined by

$$\mathrm{ch}_G(M) := \prod_{i=1}^{k} \mathfrak{p}_i^{n_i},$$

is a principal ideal. Any generator of $\mathrm{ch}_G(M)$ is called a *characteristic power series* of M, which can be assumed to be a distinguished polynomial in $\mathbb{Z}_p[[T]]$, thanks to Weierstrass' preparation theorem. The degree of the characteristic polynomial of M is clearly the λ-invariant. If M is an arbitrary finitely generated $\Lambda(G)$-module, then we set $\mu(M) := \mu(M_{\mathrm{tors}})$ where M_{tors} is the $\Lambda(G)$-torsion submodule of M.

Let F be a number field and F^{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F, with $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F) \simeq \mathbb{Z}_p$. We denote by F_∞ the maximal abelian p-extension of F^{cyc} which is unramified everywhere. In other words, F_∞ is the p-Hilbert class field of F^{cyc}. Let X_∞ denote the Galois group $\mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. As X_∞ is abelian, it has a natural structure of a Γ-module. Indeed, given an element γ in Γ and an element x in X_∞, the action is defined by

$$\gamma.x = \tilde{\gamma} x \tilde{\gamma}^{-1},$$

where $\tilde{\gamma}$ is any lift of γ to $\mathrm{Gal}(F_\infty/F)$. It is easily checked that the action is independent of the lift since X_∞ is abelian. Further, it is well known that any $\mathbb{Z}_p$-module with a continuous Γ-action has a natural structure as a compact $\mathbb{Z}_p[[\Gamma]]$-module and thus X_∞ is a compact module over the Iwasawa algebra. The following theorem is due to Iwasawa [9].

Theorem 2.2 (Iwasawa). *X_∞ is a finitely generated torsion $\Lambda(\Gamma)$-module.*

Iwasawa further conjectured that X_∞ is a finitely generated $\mathbb{Z}_p$-module, or equivalently $\mu(X_\infty) = 0$. Ferrero and Washington [5] proved that the conjecture holds when $F/\mathbb{Q}$ is an abelian extension. For $F = \mathbb{Q}$, we have $\mathbb{Q}_\infty = \mathbb{Q}^{\mathrm{cyc}}$, and there is a unique prime of $\mathbb{Q}^{\mathrm{cyc}}$ above p as p is totally ramified in $\mathbb{Q}^{\mathrm{cyc}}$. As the ideal class group of $\mathbb{Q}$ is zero, we thus have that the group $(X_\infty)_\Gamma$ of Γ-coinvariants is trivial, and hence X_∞ is itself zero. Sinnott [16] later gave a different proof of the Ferrero-Washington theorem. It should be noted that Iwasawa gave examples of noncyclotomic $\mathbb{Z}_p$-extensions of $\mathbb{Q}$ whose p-Hilbert class fields have positive μ-invariant [10].

We shall next consider other infinite extensions of F^{cyc}. Given a finite set S of primes in F that contains S_p and the archimedean primes, we recall that F_S denotes the maximal extension of F that is unramified outside S. As the primes in S_p are the only nonarchimedean primes that ramify in F^{cyc}, we have $F_S \supseteq F^{\mathrm{cyc}}$.

Definition 2.3. $F_S(p)$ is defined to be the maximal Galois extension of F in F_S such that the Galois group $\mathrm{Gal}(F_S(p)/F)$ is pro-p.

Note that the profinite degree of $F_S/F_S(p)$ is not necessarily prime to p. Also, $F_S(p) \supseteq F^{\mathrm{cyc}}$ and $F_S(p)$ has no Galois p-extensions of F in F_S, that is, the group $H^1(\mathrm{Gal}(F_S/F_S(p)), \mathbb{Z}/p)$ is zero. For a group H, let H^{ab} denote the abelianization of H.

Definition 2.4. $F_S(p)^{\mathrm{ab}}$ is the Galois extension of F^{cyc} such that $\mathrm{Gal}(F_S(p)^{\mathrm{ab}}/F^{\mathrm{cyc}})$ equals $(\mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}}))^{\mathrm{ab}}$. We denote its Galois group by X_S.

Again, as X_S is abelian, we see that it has a structure of a $\Lambda(\Gamma)$-module, and the following theorem was proved by Iwasawa [9].

Theorem 2.5 (Iwasawa). *X_S is a finitely generated $\Lambda(\Gamma)$-module of rank $r_2(F)$, the number of complex embeddings of F. Further, $\mu(X_S) = \mu(X_\infty)$.*

3 Free Pro-p Groups and Iwasawa's $\mu = 0$ Conjecture

Recall that a free pro-p group $\mathfrak{G}$ over a set T is a pro-p group $\mathfrak{G}$, along with a map $i : T \to \mathfrak{G}$ satisfying the following properties: (1) every open subgroup of $\mathfrak{G}$ contains all but a finite number of elements of $i(T)$, and (2) if $j : T \to \tilde{\mathfrak{G}}$ is any other map with the property (1) into a pro-p group $\tilde{\mathfrak{G}}$, then there exists a unique homomorphism $f : \mathfrak{G} \to \tilde{\mathfrak{G}}$ such that $j = f \circ i$.

For any group G, let $\mathrm{cd}_p(G)$ denote the p-cohomological dimension of G. Recall that $\mathrm{cd}_p(G) = n$ if the cohomology groups $H^k(G,M)$ are trivial for all $k \geq n+1$, and all p-primary torsion modules M. In particular, if G is a pro-p group, then $\mathrm{cd}_p(G) = n$ if and only if $H^k(G,M) = 0$ for all $k > n$, and M any discrete p-primary torsion G-module. The following theorem (see [15]) characterizes free pro-p groups.

Theorem 3.1. *A pro-p group $\mathfrak{G}$ is free if and only if* $\mathrm{cd}_p(\mathfrak{G}) = 1$.

We return to the number field F. The *Weak Leopoldt Conjecture* for F^{cyc} is the assertion

$$H^2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p) = 0. \tag{3.2}$$

This is equivalent to the assertion that $H_2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}), \mathbb{Z}_p) = 0$, where H_i denotes group homology. Viewing $\mathbb{Z}_p$ as the trivial Tate motive, the Weak Leopoldt Conjecture is thus a statement on the vanishing of the second cohomology group associated to the Pontryagin dual of the trivial Tate motive. Iwasawa proved that the Weak Leopoldt Conjecture for F^{cyc} holds in general for any number field F. However, the corresponding vanishing remains unknown for other $\mathbb{Z}_p$-extensions of F. With notation as before, we have the following theorem.

Theorem 3.3. *The Galois group $G_{S,p}(F^{\mathrm{cyc}}) := \mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}})$ is a free pro-p group if and only if $\mu(X_S) = 0$ (equivalently, if $\mu(X_\infty) = 0$).*

Proof. By Theorem 2.5, it suffices to consider the $\Lambda(\Gamma)$-module X_S. Consider the long exact Galois cohomology sequence associated with

$$0 \to \mathbb{Z}/p \to \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

Suppose that $G_{S,p}(F^{\mathrm{cyc}})$ is a free pro-p group. Then by Theorem 3.1, we have $\mathrm{cd}_p(G_{S,p}(F^{\mathrm{cyc}}))$ is 1 and hence $H^2(G_{S,p}(F^{\mathrm{cyc}}), \mathbb{Z}/p) = 0$. Taking Pontryagin duals of the long exact sequence, along with the vanishing result of the Weak Leopoldt Conjecture (3.2), we see that

$$p\text{-primary torsion of } H^1(G_{S,p}(F^{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p))^\vee = 0. \tag{3.4}$$

But this implies that $G_{S,p}(F^{\mathrm{cyc}})^{\mathrm{ab}}$ has no nontrivial p-torsion, and hence clearly $\mu(X_S) = 0$. For the converse, we need to use one additional fact from Iwasawa theory, namely that the Pontryagin dual $(H^1(G_{S,p}(F^{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p))^\vee$ has no finite nonzero $\Lambda(\Gamma)$-submodule [9]. Suppose now that $\mu(X_S) = 0$. By the structure theorem for finitely generated $\Lambda(\Gamma)$-modules, it follows that the p-torsion of the Pontryagin dual is finite, and further, by the above remark, it is in fact trivial. We therefore have $H^2(G_{S,p}(F^{\mathrm{cyc}}), \mathbb{Z}/p) = 0$. But the cohomological dimension of $G_{S,p}(F^{\mathrm{cyc}})$ is at most 2, as it is a closed subgroup of $\mathrm{Gal}(F_S/F)$ which has cohomological dimension 2 [15]. The conclusion now follows from Theorem 3.1. $\square$

4 An Analogue for Elliptic Curves

The next simplest motive after the trivial Tate motive is the motive associated with an elliptic curve. Guided by the philosophy that results for the Tate motive have elliptic curve analogues, one seeks the corresponding results for elliptic curves of the material in the previous section. Let E be an elliptic curve over the number field F and as before, let p be an odd prime. We take S to be the finite set consisting of primes S_p in F that lie above p, the archimedean primes, and the primes of bad reduction for the elliptic curve. Put $G_F = \mathrm{Gal}(\overline{F}/F)$ for the absolute Galois group of F. Let

$$E_{p^\infty} := \bigcup_{n \geq 0} E_{p^n},$$

where $E_{p^n} := E_{p^n}(\overline{F})$ is the discrete G_F-module of p^n-torsion points on $E(\overline{F})$. The Tate module of E, denoted $T_p(E)$, is defined by

$$T_p(E) = \varprojlim E_{p^n},$$

and $V_p(E) = T_p(E) \otimes \mathbb{Q}_p$, is the corresponding two-dimensional $\mathbb{Q}_p$-vector space with a continuous action of G_F. For the purposes of this chapter, we shall choose to be simple minded and consider the G_F-module $V_p(E)$ as the "dual of the Tate motive of the elliptic curve E." We first discuss the analogous $\Lambda(\Gamma)$-modules in this context.

As before, let F_∞ denote the p-Hilbert class field of F^{cyc} and X_∞ the Galois group $\text{Gal}(F_\infty/F^{\text{cyc}})$. At a first glance, classical Iwasawa theory for elliptic curves suggests that the corresponding $\Lambda(\Gamma)$-module in this context is the Pontryagin dual of the Selmer group over the cyclotomic extension. Recall that for a finite Galois extension L of F, the Selmer group $S(E/L)$ of E over L is a discrete $\text{Gal}(L/F)$-module and is defined as

$$S(E/L) = \text{Ker}\left(H^1(\text{Gal}(F_S/L), E_{p^\infty})) \to \oplus_{v\in S} J_v(E/L)\right), \tag{4.1}$$

where

$$J_v(E/L) = \oplus_{w|v} H^1(\text{Gal}(\bar{L}_w/L_w), E)(p).$$

The Selmer group of E over F^{cyc} is defined as the direct limit of $S(E/L)$ as L varies over finite extensions of F in F^{cyc}. Its Pontryagin dual is denoted by $\mathfrak{X}(E/F^{\text{cyc}})$ and is well known to be a finitely generated module over $\Lambda(\Gamma)$. It is a deep conjecture due to Mazur that if E has good ordinary reduction at the primes above p, $\mathfrak{X}(E/F^{\text{cyc}})$ is a torsion $\Lambda(\Gamma)$-module and there are plenty of numerical examples known where this conjecture holds. With this knowledge, one is naturally led to wonder if $\mathfrak{X}(E/F^{\text{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module, which would be the analogue of Iwasawa's $\mu = 0$ conjecture. However, Mazur already gave examples where this is not true, and the fact that the μ-invariant of $\mathfrak{X}(E/F^{\text{cyc}})$ is not zero causes endless technical difficulties in Iwasawa theory! An explicit example is the elliptic curve $E/\mathbb{Q}$ of conductor 11, defined by

$$E : y^2 + y = x^3 - x^2 - 10x - 20.$$

For the prime $p = 5$, it is known that $\mathfrak{X}(E/\mathbb{Q}^{\text{cyc}})$ is not a finitely generated $\mathbb{Z}_p$-module. One is thus naturally led to speculate on the common ground in this context for the trivial Tate motive and the motive of an elliptic curve.

Definition 4.2. The *fine Selmer group* for E over a finite extension L of F, denoted $R(E/L)$ is defined by

$$R(E/L) = \text{Ker}\left(H^1(\text{Gal}(F_S/L), E_{p^\infty}) \to \oplus_{v\in S} K_v^1(L)\right),$$

where

$$K_v^1(E/L) = \oplus_{w|v}\, H^1(\text{Gal}(\bar{L}_w/L_w), E_{p^\infty}).$$

The fine Selmer group of E over F^{cyc}, denoted $R(E/F^{\mathrm{cyc}})$ is defined to be the direct limit of $R(E/L)$ as L varies over finite extensions of F in F^{cyc}.

The fine Selmer group $R(E/F^{\mathrm{cyc}})$ is a discrete finitely generated module over the Iwasawa algebra $\Lambda(\Gamma)$, and its compact Pontryagin dual is denoted by $\mathfrak{Y}(E/F^{\mathrm{cyc}})$. This latter module is clearly a quotient of $\mathfrak{X}(E/F^{\mathrm{cyc}})$. The Weak Leopoldt Conjecture for elliptic curves in this context is the assertion that

$$H^2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}), E_{p^\infty}) = 0. \tag{4.3}$$

This conjecture is still open and is known to be true, for instance, if $F = \mathbb{Q}$ and $E(\mathbb{Q})$ has Mordell–Weil rank at most 1. A deep result of Kato [11] proves (4.3) for all but a finite number of primes p for every elliptic curve E over $\mathbb{Q}$. If (4.3) holds, then one can show (see [3, Lemma 3.1]) that $\mathfrak{Y}(E/F^{\mathrm{cyc}})$ is a torsion $\Lambda(\Gamma)$-module. We formulated the following Conjecture jointly with Coates [3].

Conjecture 4.4 (Coates–Sujatha). $\mathfrak{Y}(E/F^{\mathrm{cyc}})$ *is a finitely generated* $\mathbb{Z}_p$*-module.*

We believe that $\mathfrak{Y}(E/F^{\mathrm{cyc}})$ is the analogue of X_∞ in this context, and that the above conjecture is the right analogue of Iwasawa's $\mu = 0$ conjecture for the motive of an elliptic curve. In fact, the Galois group X_∞ has a natural quotient X'_∞, which is the Galois group of the maximal abelian p-extension of F^{cyc} that is unramified everywhere, and in which all primes above p split completely. Note that all other primes which do not lie above p automatically split in any unramified p-extension. Iwasawa showed that $\mu(X_\infty) = \mu(X'_\infty)$. Let $F(E_{p^\infty})$ denote the Galois extension of F obtained by attaching to F the coordinates of all p-primary torsion points of $E(\overline{F})$. The following result is proved in [3, Theorem 3.4].

Theorem 4.5. *Let p be an odd prime number such that the extension $F(E_{p^\infty})/F$ is pro-p. Then Conjecture 4.4 holds for E over F^{cyc} if and only if the Iwasawa $\mu = 0$ conjecture holds for F^{cyc}.*

Thus, if Iwasawa's $\mu = 0$ conjecture were known to be true for all number fields, then Conjecture 4.4 would follow. In general however, Conjecture 4.4 turns out to be rather delicate to prove. This is to be expected, given its close relationship to Iwasawa's $\mu = 0$ conjecture. Analogous to the case of the Tate motive, one can establish the following result, which was independently noticed by Greenberg [7].

Proposition 4.6. *Assume* (4.3) *holds. Then Conjecture 4.4 is equivalent to the assertion that* $H^2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}), E_p) = 0$.

Proof. We only give a sketch of the proof. Consider the $\Lambda(\Gamma)$-modules

$$\mathscr{Z}^2(T_p(E)/F^{\mathrm{cyc}}) := \varprojlim_{F'} H^2(\mathrm{Gal}(F_S/F'), T_p(E))$$

and

$$\mathscr{Z}^2(E_p/F^{\mathrm{cyc}}) := \varprojlim_{F'} H^2(\mathrm{Gal}(F_S/F'), E_p),$$

where the inverse limit is taken with respect to the natural corestriction maps over all finite extensions F' of F contained in F^{cyc}. It can be shown (see [3]) that the modules $\mathscr{Z}^2(E_p/F^{\mathrm{cyc}})$ and $(H^2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}),E_p))^\vee$ have the same μ-invariant. Hence, the vanishing of $H^2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}),E_p)$ is equivalent to the assertion that $\mathscr{Z}^2(E_p/F^{\mathrm{cyc}})$ is finite. On the other hand, if (4.3) holds, then it can be shown [3] that $\mathscr{Z}^2(T_pE/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. Combining this with the fact that

$$\mathscr{Z}^2(T_pE/F^{\mathrm{cyc}})/p \simeq \mathscr{Z}^2(E_p/F^{\mathrm{cyc}}),$$

and that the latter has μ-invariant zero if it is finite, it is easily seen that the finiteness of $\mathscr{Z}^2(E_p/F^{\mathrm{cyc}})$ is equivalent to the assertion that $\mathscr{Z}^2(T_pE/F^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module. To complete the proof, we only need to remark that $\mathscr{Z}^2(T_pE/F^{\mathrm{cyc}})$ and $\mathfrak{Y}(E/F^{\mathrm{cyc}})$ differ by finitely generated $\mathbb{Z}_p$-modules, a fact that can be deduced from the Poitou–Tate exact sequence. □

A natural question that arises is whether Conjecture 4.4 is isogeny invariant. Though we have been unable to establish this in full generality, we shall prove the following theorem.

Theorem 4.7. *Let $E/\mathbb{Q}$ be an elliptic curve with a rational p-isogeny over $\mathbb{Q}$. Then Conjecture 4.4 holds for E/F^{cyc}.*

Proof. Let W denote the kernel of the isogeny. Put $F = \mathbb{Q}(\mu_p, W)$ for the abelian extension of $\mathbb{Q}$ defined as the composite of $\mathbb{Q}(\mu_p)$ and the trivializing extension of W. Also let $F_1 = \mathbb{Q}(E_p)$. It is easy to check that the hypothesis implies that F_1/F is a Galois p-extension. Further, as $F/\mathbb{Q}$ is abelian, Iwasawa's $\mu = 0$ conjecture holds for the Galois group of $F_\infty/F^{\mathrm{cyc}}$, where F_∞ is the maximal abelian p-extension of F^{cyc} unramified everywhere. Let $F_{S,p}$ denote the maximal pro-p quotient of $\mathbb{Q}_S/F$. By Theorem 3.3, the Galois group $\mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}})$ is free pro-p. Hence, the subgroup $\mathrm{Gal}(F_S(p)/F_1^{\mathrm{cyc}})$ is also free pro-p. By Theorem 3.1, we deduce that the cohomology groups $H^2(\mathrm{Gal}(\mathbb{Q}_S/F_1^{\mathrm{cyc}}),E_p)$ and $H^2(\mathrm{Gal}(\mathbb{Q}_S/F^{\mathrm{cyc}}),E_p)$ are trivial. Let Δ be the Galois group of $F/\mathbb{Q}$; it can also be identified with the Galois group $F^{\mathrm{cyc}}/\mathbb{Q}^{\mathrm{cyc}}$. Note that Δ has order dividing $(p-1)^2$ and is hence prime to p. From the Hochschild–Serre spectral sequence

$$H^p(\Delta, H^q(\mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}}),E_p)) \Rightarrow H^n(\mathrm{Gal}(\mathbb{Q}_S(p)/\mathbb{Q}^{\mathrm{cyc}}),E_p),$$

it immediately follows that $H^2(\mathrm{Gal}(\mathbb{Q}_S(p)/\mathbb{Q}^{\mathrm{cyc}}),E_p) = 0$. To finish the proof of the theorem, we need to prove that $H^2(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}^{\mathrm{cyc}}),E_p) = 0$, by Proposition 4.6. To this end, consider the Hochschild–Serre spectral sequence

$$H^p(\mathrm{Gal}(F_S(p)/\mathbb{Q}^{\mathrm{cyc}}), H^q(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)),E_p)) \Rightarrow H^n(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}^{\mathrm{cyc}}),E_p).$$

The module E_p is trivialized over $F_S(p)$ as the field F_1 is contained in $F_S(p)$ by our hypothesis. Thus $H^1(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)),E_p) \simeq H^1(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)),\mathbb{Z}/p) = 0$, by the definition of $F_S(p)$. Further, $H^2(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)),E_p) \simeq H^2(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)),\mathbb{Z}/p \oplus \mathbb{Z}/p) = 0$ (see [15]). Finally, since $\mathrm{cd}_p(\mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}}) = 2$, we conclude from the above Hochschild–Serre spectral sequence that $H^2(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}^{\mathrm{cyc}}), E_p) = 0$ and this completes the proof of the theorem. $\square$

We end this chapter with a few other observations. It is entirely pertinent to wonder about the analogue of Conjecture A for elliptic curves over a general $\mathbb{Z}_p$-extension. In other words, suppose that E is an elliptic curve over a number field F and that F_∞ is an arbitrary $\mathbb{Z}_p$-extension of F. As before, let S be the finite set of primes containing the primes in F that lie above p, and the primes of bad reduction for E. Let $\mathfrak{Y}(E/F_\infty)$ denote the dual of the fine Selmer group considered as a module over $\Lambda(G)$ where $G = \mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p$. Assuming that $\mathfrak{Y}(E/F_\infty)$ is a $\Lambda(G)$-torsion module, when is $\mathfrak{Y}(E/F_\infty)$ a finitely generated $\mathbb{Z}_p$-module?

Let E be an elliptic curve with complex multiplication by an imaginary quadratic field K of class number 1. Assume that E is defined over K and that the odd prime p splits into prime $p = \mathfrak{p}\mathfrak{p}^*$ in the ring of integers $\mathscr{O}_K$ of K. Let $K(E_{\mathfrak{p}^n})$ denote the field extension of K obtained by adjoining all the $\mathfrak{p}^n$-division points of E and consider the infinite Galois extension

$$K_\infty := K(E_{\mathfrak{p}^\infty}) = \bigcup_{n \geq 0} K(E_{\mathfrak{p}^n}).$$

Then $K(E_{\mathfrak{p}^\infty})$ is $\mathbb{Z}_p$-extension of $K(E_\mathfrak{p})$ and we write $G = \mathrm{Gal}(K(E_{\mathfrak{p}^\infty})/K)$ for the corresponding Galois group and $\Lambda(G)$ for the associated Iwasawa algebra. Let X_∞ be the maximal abelian p-extension of K_∞ that is unramified outside of the set of primes above $\mathfrak{p}$. It is known [13] that X_∞ is a finitely generated torsion $\Lambda(G)$-module. Let $S^\mathfrak{p}(E/K_\infty)$ (resp., $R^\mathfrak{p}(E/K_\infty)$) denote the $\mathfrak{p}$-Selmer group (resp., $\mathfrak{p}$-fine Selmer group) of E over K_∞. To be precise, these modules are defined by taking $\mathfrak{p}$ instead of p in (4.1) and Definition 4.2, respectively. Let $\mathfrak{X}^\mathfrak{p}(E/K_\infty)$ and $\mathfrak{Y}^\mathfrak{p}(E/K_\infty)$ be the respective compact duals of the Selmer group and the fine Selmer group. We then have [13]

$$S^\mathfrak{p}(E/K_\infty) = \mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty}),$$

and hence it follows that $\mathfrak{X}^\mathfrak{p}(E/K_\infty)$ and $\mathfrak{Y}^\mathfrak{p}(E/K_\infty)$ are both finitely generated $\Lambda(G)$-torsion modules. It was shown by Gillard [6] and Schneps [14] independently that X_∞ has μ-invariant zero. We denote by K_S the maximal extension of K that is unramified outside the primes of S. Let $G_{S,p}(K_\infty)$ denote the maximal pro-p quotient of the Galois group $\mathrm{Gal}(K_S/K_\infty)$. By a result of Perrin-Riou [13], it is known that the Weak Leopoldt Conjecture holds for K_∞ and the Galois modules $E_{\mathfrak{p}^\infty}$ and E_{p^∞}; in other words that

$$H^2(\mathrm{Gal}(K_S/K_\infty), E_{\mathfrak{p}^\infty}) = 0 \quad \text{and} \quad H^2(\mathrm{Gal}(K_S/K_\infty), E_{p^\infty}) = 0. \tag{4.8}$$

Arguing as in Sect. 3 (cf. Theorem 3.3), it then follows that $G_{S,p}(K_\infty)$ is free and hence has p-cohomological dimension at most 1. Further, using the Hochschild–Serre spectral sequence as in the proof of Theorem 4.7, one then sees that

$$H^2(\mathrm{Gal}(K_S/K_\infty), E_\mathfrak{p}) = 0 \quad \text{and} \quad H^2(\mathrm{Gal}(K_S/K_\infty), E_p) = 0.$$

It seems difficult to directly deduce Conjecture A for K^{cyc} or F^{cyc}, where $F = K(E_{\mathfrak{p}})$ by these methods. In [2], the following stronger conjecture was put forth (see also [4]).

Conjecture 4.9. *Let K be an imaginary quadratic field and let E be an elliptic curve defined over K such that* $\mathrm{End}_K(E) \otimes \mathbb{Q}$ *is isomorphic to K. Let p be an odd prime which splits in K, and such that E has good reduction at both primes of K above p. Then the dual Selmer group of E over K^{cyc} is a finitely generated $\mathbb{Z}_p$-module. In particular, if E is defined over $\mathbb{Q}$, the dual Selmer group of E over $\mathbb{Q}^{\mathrm{cyc}}$ is a finitely generated $\mathbb{Z}_p$-module.*

In this case, let $F = K(E_p)$ and $F_\infty = K(E_{p^\infty})$, and put $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. All we know at present is that the dual Selmer group of E over F_∞ is a finitely generated $\Lambda(H)$-module if and only if the dual Selmer group of E over F^{cyc} is a finitely generated $\mathbb{Z}_p$-module.

Acknowledgements It is a pleasure to acknowledge the hospitality provided by Postech University, Pohang, Korea, while this work was under preparation. We would also like to warmly thank YoungJu Choie for making the visit memorable, and John Coates for helpful discussions and comments on this chapter.

References

1. N. Bourbaki, Elements of Mathematics, Commutative Algebra, Chaps. 1–7, Springer, Berlin (1989)
2. J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, *The* GL_2 *main conjecture for elliptic curves without complex multiplication*, Pub. Math. IHES **101** (2005), 163–208
3. J. Coates, R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331** (2005), 809–839
4. ———, *On the $M_H(G)$-conjecture for elliptic curves* (in preparation)
5. B. Ferrero, L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. Math. **109** (1979), 377–395
6. R. Gillard, *Transformation de Mellin-Leopoldt des fonctions elliptiques*, J. Number Theory **25** (1987), 379–393
7. R. Greenberg, *Iwasawa Theory, Projective Modules, and Modular Representations*, Mem. AMS (in press)
8. K. Iwasawa, *On the theory of cyclotomic fields*, J. Math. Soc. Jpn. **20** (1964), 42–82
9. ———, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. Math. **98** (1973), 246–326
10. ———, *On the μ-invariants of Z_1-extensions*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo (1973), 1–11
11. K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques III*, Astérisque **295** (2004), 117–290
12. M. Lazard, *Groupes analytiques p-adiques*, Pub. Math. IHES **26** (1965), 389–603
13. B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Mém. Soc. Math. France (N.S.) **17** (1984)
14. L. Schneps, *On the μ-invariant of p-adic L-functions attached to elliptic curves with complex multiplication*, J. Number Theory **25** (1987), 20–33
15. J.-P. Serre, Cohomologie Galoisienne, 5th edition. Lecture Notes in Mathematics, Vol. 5. Springer, Berlin (1994)

16. W. SINNOTT, *On the* μ*-invariant of the* Γ*-transform of a rational function*, Invent. Math. **75** (1984), 273–282
17. C. WUTHRICH, *Extending Kato's result to curves with p-isogenies*, Math. Res. Lett. **13** (2006), 713–718

Cohomological Invariants of Central Simple Algebras with Involution

Jean-Pierre Tignol

To Parimala, with gratitude and admiration

Summary This survey reviews the various invariants with values in Galois cohomology groups that have been defined for involutions on central simple algebras following the model of the discriminant, Clifford invariant, and Arason invariant of quadratic forms. From the orthogonal case to the unitary case to the symplectic case, the degree of the invariants increases but their properties are similar.

This text is based on two lectures delivered in January 2009 at the conference "Quadratic forms, linear algebraic groups, and Galois cohomology" held at the

Jean-Pierre Tignol
Département de mathématique, Université catholique de Louvain, Chemin du cyclotron, 2, B-1348 Louvain-la-Neuve, Belgium
e-mail: Jean-Pierre.Tignol@uclouvain.be

2010 Mathematics subject classification. 11E72.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_8,

University of Hyderabad. The purpose was to survey the cohomological invariants that have been defined for various types of involutions on central simple algebras on the model of quadratic form invariants. I seized the occasion to make explicit some of the classification or structure results that may be expected from future invariants, and to compile a fairly extensive list of references. As this list makes clear, Parimala's contributions to the subject are all-pervasive.

Throughout these notes, F denotes a field of characteristic different from 2 and F_{s} a separable closure of F. We identify $\mu_2 := \{\pm 1\}$ with $\mathbb{Z}/2\mathbb{Z}$. For any integer $n \geq 0$, we let $H^n(F)$ be the Galois cohomology group:

$$H^n(F) := H^n(\mathrm{Gal}(F_{\mathrm{s}}/F), \mathbb{Z}/2\mathbb{Z}).$$

The Kummer exact sequence

$$1 \to \mu_2 \to F_{\mathrm{s}}^{\times} \xrightarrow{2} F_{\mathrm{s}}^{\times} \to 1$$

and Hilbert's Theorem 90 yield identifications $H^1(F) = F^{\times}/F^{\times 2}$ and $H^2(F) = {}_2\mathrm{Br}(F)$, the 2-torsion subgroup of the Brauer group of F. For $a \in F^{\times}$, we let $(a) \in H^1(F)$ denote the cohomology class given by the square class $aF^{\times 2}$. We use the notation $\cdot$ for the cup product in the cohomology ring $H^*(F)$, so for $a, b \in F^{\times}$ the Brauer class of the quaternion algebra $(a,b)_F$ is $(a) \cdot (b)$.

1 Introduction: Classification of Quadratic Forms

Various invariants are classically defined to determine whether quadratic forms over an arbitrary field F are isometric. The first invariant is of course the dimension. To obtain an invariant that vanishes on hyperbolic forms, one considers the dimension modulo 2:

$$e_0(q) = \dim q \pmod 2 \in \mathbb{Z}/2\mathbb{Z}.$$

The next invariant is the discriminant: for q a quadratic form of dimension n, we set

$$e_1(q) = (-1)^{n(n-1)/2} \det q \in F^{\times}/F^{\times 2}.$$

Thus, e_1 is well defined on the Witt group WF; but it is a group homomorphism only when restricted to the ideal IF of even-dimensional forms, which is the kernel of e_0.

In his foundational paper, Witt defined as a further invariant the Brauer class of the Clifford or even Clifford algebra (depending on which is central simple over F):

$$e_2(q) = \begin{cases} [C(q)] \in {}_2\mathrm{Br}(F) & \text{if } \dim q \text{ is even,} \\ [C_0(q)] \in {}_2\mathrm{Br}(F) & \text{if } \dim q \text{ is odd.} \end{cases}$$

The map e_2 is well defined on WF but it is a group homomorphism only on the square[1] I^2F of IF, which is the kernel of e_1.

Note that the "classical" invariants above take their values in cohomology groups:

$$\mathbb{Z}/2\mathbb{Z} = H^0(F), \quad F^\times/F^{\times 2} = H^1(F), \quad {}_2\mathrm{Br}(F) = H^2(F).$$

They were vastly generalized during the last quarter of the twentieth century: see Pfister's survey [42] for an account of the historical development of the subject. After Voevodsky's proof of the Milnor conjecture and additional work of Orlov–Vishik–Voevodsky, we have surjective homomorphisms

$$e_n\colon I^nF \to H^n(F) \quad \text{for all } n \geq 0$$

defined on n-fold Pfister forms $\langle\langle a_1,\dots,a_n\rangle\rangle := \langle 1,-a_1\rangle \otimes \cdots \otimes \langle 1,-a_n\rangle$ by

$$e_n\big(\langle\langle a_1,\dots,a_n\rangle\rangle\big) = (a_1)\cdot \cdots \cdot (a_n).$$

These homomorphisms satisfy

$$\ker e_n = I^{n+1}F \quad \text{for all } n \geq 0.$$

On the other hand, the Arason–Pfister Hauptsatz [13, Theorem 23.7] states that the dimension of any anisotropic quadratic form q representing a nonzero element in I^nF satisfies $\dim q \geq 2^n$, hence $\bigcap_n I^nF = \{0\}$. Therefore, the problem of deciding whether two quadratic forms q_1 and q_2 over F are isometric can in principle be solved by computing cohomology classes: indeed, q_1 and q_2 are isometric if and only if $\dim q_1 = \dim q_2$ and $q_1 - q_2$ is hyperbolic, and the latter condition can be checked by computing successively[2] $e_0(q_1-q_2), e_1(q_1-q_2), e_2(q_1-q_2), \dots$, which should all vanish. In view of the Arason–Pfister Hauptsatz, it actually suffices to check that $e_d(q_1-q_2) = 0$ for all $d \geq 0$ with $2^d \leq \dim q_1 + \dim q_2$.

This remarkably complete classification result is a model that we want to emulate for other algebraic objects. The problem can be formalized as follows: we are given a base field F and a functor $\mathfrak{A}\colon \mathsf{Fields}_F \to \mathsf{Sets}$ from the category of fields containing F, where the morphisms are F-algebra homomorphisms, to the category of sets. Typically, $\mathfrak{A}(K)$ is the set of K-isomorphism classes of some objects (like quadratic forms) that allow scalar extension. An *invariant* of $\mathfrak{A}$ with values in a functor $\mathfrak{H}\colon \mathsf{Fields}_F \to \mathsf{Sets}$ is a natural transformation of functors:

$$e\colon \mathfrak{A} \to \mathfrak{H}.$$

Typically, $\mathfrak{H}$ is in fact a functor to the category of abelian groups. If it is a Galois cohomology functor $\mathfrak{H}(K) = H^d(K,M)$ for some discrete Galois module M, the invariant is called a *cohomological invariant of degree d*. For examples and background information, we refer to Serre's contribution to the monograph [17]. In particular,

[1] For any integer $n \geq 2$, we let $I^nF = (IF)^n$.

[2] For $d \geq 3$, the element $e_d(q_1-q_2)$ is defined only if $e_{d-1}(q_1-q_2) = 0$.

cohomological invariants of quadratic forms are determined in [17, Sect. 17]: they are generated by the so-called Stiefel–Whitney invariants. (The invariants e_1 and e_2 above can be computed in terms of Stiefel–Whitney classes, but *not* e_i for $i \geq 3$, see [32, pp. 135, 367].)

In the present notes, we consider the case where $\mathfrak{A}(F)$ is the set of isomorphism classes of central simple F-algebras with involution, as explained in the next section. Our aim is not to describe the collection of *all* cohomological invariants of $\mathfrak{A}$, but rather to define a sequence of invariants $e_1, e_2, \dots$, each of which is defined on the subfunctor of $\mathfrak{A}$ on which the preceding invariant vanishes, just as in the case of quadratic forms. Invariants of degree 2 are essentially Brauer classes of the *Tits algebras* that arise in the representation theory of linear algebraic groups [53]. Indeed, central simple algebras with involution define torsors under adjoint classical groups (see Sect. 2), and our approach via central isogenies owes much to Tits's discussion of what he calls the β-invariant in [53, 54].

From the Bayer-Fluckiger–Parimala proof of Serre's conjecture II for classical groups [2], it follows that the invariants of degree 1 and 2 are sufficient to classify involutions over a field of cohomological dimension 1 or 2. We shall not address this topic here, and refer to [8, 35] for this classification. Below, we aim at classification results of a different kind, restricting the dimension of the algebra rather than the cohomological dimension of the center (see Theorem 3.1 for a paradigmatic case).

2 From Quadratic Forms to Involutions

In these notes, an *involution* on a ring is an antiautomorphism of order 2. The involution is said to be *of the first kind* if its restriction to the center is the identity; otherwise, this restriction is an automorphism of order 2 and the involution is said to be *of the second kind*.

Every quadratic form q on an F-vector space V defines an involution ad_q on the endomorphism algebra $\mathrm{End}_F V$, as follows: letting b denote the bilinear polar form of q, the adjoint involution $\mathrm{ad}_q \colon \mathrm{End}_F V \to \mathrm{End}_F V$ is uniquely determined by the property that

$$b\big(x, f(y)\big) = b\big(\mathrm{ad}_q(f)(x), y\big) \quad \text{for all } x, y \in V \text{ and } f \in \mathrm{End}_F V.$$

Note that the involution is really adjoint to the bilinear form, not to the quadratic form, hence we also use the notation ad_b for ad_q. Since every F-automorphism of $\mathrm{End}_F V$ is inner, it is easy to check that every F-linear involution on $\mathrm{End}_F V$ is adjoint to a nonsingular bilinear form that is either symmetric or skew-symmetric. There are therefore two types of involutions of the first kind on $\mathrm{End}_F V$, which can be distinguished by the dimension of their space of symmetric elements: the *orthogonal* involutions are adjoint to quadratic forms (or symmetric bilinear forms) and the *symplectic* involutions are adjoint to skew-symmetric bilinear forms. The involutions actually determine up to a scalar factor the form to which they are adjoint, so mapping each nonsingular symmetric or skew-symmetric form b to the adjoint involution ad_b defines bijections:

$$\boxed{\begin{array}{l}\text{nonsingular symmetric}\\ \text{bilinear forms on } V \text{ up}\\ \text{to a scalar factor}\end{array}} \quad \longleftrightarrow \quad \boxed{\begin{array}{l}\text{orthogonal involutions}\\ \text{on } \mathrm{End}_F V\end{array}}$$

and

$$\boxed{\begin{array}{l}\text{nonsingular skew-symmetric}\\ \text{bilinear forms on } V \text{ up to a}\\ \text{scalar factor}\end{array}} \quad \longleftrightarrow \quad \boxed{\begin{array}{l}\text{symplectic involutions}\\ \text{on } \mathrm{End}_F V\end{array}}$$

Central simple F-algebras are twisted forms (in the sense of Galois cohomology) of endomorphism algebras; therefore, one may also distinguish two types of involutions of the first kind on a central simple F-algebra A: an involution $\sigma\colon A \to A$ is called *orthogonal* (resp., *symplectic*) if for any splitting field K and under any K-isomorphism $A \otimes_F K \simeq \mathrm{End}_K V$, the involution $\sigma \otimes \mathrm{Id}_K$ obtained by scalar extension is adjoint to a nonsingular symmetric (resp., skew-symmetric) bilinear form. Note that symplectic involutions exist only on central simple algebras of even degree, since every skew-symmetric bilinear form on an odd-dimensional vector space is singular.

Involutions on a central simple algebra can also be obtained by adjunction, as in the split case: if we fix a representation $A = \mathrm{End}_D V$, where D is a central division F-algebra Brauer equivalent to A and V is a (right) D-vector space, and choose an involution of the first kind θ on D, then every involution of the first kind on A is adjoint to a nonsingular hermitian or skew-hermitian form on V with respect to θ, and this hermitian form is uniquely determined up to a factor in $F^\times$.

The correspondence between involutions of the first kind and bilinear forms can also be described in terms of the corresponding automorphism groups. Recall that the orthogonal group O_n is the group of isometries of the standard form $\langle 1, \dots, 1\rangle$ of dimension n:

$$\mathrm{O}_n(F) = \mathrm{Aut}(\langle 1, \dots, 1\rangle).$$

Let $H^1(F, \mathrm{O}_n)$ denote the nonabelian Galois cohomology set:

$$H^1(F, \mathrm{O}_n) = H^1\big(\mathrm{Gal}(F_{\mathrm{s}}/F), \mathrm{O}_n(F_{\mathrm{s}})\big).$$

The usual technique of nonabelian Galois cohomology (see [49, Chap. III, Sect. 1] or [29, (29.28)]) yields a canonical bijection:

$$\boxed{\begin{array}{l}\text{isometry classes of quadratic}\\ \text{forms of dimension } n \text{ over } F\end{array}} \quad \longleftrightarrow \quad H^1(F, \mathrm{O}_n). \tag{2.1}$$

This bijection maps the isometry class of the standard form to the distinguished element in $H^1(F, \mathrm{O}_n)$.

The transpose involution t on $M_n(F) = \operatorname{End}_F F^n$ is adjoint to the standard form; its automorphism group consists of the inner automorphisms $\operatorname{Int}(g)$ such that

$$\operatorname{Int}(g) \circ t = t \circ \operatorname{Int}(g).$$

This condition amounts to $\operatorname{Int}(g^{\mathrm{t}}g) = \mathrm{Id}_V$, hence to $g^{\mathrm{t}}g \in F^\times$; it defines the group $\mathrm{GO}_n(F)$ of *similitudes* of the standard form:

$$\mathrm{GO}_n(F) = \{g \in \mathrm{GL}_n(F) \mid g^{\mathrm{t}}g \in F^\times\}.$$

The automorphisms of the transpose involution are the $\operatorname{Int}(g)$ with $g \in \mathrm{GO}_n(F)$, hence

$$\operatorname{Aut}(t) = \mathrm{PGO}_n(F) := \mathrm{GO}_n(F)/F^\times.$$

Again, Galois cohomology yields a bijection (see [29, Sect. 29.F]):

$$\boxed{\begin{array}{l}\text{isomorphism classes of orthogonal}\\ \text{involutions on central simple alge-}\\ \text{bras of degree } n\end{array}} \quad \longleftrightarrow \quad H^1(F, \mathrm{PGO}_n). \tag{2.2}$$

Under this bijection, the isomorphism class of the transpose involution corresponds to the distinguished element of $H^1(F, \mathrm{PGO}_n)$. The canonical map $\mathrm{O}_n(F_{\mathrm{s}}) \to \mathrm{PGO}_n(F_{\mathrm{s}})$ yields a map $H^1(F, \mathrm{O}_n) \to H^1(F, \mathrm{PGO}_n)$. Under the bijections (2.1) and (2.2), this map carries the isometry class of any quadratic form q of dimension n to the isomorphism class of the adjoint involution ad_q on the split algebra of degree n.

In view of the close relationship between quadratic forms and (orthogonal) involutions, it may be expected that invariants for quadratic forms have counterparts for involutions. There is, however, a significant difference to keep in mind: in contrast with quadratic forms, there is no[3] direct sum of involutions. Therefore, the problem of deciding whether two involutions are isomorphic cannot be readily reduced to the problem of deciding whether an involution is hyperbolic (i.e., adjoint to a hyperbolic hermitian or skew-hermitian form).

In the next sections, we successively discuss orthogonal involutions, involutions of the second kind (also called *unitary* involutions), and symplectic involutions. In each case, some invariants with striking common features are defined.

3 Orthogonal Involutions

Any involution of the first kind on a central simple algebra A defines an isomorphism between A and its opposite algebra, hence $2[A] = 0$ in the Brauer group. Therefore, A is split if its degree is odd, and in this case every involution is orthogonal and adjoint to a quadratic form q. Upon scaling, q can be assumed to have trivial discriminant; it is then uniquely determined. (These observations also follow from the equality

[3] More exactly, direct sums of involutions are defined only with some additional data (see [11]).

$\mathrm{PGO}_n = \mathrm{O}_n$ for n odd.) Thus, the case of involutions on central simple algebras of odd degree immediately reduces to the case of quadratic forms; we shall not discuss it further.

In this section, we consider orthogonal involutions on central simple algebras of even degree. We first review in Sects. 3.1 and 3.2 the cases where the algebra has Schur index 1 or 2. A collection of invariants e_i can then be defined for all i. In the following sections, we successively discuss invariants e_1, e_2, and e_3 without restriction on the index of the algebra.

3.1 The Split Case

Just as for involutions on central simple algebras of odd degree, the case of orthogonal involutions on *split* central simple algebras of even degree reduces to the case of quadratic forms. Note that if $q \in I^d F$ for some $d \geq 1$, then for any $\lambda \in F^\times$ we have

$$q \equiv \lambda q \bmod I^{d+1}F,$$

hence $e_d(q) = e_d(\lambda q)$. Since e_d only depends on the similarity class of q, we may consider it as attached to the isomorphism class of the adjoint involution and set

$$e_d(\mathrm{ad}_q) := e_d(q) \quad \text{for } q \in I^d F.$$

We thus have a collection of invariants $(e_d)_{d\geq 1}$ of orthogonal involutions on split central simple algebras of even degree. For a given involution σ, the invariant $e_d(\sigma)$ is defined if and only if all the previous invariants $e_1(\sigma), \dots, e_{d-1}(\sigma)$ are defined and vanish.

The following theorem easily follows from corresponding results for quadratic forms. It provides us with a benchmark against which to compare the invariants we aim to define in the nonsplit case.

Theorem 3.1. *Let σ be an orthogonal involution on a* split *central simple algebra A of even degree. Let also d be an arbitrary integer, $d \geq 1$.*

Hyperbolicity: *If $\deg A < 2^{d+1}$, we have $e_i(\sigma) = 0$ for all $i = 1, \dots, d$ if and only if σ is hyperbolic.*

Decomposition: *If $\deg A = 2^{d+1}$, we have $e_i(\sigma) = 0$ for all $i = 1, \dots, d$ if and only if (A, σ) decomposes into a tensor product of quaternion algebras with involution:*

$$(A,\sigma) = (Q_1,\sigma_1) \otimes_F \cdots \otimes_F (Q_{d+1},\sigma_{d+1}).$$

Classification: *If $\deg A = 2^d$, orthogonal involutions on A with $e_i = 0$ for $i = 1, \dots, d-1$ are classified by their e_d-invariant.*

Proof. Let $\sigma = \mathrm{ad}_q$, hence $\dim q = \deg A$. We have $e_i(\sigma) = 0$ for $i = 1, \dots, d$ if and only if $q \in I^{d+1}F$, hence the hyperbolicity criterion readily follows from the Arason–Pfister Hauptsatz. If $\deg A = 2^{d+1}$ and $e_i(\sigma) = 0$ for $i = 1,\dots,d$, then q is a multiple of a $(d+1)$-fold Pfister form (see [32, Theorem X.5.6]). If $(V_1,q_1),\dots,(V_{d+1},q_{d+1})$ are two-dimensional quadratic spaces such that $q \simeq q_1 \otimes \cdots \otimes q_{d+1}$, then

$$(A,\sigma) \simeq (\mathrm{End}_F V_1, \mathrm{ad}_{q_1}) \otimes_F \cdots \otimes_F (\mathrm{End}_F V_{d+1}, \mathrm{ad}_{q_{d+1}}).$$

The right-hand side is a tensor product of (split) quaternion algebras with (orthogonal) involution. Conversely, if (A,σ) is a tensor product of quaternion algebras with involution, the solution of the Pfister factor conjecture by Becher [5] shows that q is a multiple of some $(d+1)$-fold Pfister form, hence $e_i(q) = 0$ for $i = 1,\dots,d$.

Now, suppose $\deg A = 2^d$ and $\sigma = \mathrm{ad}_q$, $\sigma' = \mathrm{ad}_{q'}$ are orthogonal involutions on A with $e_i(\sigma) = e_i(\sigma')$ for $i = 1,\dots,d-1$, that is, q, $q' \in I^dF$. Let $\lambda \in F^\times$ (resp., $\lambda' \in F^\times$) be a represented value of q (resp., q'). As observed at the beginning of this section, we have

$$e_d(\sigma) = e_d(q) = e_d(\lambda q) \quad \text{and} \quad e_d(\sigma') = e_d(q') = e_d(\lambda' q').$$

If $e_d(\sigma) = e_d(\sigma')$, then $\lambda q - \lambda' q' \in I^{d+1}F$. But since λq and $\lambda' q'$ both represent 1, the dimension of the anisotropic kernel of $\lambda q - \lambda' q'$ is bounded as follows:

$$\dim(\lambda q - \lambda' q')_{\mathrm{an}} \le 2\deg A - 2 < 2^{d+1}.$$

By the Arason–Pfister Hauptsatz it follows that $\lambda q \simeq \lambda' q'$, hence σ and σ' are isomorphic. $\square$

Remark 3.2. A result of Jacobson [24, Theorem 3.12] (see also [37]) on quadratic forms of dimension 6 with trivial discriminant also shows that orthogonal involutions with $e_1 = 0$ on a split central simple algebra of degree 6 are classified by their e_2-invariant (see also Theorem 3.10). As pointed out by Becher, the classification result in Theorem 3.1 may hold under much less stringent conditions on $\deg A$; it might be interesting to determine exactly in which degrees orthogonal involutions with $e_i = 0$ for $i = 1,\dots,d-1$ are classified by their e_d-invariant.

3.2 *The Case of Index 2*

In this section, we assume that the Schur index $\mathrm{ind} A$ is 2, that is, A is Brauer equivalent to some quaternion division F-algebra Q. Then A can be represented as

$$A = \mathrm{End}_Q V$$

for some right Q-vector space V of dimension $\dim_Q V = (1/2)\deg A$, and every orthogonal involution σ on A is adjoint to some skew-hermitian form h on V with respect to the conjugation involution on Q. The form h is uniquely determined up to a factor in $F^{\times}$. Berhuy [6] defined a complete system of invariants for skew-hermitian forms over Q, which readily yield invariants of orthogonal involutions on A since these invariants are constant on similarity classes of skew-hermitian forms. The idea is to extend scalars to the function field $F(X)$ of the Severi-Brauer variety X of Q (this variety is a projective conic) and to use the fact that the unramified cohomology of $F(X)$ comes from F.

More precisely, if σ is an orthogonal involution on A, then after scalar extension to $F(X)$ the involution $\sigma_{F(X)}$ is an orthogonal involution on the split algebra $A_{F(X)}$. If $e_i(\sigma_{F(X)})$ is defined for some $i \geq 1$, then it actually lies in the unramified subgroup $H^i_{nr}\big(F(X)\big)$, and Berhuy [6, Proposition 9] shows that there is a unique element

$$e_i(\sigma) \in \begin{cases} H^1(F) & \text{if } i = 1, \\ H^i(F, \mu_4^{\otimes i-1})/[A] \cdot H^{i-2}(F) & \text{if } i \geq 2 \end{cases}$$

such that

$$e_i(\sigma)_{F(X)} = e_i(\sigma_{F(X)}).$$

Note that for $i \geq 2$, the group $[A] \cdot H^{i-2}(F)$ can be identified with the kernel of the scalar extension map $H^i(F, \mu_4^{\otimes i-1}) \to H^i(F(X), \mu_4^{\otimes i-1})$, as shown in the proof of Berhuy [6, Proposition 9].

Theorem 3.3. *Let σ be an orthogonal involution on a central simple algebra A of index 2 and let d be an arbitrary integer, $d \geq 1$:*

(1) If $\deg A < 2^{d+1}$, we have $e_i(\sigma) = 0$ for all $i = 1, \dots, d$ if and only if σ is hyperbolic.
(2) If $\deg A = 2^{d+1}$, we have $e_i(\sigma) = 0$ for all $i = 1, \dots, d$ if and only if (A, σ) decomposes into a tensor product of quaternion algebras with involution:

$$(A, \sigma) = (Q_1, \sigma_1) \otimes_F \cdots \otimes_F (Q_{d+1}, \sigma_{d+1}).$$

Proof. By definition of $e_i(\sigma)$, we have $e_i(\sigma) = 0$ if and only if $e_i(\sigma_{F(X)}) = 0$. The hyperbolicity criterion (1) follows from the split case (Theorem 3.1) since Parimala–Sridharan–Suresh [41] and Dejaiffe [12] have proved that $\sigma_{F(X)}$ is hyperbolic if and only if σ is hyperbolic. Likewise, in case (2), Theorem 3.1 shows that $(A, \sigma)_{F(X)}$ decomposes into a tensor product of quaternion algebras with involution. By a theorem of Becher [5, Theorem 2], it follows that (A, σ) has a similar decomposition. (Becher's theorem also shows that the decomposition can be chosen in such a way that $Q_1 = Q$ is the quaternion algebra Brauer equivalent to A and Q_i is split for $i \geq 2$.) □

I do not know whether the analogue of the classification result from Theorem 3.1 holds for algebras of index 2 (except for the cases of low degree discussed in Theorems 3.6 and 3.10). The issue is whether skew-hermitian forms over Q are similar when they are similar after scalar extension to $F(X)$.

3.3 Discriminant

Let n be an even integer, $n = 2m$. A first invariant of orthogonal involutions on central simple algebras of degree n arises from the fact that PGO_n is not connected: if $g \in \mathrm{GO}_n(F)$, say $g^t g = \lambda \in F^\times$, then $(\det g)^2 = \lambda^n$, hence $\det g = \pm\lambda^m$. The map $g \mapsto \lambda^m(\det g)^{-1} \in \mu_2$ yields a homomorphism $\delta\colon \mathrm{PGO}_n(F) \to \mu_2$, hence an exact sequence of algebraic groups

$$1 \to \mathrm{PGO}_n^+ \to \mathrm{PGO}_n \xrightarrow{\delta} \mu_2 \to 1. \tag{3.4}$$

We thus get a map

$$\delta^1 : H^1(F, \mathrm{PGO}_n) \to H^1(F) = F^\times/F^{\times 2}, \tag{3.5}$$

which defines the *determinant* of orthogonal involutions on central simple algebras of degree n. The *discriminant* is the determinant with a change of sign if m is odd: for σ an orthogonal involution on a central simple algebra of degree n, we set

$$e_1(\sigma) = \operatorname{disc}\sigma = (-1)^{n/2}\det\sigma \in F^\times/F^{\times 2}.$$

Alternatively, the discriminant can be directly obtained by substituting in the discussion earlier the group $\mathrm{PGO}(m\mathbb{H})$ of the hyperbolic space of dimension n for PGO_n. *Since the discriminant is more useful than the determinant for our purposes, we change notation and let henceforth*

$$\mathrm{PGO}_{2m} = \mathrm{PGO}(m\mathbb{H}).$$

The determinant and discriminant of quadratic forms can be defined similarly from the exact sequence

$$1 \to \mathrm{O}_n^+ \to \mathrm{O}_n \xrightarrow{\delta} \mu_2 \to 1.$$

Therefore, for any quadratic form q of dimension n,

$$\det \mathrm{ad}_q = \det q \quad \text{and} \quad \operatorname{disc}\mathrm{ad}_q = \operatorname{disc} q.$$

It follows that the e_1-invariant defined earlier coincides with the e_1-invariant defined in Sects. 3.1 and 3.2 when $\operatorname{ind} A \le 2$.

Knus–Parimala–Sridharan [30] give a nice direct definition of the determinant: if σ is an orthogonal involution on a central simple algebra A of even degree, they show that all the skew-symmetric units have the same reduced norm up to squares and that

$$\det\sigma = \mathrm{Nrd}_A(a)F^{\times 2} \quad \text{for any } a \in A^\times \text{ such that } \sigma(a) = -a.$$

In a slightly different form, this formula already appears in Tits's seminal work [52, Sect. 2.6].

This first invariant is of course rather weak. Yet, we have the following result.

Theorem 3.6. *Let σ be an orthogonal involution on a central simple algebra A:*

(a) If $\deg A < 4$ *(i.e., A is a quaternion algebra), σ is hyperbolic if and only if* $e_1(\sigma) = 0$.

(b) If $\deg A = 4$, *then* $e_1(\sigma) = 0$ *if and only if A decomposes as a tensor product of quaternion algebras with involution:*

$$(A, \sigma) = (Q_1, \sigma_1) \otimes (Q_2, \sigma_2). \tag{3.7}$$

(c) If $\deg A = 2$, *orthogonal involutions on A are classified by their e_1-invariant.*

Part (b) was first observed by Knus–Parimala–Sridharan [30]. Note that in any decomposition of the form (3.7), the involutions σ_1 and σ_2 are of the same type (orthogonal or symplectic) since σ is orthogonal. However, when there is any decomposition of the type (3.7), there is one where σ_1 and σ_2 are the quaternion conjugations (which are the unique symplectic involutions on Q_1 and Q_2). The subalgebras Q_1 and Q_2 are then uniquely determined by σ (see [29, p. 215]) (or (3.11)).

3.4 Clifford Algebras

An analogue of the even Clifford algebra of quadratic forms has been defined for orthogonal involutions by Jacobson [23] (by Galois descent) and by Tits [52] (rationally) (see also [29, Sect. 8]). For σ an orthogonal involution on a central simple F-algebra A of degree $n = 2m$, the Clifford algebra $C(A, \sigma)$ has dimension 2^{n-1} and its center $Z(A, \sigma)$ is isomorphic to $F(\sqrt{\operatorname{disc}\sigma})$ if $\operatorname{disc}\sigma \neq 1$, to $F \times F$ if $\operatorname{disc}\sigma = 1$. It is simple if $Z(A, \sigma)$ is a field and is a direct product of two central simple F-algebras $C_+(A, \sigma)$ and $C_-(A, \sigma)$ of degree 2^{m-1} if $Z(A, \sigma) \simeq F \times F$. For any quadratic form q on an F-vector space V of even dimension, we have

$$C(\operatorname{End}_F V, \operatorname{ad}_q) = C_0(q).$$

If $\operatorname{disc} q = 1$, then $C_+(\operatorname{End}_F V, \operatorname{ad}_q)$ and $C_-(\operatorname{End}_F V, \operatorname{ad}_q)$ are isomorphic and Brauer equivalent to the full Clifford algebra $C(q)$.

The construction of the Clifford algebra $C(A, \sigma)$ is functorial and may be used to obtain a second invariant of orthogonal involutions of even degree and trivial discriminant in the same spirit as the Witt invariant of quadratic forms, as we proceed to show.

The set of isomorphism classes of orthogonal involutions of trivial discriminant on central simple algebras of even degree $n = 2m$ corresponds under the bijection (2.2) to the kernel of the map δ^1 of (3.5), which is the image of $H^1(F, \mathrm{PGO}_n^+)$ in $H^1(F, \mathrm{PGO}_n)$. These involutions can therefore be classified by $H^1(F, \mathrm{PGO}_n^+)$, but the map $H^1(F,\mathrm{PGO}_n^+) \to H^1(F,\mathrm{PGO}_n)$ is generally *not* injective: a given central simple F-algebra A of degree n with an orthogonal involution σ of trivial discriminant can be the image of two different elements in $H^1(F,\mathrm{PGO}_n^+)$, depending on the choice of an F-algebra isomorphism $\varphi\colon Z(A,\sigma) \xrightarrow{\sim} F\times F$. We thus have a bijection:

$$\boxed{\begin{array}{l}\text{isomorphism classes of triples}\\ (A,\sigma,\varphi)\text{ as above}\end{array}} \quad\longleftrightarrow\quad H^1(F,\mathrm{PGO}_n^+).$$

If φ, $\varphi'\colon Z(A,\sigma) \xrightarrow{\sim} F\times F$ are the two different isomorphisms, the triples (A,σ,φ) and (A,σ,φ') are isomorphic if and only if (A,σ) has an automorphism whose induced action on $C(A,\sigma)$ swaps the two components or, equivalently, if A contains an improper similitude, that is, an element g such that $\sigma(g)g\in F^\times$ and $\mathrm{Nrd}_A(g) = -(\sigma(g)g)^{n/2}$. This readily follows from the exact sequence below, which is a part of the cohomology sequence derived from a twisted version of (3.4):

$$\mathrm{PGO}(A,\sigma) \xrightarrow{\delta} \mu_2 \to H^1(F,\mathrm{PGO}^+(A,\sigma)) \to H^1(F,\mathrm{PGO}(A,\sigma)) \xrightarrow{\delta^1} H^1(F).$$

In particular, if A is split, then the triples (A,σ,φ) and (A,σ,φ') are isomorphic.

The group PGO_n^+ has a simply connected cover Spin_n and we have an exact sequence of algebraic groups:

$$1 \to \mu \to \mathrm{Spin}_n \to \mathrm{PGO}_n^+ \to 1, \tag{3.8}$$

where μ is the center of Spin_n:

$$\mu = \begin{cases}\mu_4 & \text{if } n\equiv 2 \bmod 4,\\ \mu_2\times\mu_2 & \text{if } n\equiv 0 \bmod 4.\end{cases}$$

The cohomology sequence associated to (3.8) yields a map

$$\partial\colon H^1(F,\mathrm{PGO}_n^+) \to H^2(F,\mu),$$

which can be viewed as a cohomological invariant of degree 2 of algebras with orthogonal involution of trivial discriminant – except that one has to factor out the effect of changing (A,σ,φ) into (A,σ,φ'). The images under ∂ of the elements in $H^1(F,\mathrm{PGO}_n^+)$ corresponding to (A,σ,φ) and (A,σ,φ') are

$$[C_+(A,\sigma)] \text{ and } [C_-(A,\sigma)] \in H^2(F,\mu_4) \subset \mathrm{Br}(F) \quad \text{if } n\equiv 2 \bmod 4,$$

and, if $n\equiv 0 \bmod 4$,

$$\big([C_+(A,\sigma)],[C_-(A,\sigma)]\big) \text{ and } \big([C_-(A,\sigma)],[C_+(A,\sigma)]\big) \in H^2(F)\times H^2(F).$$

When $n\equiv 2 \bmod 4$, we have (see [29, (9.15) and (9.16)])

$$2[C_+(A,\sigma)] = 2[C_-(A,\sigma)] = [A] \quad\text{and}\quad [C_+(A,\sigma)]+[C_-(A,\sigma)] = 0. \tag{3.9}$$

When $n \equiv 0 \bmod 4$, we have (see [29, (9.13) and (9.14)])

$$2[C_+(A,\sigma)] = 2[C_-(A,\sigma)] = 0 \quad \text{and} \quad [C_+(A,\sigma)] + [C_-(A,\sigma)] = [A].$$

Thus, in both cases, we have

$$[C_+(A,\sigma)] - [C_-(A,\sigma)] = [A].$$

Therefore, letting B_A^2 denote the subgroup of $\mathrm{Br}(F)$ generated by $[A]$, that is, $B_A^2 = \{0,[A]\} = [A] \cdot H^0(F)$, we may set

$$e_2(\sigma) = [C_+(A,\sigma)] + B_A^2 = [C_-(A,\sigma)] + B_A^2 \in \mathrm{Br}(F)/B_A^2.$$

If q is a quadratic form of trivial discriminant on an even-dimensional vector space V, we have $B_{\mathrm{End}V}^2 = \{0\}$ and

$$e_2(\mathrm{ad}_q) = e_2(q) \in H^2(F).$$

Therefore, the e_2-invariant defined earlier coincides with the e_2-invariant of Sects. 3.1 and 3.2 when $\mathrm{ind}A \leq 2$.

Theorem 3.10. *Let σ be an orthogonal involution on a central simple F-algebra A of even degree:*

(a) If $\deg A < 8$, *then* $e_1(\sigma) = e_2(\sigma) = 0$ *if and only if σ is hyperbolic.*
(b) If $\deg A = 8$, *then* $e_1(\sigma) = e_2(\sigma) = 0$ *if and only if (A,σ) has a decomposition of the form*

$$(A,\sigma) = (Q_1,\sigma_1) \otimes_F (Q_2,\sigma_2) \otimes_F (Q_3,\sigma_3)$$

for some quaternion F-algebras Q_1, Q_2, Q_3.
(c) If $\deg A = 4$ *or* 6, *orthogonal involutions on A with $e_1 = 0$ are classified by their e_2-invariant.*
(d) If $\deg A \equiv 2 \bmod 4$, *then* $(A,\sigma) \simeq (\mathrm{End}_F V, \mathrm{ad}_q)$ *for some quadratic form $q \in I^3F$ if and only if $e_2(\sigma) = 0$.*

Sketch of proof. If $\deg A = 4$, the two components $C_\pm(A,\sigma)$ of the Clifford algebra are quaternion algebras. Letting $\sigma_\pm$ denote the quaternion conjugation on $C_\pm(A,\sigma)$, we have a decomposition

$$(A,\sigma) \simeq (C_+(A,\sigma),\sigma_+) \otimes_F (C_-(A,\sigma),\sigma_-), \tag{3.11}$$

which arises from the coincidence of Dynkin diagrams $D_2 = A_1 \times A_1$ (see [29, (15.12)]). Since $e_2(\sigma)$ determines the pair $\{C_+(A,\sigma), C_-(A,\sigma)\}$, it follows that orthogonal involutions of trivial discriminant on A are classified by their e_2-invariant. If $C_+(A,\sigma)$ or $C_-(A,\sigma)$ is split, then the corresponding involution σ_+ or σ_- is hyperbolic, hence σ also is hyperbolic.

If $\deg A = 6$, then $C_+(A,\sigma)$ and $C_-(A,\sigma)$ are central simple F-algebras of degree 4. The exterior power construction λ^2 yields a central simple F-algebra

$\lambda^2 C_+(A,\sigma)$ (resp., $\lambda^2 C_-(A,\sigma)$) of degree 6 endowed with a canonical involution γ_+ (resp., γ_-). As a consequence of the coincidence of Dynkin diagrams $D_3 = A_3$ (see [29, (15.32)]), we have isomorphisms

$$(A,\sigma) \simeq (\lambda^2 C_+(A,\sigma),\gamma_+) \simeq (\lambda^2 C_-(A,\sigma),\gamma_-).$$

Since $e_2(\sigma)$ determines the pair $\{[C_+(A,\sigma)],[C_-(A,\sigma)]\}$, it follows that orthogonal involutions of trivial discriminant on A are classified by their e_2-invariant.

Now, suppose $\deg A \equiv 2 \bmod 4$. If $C_+(A,\sigma)$ is split, it follows from (3.9) that $[A] = 0$. Similarly, if $[C_+(A,\sigma)] = [A]$, then since (3.9) shows that $2[C_+(A,\sigma)] = [A]$ it follows that $[C_+(A,\sigma)] = [A] = 0$. Therefore, in each case we have $(A,\sigma) \simeq (\operatorname{End}_F V, \operatorname{ad}_q)$ for some quadratic form q, and

$$e_2(q) = e_2(\sigma) = 0,$$

hence $q \in I^3 F$. In particular, if $\deg A = 6$ we have $\dim q = 6$, hence q is hyperbolic.

Finally, (b) is a consequence of triality (see [29, Sect. 42.B]), which shows that for the canonical involutions σ_+, σ_- on $C_+(A,\sigma)$, $C_-(A,\sigma)$, we have

$$C\big(C_+(A,\sigma),\sigma_+\big) \simeq (A,\sigma) \times (C_-(A,\sigma),\sigma_-).$$

If $C_+(A,\sigma)$ is split, then (A,σ) is isomorphic to one of the components of the even Clifford algebra of a quadratic form of dimension 8, from which the existence of a decomposition easily follows. □

In view of part (d) of Theorem 3.10, the case of orthogonal involutions with $e_1 = e_2 = 0$ on central simple algebras of degree $2 \pmod 4$ is reduced to the split case. We thus have invariants e_i as in Sect. 3.1, and Theorem 3.1 applies. Therefore, in the rest of this section, we only consider central simple algebras of degree $0 \pmod 4$.

3.5 Higher Invariants

The hope to define further invariants of orthogonal involutions on the model of the Arason e_3-invariant of quadratic forms was dashed by an example of Quéguiner-Mathieu [45] or [4, Sect. 3.4]. The following variation on Quéguiner-Mathieu's example was suggested by Becher: consider quaternion algebras with orthogonal involutions (Q_1,σ_1), (Q_2,σ_2), and (Q_3,σ_3) over an arbitrary field F, and let

$$(A,\sigma) = (Q_1,\sigma_1) \otimes_F (Q_2,\sigma_2) \otimes_F (Q_3,\sigma_3).$$

Suppose A is division. We have $\operatorname{disc}\sigma = 1$ and, as observed in Theorem 3.10, $e_2(\sigma) = 0$. Suppose we could find a functorial invariant $e_3(\sigma)$ in some quotient $H^3(F)/E(A)$ of $H^3(F)$, and let

$$e_3(\sigma) = \sum_i (a_i)\cdot(b_i)\cdot(c_i) + E_A \quad \text{for some } a_i, b_i, c_i \in F^\times.$$

Let K be the function field of the product of the quadrics:

$$x_0^2 - a_i x_1^2 - b_i x_2^2 + a_i b_i x_3^2 - c_i x_4^2 = 0.$$

We have $e_3(\sigma)_K = 0$, hence $e_3(\sigma_K) = 0$ by functoriality. Now, a theorem of Merkurjev on the index reduction of central simple algebras over the function field of quadrics [13, Corollary 30.10] shows that A_K is a division algebra. After scalar extension to its generic splitting field L, which is the field of functions on the Severi-Brauer variety of A_K, we have

$$(A_K, \sigma_K)_L \simeq (\mathrm{End}_L V, \mathrm{ad}_{q_\sigma})$$

for some eight-dimensional quadratic form q_σ over L, which must be anisotropic by a theorem of Karpenko [27]. But since $e_1(\sigma_K) = e_2(\sigma_K) = e_3(\sigma_K) = 0$, functoriality yields $e_i(q_\sigma) = 0$ for $i = 1,2,3$, hence q_σ is hyperbolic: this is a contradiction.

The same idea can be used more generally to prove that there is no functorial invariant $e_3(\sigma)$ in a quotient of a cohomology group $H^3(F,M)$ of any torsion module M, because F has an extension K of cohomological dimension 2 such that A_K is a division algebra (see [39, Proof of Theorem 4]).

On the other hand, Rost defined for all simply connected algebraic groups a cohomological invariant of degree 3 that generalizes the Arason invariant in the following sense: the Rost invariant of any element $\xi \in H^1(F, \mathrm{Spin}_n)$ is the Arason invariant of the quadratic form of dimension n corresponding to the image of ξ in $H^1(F, \mathrm{O}_n)$. The Rost invariant of Spin groups can be used to define a *relative* invariant of orthogonal involutions, as was shown by Garibaldi [15]. (Bayer-Fluckiger and Parimala [3] used a similar technique to obtain a relative invariant of hermitian forms.) We next describe his procedure.

Suppose σ_0 is a given orthogonal involution with $e_1(\sigma_0) = e_2(\sigma_0) = 0$ on a central simple algebra A of degree $0 \pmod 4$. We consider the twisted version of (3.8)

$$1 \to \mu_2 \times \mu_2 \to \mathrm{Spin}(A,\sigma_0) \to \mathrm{PGO}^+(A,\sigma_0) \to 1$$

and the associated cohomology sequence

$$H^1(F) \times H^1(F) \to H^1\big(F, \mathrm{Spin}(A,\sigma_0)\big) \to H^1\big(F, \mathrm{PGO}^+(A,\sigma_0)\big) \xrightarrow{\partial} H^2(F) \times H^2(F). \tag{3.12}$$

Let σ be another involution on A with $e_1(\sigma) = e_2(\sigma) = 0$. As observed in Sect. 3.4 (in the nontwisted case), the cohomology class in $H^1\big(F, \mathrm{PGO}(A,\sigma_0)\big)$ associated with (A,σ) lifts in two ways to $H^1\big(F, \mathrm{PGO}^+(A,\sigma_0)\big)$, to cohomology classes η, η' corresponding to triples (A,σ,φ), (A,σ,φ'), where φ and φ' are the two F-algebra isomorphisms $Z(A,\sigma) \xrightarrow{\sim} Z(A,\sigma_0)$ $(\simeq F \times F)$. The images of η, η' under ∂ are the two components of $C(A,\sigma) \otimes_{Z(A,\sigma_0)} C(A,\sigma_0)$, where the tensor product is taken with respect to the isomorphism φ or φ'; we thus get for $\partial(\eta)$ and $\partial(\eta')$ the pairs

$$\big([C_+(A,\sigma) \otimes_F C_+(A,\sigma_0)], [C_-(A,\sigma) \otimes_F C_-(A,\sigma_0)]\big)$$

and

$$\big([C_-(A,\sigma)\otimes_F C_+(A,\sigma_0)],[C_+(A,\sigma)\otimes_F C_-(A,\sigma_0)]\big).$$

Since $e_2(\sigma)=0$, one of the components $C_\pm(A,\sigma)$ is split and the other is Brauer equivalent to A. The same holds for σ_0 since $e_2(\sigma_0)=0$; therefore, we have $\partial(\eta)=0$ or $\partial(\eta')=0$, and at least one of η,η' lifts to some $\xi\in H^1\big(F,\mathrm{Spin}(A,\sigma_0)\big)$. The analysis of the exact sequence (3.12) given in [15] shows how the Rost invariant of ξ varies when a different lift ξ' is chosen: the difference of Rost invariants $R(\xi)-R(\xi')$ lies in the subgroup $B_A^3\subset H^3(F,\mu_4^{\otimes 2})$, which is defined to be the image under the injection $H^3(F)\hookrightarrow H^3(F,\mu_4^{\otimes 2})$ of the subgroup

$$[A]\cdot H^1(F)=\{[A]\cdot(\lambda)\mid \lambda\in F^\times\}\subset H^3(F).$$

Therefore, a relative e_3-invariant of involutions with $e_1=e_2=0$ on A is defined by

$$e_3(\sigma/\sigma_0)=R(\xi)+B_A^3\in H^3(F,\mu_4^{\otimes 2})/B_A^3.$$

In the particular case where the Schur index $\operatorname{ind}A$ divides $(1/2)\deg A$, that is, when $A\simeq M_2(A')$ for some central simple algebra A', we may choose for σ_0 a hyperbolic involution and thus consider $e_3(\sigma/\sigma_0)$ as an absolute invariant $e_3(\sigma)$. When $(A,\sigma)\simeq(\mathrm{End}_F V,\mathrm{ad}_q)$, we have $B_A^3=\{0\}$ and

$$e_3(\mathrm{ad}_q)=e_3(q)$$

in view of the relation between the Rost and the Arason invariants. Therefore, the e_3-invariant defined earlier coincides with the e_3-invariant of Sects. 3.1 and 3.2 when $\operatorname{ind}A\le 2$.

In the case where $\deg A=8$ (and $\operatorname{ind}A$ divides 4), an explicit computation of the e_3-invariant was recently obtained by Quéguiner-Mathieu and Tignol: if $e_1(\sigma)=e_2(\sigma)=0$, we may find a decomposition

$$(A,\sigma)\simeq(M_2(F),\mathrm{ad}_{\langle\langle\lambda\rangle\rangle})\otimes_F(D,\theta)$$

for some $\lambda\in F^\times$, some central simple F-algebra D of degree 4, and some orthogonal involution θ on D such that the quaternion F-algebra $(\operatorname{disc}\theta,\lambda)_F$ is split: see [5] if $\operatorname{ind}A=1$ or 2 and [38] if $\operatorname{ind}A=4$. The Clifford algebra $C(D,\theta)$ is a quaternion algebra over a quadratic étale F-algebra Z, which is isomorphic to $F(\sqrt{\operatorname{disc}\theta})$ if $\operatorname{disc}\theta\neq 1$ and to $F\times F$ if $\operatorname{disc}\theta=1$. Therefore, we may find an element $\ell\in Z$ such that $N_{Z/F}(\ell)=\lambda$. The e_3-invariant is

$$e_3(\sigma)=\mathrm{cor}_{Z/F}\big((\ell)\cdot[C(D,\theta)]\big)+B_A^3\in H^3(F)/B_A^3,$$

as can be seen by extending scalars to the function field F_A of the Severi-Brauer variety of A, since the map $H^3(F)/B_A^3\to H^3(F_A)$ induced by scalar extension from F to F_A is injective. (Note that in this special case where $\deg A=8$ and one of the components of the Clifford algebra is split, the Rost invariant has exponent 2, see [17, p. 146].)

Theorem 3.13. *Let σ be an orthogonal involution on a central simple algebra A of even degree with* $\mathrm{ind}A \mid (1/2)\deg A$. *If* $\deg A < 16$*, the involution σ is hyperbolic if and only if* $e_1(\sigma) = e_2(\sigma) = e_3(\sigma) = 0$.

Proof. The "only if" part is clear. We may thus assume $e_i(\sigma) = 0$ for $i = 1,2,3$, and we have to show that σ is hyperbolic. If $\deg A < 8$, the theorem follows from Theorem 3.10(a). If A is split (which, by Theorem 3.10(d), occurs in particular when $\deg A \equiv 2 \pmod 4$), the theorem follows from Theorem 3.1. Likewise, the theorem follows from Theorem 3.3 if $\mathrm{ind}A = 2$. Therefore, it suffices to consider the case where $\deg A = 8$ and $\mathrm{ind}A = 4$. Let F_A be the function field of the Severi-Brauer variety of A. Since A splits over F_A, and since the theorem holds in the split case, $(A,\sigma)_{F_A}$ is hyperbolic. It follows that σ is hyperbolic by a theorem of Sivatski [50, Proposition 3] (based on a result of Laghribi [31, Théorème 4]). □

Theorem 3.13 yields the expected hyperbolicity criterion for $\deg A < 16$, under the hypothesis that $\mathrm{ind}A \mid (1/2)\deg A$ (which is necessary for σ to be hyperbolic). Whether the decomposition criterion holds when $\deg A = 16$ is an open question, which is addressed by Garibaldi [15]. By contrast, Quéguiner-Mathieu and Tignol have used an example of Hoffmann [22] and a result of Sivatski [50, Proposition 4] to construct nonisomorphic orthogonal involutions σ, σ' on a central simple algebra A of degree 8 and index 4 such that

$$e_1(\sigma) = e_1(\sigma') = e_2(\sigma) = e_2(\sigma') = 0 \quad \text{and} \quad e_3(\sigma) = e_3(\sigma'),$$

hence the classification criterion does *not* hold in degree 8. If σ_0 is a fixed orthogonal involution with $e_1(\sigma_0) = e_2(\sigma_0) = 0$ on a central simple algebra A of degree 8 and index 4, orthogonal involutions σ on A with $e_1(\sigma) = e_2(\sigma) = 0$ and $e_3(\sigma) = e_3(\sigma_0)$ are classified by a relative invariant:

$$e_4(\sigma/\sigma_0) \in H^4(F)/B^4_{\sigma_0},$$

where

$$B^4_{\sigma_0} = \{(a)\cdot e_3(\sigma_0) \mid a \in F^\times,\ (a)\cdot[A] = 0\}.$$

Garibaldi [15] shows how to use the Rost invariant of groups of type E_8 to obtain an *absolute* e_3-invariant for orthogonal involutions on central simple algebras of degree 16.

4 Unitary Involutions

Let $K = F(\sqrt{a})$ be a quadratic field extension of F with nontrivial automorphism ι. For each integer $n \geq 1$, let h_n be the n-dimensional hermitian form over K with maximal Witt index, defined for $x = (x_1,\dots,x_n)$ and $y = (y_1,\dots,y_n) \in K^n$ by

$$h_n(x,y) = \iota(x_1)y_1 - \iota(x_2)y_2 + \cdots - (-1)^n\iota(x_n)y_n = \iota(x)\cdot d_n\cdot y^{\mathrm{t}},$$

where d_n is the diagonal matrix of order n:

$$d_n := \mathrm{diag}(1,-1,\dots,-(-1)^n).$$

Let also $\tau\colon M_n(K) \to M_n(K)$ be the unitary involution defined by

$$\tau(m) = d_n^{-1}\cdot\iota(m)^{\mathrm{t}}\cdot d_n \quad \text{for } m\in M_n(K).$$

The unitary group $\mathrm{U}_{n,K}$ is the group of K-automorphisms of h_n:

$$\mathrm{U}_{n,K}(F) := \mathrm{Aut}_K(h_n) = \{u \in \mathrm{GL}_n(K) \mid \tau(u) = u^{-1}\}.$$

As in the orthogonal case, we may consider the group of similitudes

$$\mathrm{GU}_{n,K}(F) := \{g\in \mathrm{GL}_n(K) \mid \tau(g)g \in F^\times\}$$

and the corresponding projective group

$$\mathrm{PGU}_{n,K}(F) := \mathrm{Aut}_K(M_n(K),\tau) = \mathrm{GU}_{n,K}/K^\times.$$

Galois cohomology (see [29, Sect. 29.D]) yields a bijection:

$$\boxed{\begin{array}{l}K\text{-isomorphism classes of central}\\ \text{simple } K\text{-algebras of degree } n\\ \text{with unitary involution}\end{array}} \quad\longleftrightarrow\quad H^1(F,\mathrm{PGU}_{n,K}).$$

More precisely, the set on the left consists of the isomorphism classes of triples (B,τ,φ), where B is a central simple algebra of degree n over a quadratic extension Z of F, τ is an involution on B that restricts to the nontrivial F-automorphism of Z, and $\varphi\colon Z \xrightarrow{\sim} K$ is an F-algebra isomorphism.

4.1 The (Quasi)split Case

When B is split, the study of unitary involutions reduces to the quadratic form case by an observation due to Jacobson: every hermitian form $h\colon V\times V\to K$ on a K-vector space V yields a quadratic form $q_h\colon V\to F$ on V (viewed as an F-vector space) by

$$q_h(x) = h(x,x) \quad \text{for } x\in V.$$

The quadratic form uniquely determines h because it is easily verified that if $\alpha = \sqrt{a}\in K$ satisfies $\iota(\alpha) = -\alpha$, then

$$h(x,y) = \frac{1}{2}\big(q_h(x+y) - q_h(x) - q_h(y) + q_h(x+y\alpha)\alpha^{-1} - q_h(x)\alpha^{-1} - q_h(y\alpha)\alpha^{-1}\big).$$

Therefore, the invariants of h and q_h are the same and the invariants of ad_h are the invariants of the similarity class of q_h (which is always even dimensional since $\dim_F V = 2\dim_K V$). If $e_i(q_h)$ is defined for some i, we set

$$e_i(\mathrm{ad}_h) = e_i(q_h) \in H^i(F).$$

The correspondence between the involutions adjoint to h and to q_h is made explicit in the following lemma (which is a very special case of a result of Garibaldi and Quéguiner-Mathieu [19, Proposition 1.9]).

Lemma 4.1. *Let B be a split central simple algebra over $K = F(\sqrt{a})$ and let τ be a unitary involution on B. There is a split central simple F-algebra A of degree* $\deg A = 2\deg B$ *and an orthogonal involution σ on A such that (B,τ) embeds in (A,σ):*

$$(B,\tau) \hookrightarrow (A,\sigma).$$

For a given embedding $B \subset A$, the orthogonal involution σ is uniquely determined by the condition that $\sigma|_B = \tau$. For any integer i, the invariant $e_i(\tau)$ is defined if and only if $e_i(\sigma)$ is defined, and

$$e_i(\tau) = e_i(\sigma).$$

Proof. Let $B = \mathrm{End}_K V$ for some K-vector space V and $\tau = \mathrm{ad}_h$ for some hermitian form h on V. Define $A = \mathrm{End}_F V$, so there is a canonical embedding $B \hookrightarrow A$, and let $\sigma = \mathrm{ad}_{q_h}$, the orthogonal involution on A adjoint to the quadratic form q_h. It is readily verified that $\sigma|_B = \tau$. If σ' is another orthogonal involution on A such that $\sigma'|_B = \tau$, then $\sigma' = \mathrm{Int}(s) \circ \sigma$ for some $s \in A^\times$ such that $\sigma(s) = s$ and $sx = xs$ for all $x \in B$. Since s centralizes B, we must have $s \in K^\times$; the condition $\sigma(s) = s$ then amounts to $\iota(s) = s$, hence $s \in F^\times$ and therefore $\sigma' = \sigma$. By definition of $e_i(\tau)$, we have

$$e_i(\tau) = e_i(q_h) = e_i(\sigma).$$

$\square$

If $(v_1,\dots,v_n)$ is a K-base of V where the hermitian form h is diagonal,

$$h = \langle a_1,\dots,a_n\rangle_K,$$

then $a_1,\dots,a_n \in F^\times$ and $(v_1, v_1\alpha, \dots, v_n, v_n\alpha)$ is an orthogonal F-base of V where the quadratic form q_h is

$$q_h = \langle 1, -a\rangle \otimes \langle a_1,\dots,a_n\rangle.$$

Therefore,

$$e_1(\mathrm{ad}_h) = \begin{cases} (a) & \text{if } n \text{ is odd,} \\ 0 & \text{if } n \text{ is even,} \end{cases}$$

and, when n is even,

$$e_2(\mathrm{ad}_h) = (a, (-1)^{n/2}a_1,\dots,a_n)_F \in H^2(F).$$

The *discriminant* $\operatorname{disc} h$ is defined as the image of $(-1)^{n/2}a_1,\dots,a_n$ in the factor group $F^\times/N_{K/F}(K^\times)$; the preceding equation may thus be rewritten as

$$e_2(\mathrm{ad}_h)=(a,\operatorname{disc} h)_F.$$

To discuss decompositions into tensor products of quaternion algebras, it is useful to keep in mind the following theorem of Albert: if τ is a unitary involution on a quaternion algebra Q over $K=F(\sqrt{a})$, then there is a unique quaternion F-algebra Q' with conjugation involution γ such that

$$(Q,\tau)=(Q',\gamma)\otimes_F(K,\iota),$$

where ι is the nontrivial F-automorphism of K. (The quaternion algebra Q' is in fact the discriminant algebra $D(Q,\tau)$: see the proof of Theorem 4.5.) Therefore, every tensor product of quaternion K-algebras with unitary involution has an alternative decomposition:

$$(Q_1,\tau_1)\otimes_K\cdots\otimes_K(Q_n,\tau_n)=(Q_1',\gamma_1)\otimes_F\cdots\otimes_F(Q_n',\gamma_n)\otimes_F(K,\iota).$$

Theorem 4.2. *Let τ be a unitary involution on a* split *central simple algebra B of even degree over $K=F(\sqrt{a})$, and let d be an arbitrary integer, $d\geq 1$:*

(a) If $\deg B<2^d$, we have $e_i(\tau)=0$ for $i=2,\dots,d$ if and only if τ is hyperbolic.
(b) If $\deg B=2^d$, we have $e_i(\tau)=0$ for $i=2,\dots,d$ if and only if (B,τ) decomposes into a tensor product of quaternion algebras with unitary involutions:

$$(B,\tau)=(Q_1,\tau_1)\otimes_K\cdots\otimes_K(Q_d,\tau_d).$$

(c) If $\deg B=2^{d-1}$, unitary involutions on B with $e_i=0$ for $i=2,\dots,d-1$ are classified by their e_d-invariant.

Comparing with Theorem 3.1, note the shift in the degree of the algebra.

Proof. Let $\tau=\mathrm{ad}_h$, so $e_i(\tau)=e_i(q_h)$ when defined. Note that $\dim q_h=2\deg B$, so in case (a) q_h is hyperbolic if and only if $q_h\in I^{d+1}F$, and this condition is equivalent to $e_i(q_h)=0$ for $i=2,\dots,d$. If $\deg B=2^d$ and $e_i(\tau)=0$ for $i=2,\dots,d$, then q_h is a $(d+1)$-Pfister form of the type

$$q_h=\langle\langle a,a_1,\dots,a_d\rangle\rangle\quad\text{for some } a_1,\dots,a_d\in F^\times,$$

hence

$$h=\langle\langle a_1,\dots,a_d\rangle\rangle_K.$$

Therefore,

$$\begin{aligned}(B,\tau)&=(M_2(F),\mathrm{ad}_{\langle\langle a_1\rangle\rangle})\otimes_F\cdots\otimes_F(M_2(F),\mathrm{ad}_{\langle\langle a_d\rangle\rangle})\otimes_F(K,\iota)\\&=(M_2(K),\mathrm{ad}_{\langle\langle a_1\rangle\rangle_K})\otimes_K\cdots\otimes_K(M_2(K),\mathrm{ad}_{\langle\langle a_d\rangle\rangle_K}).\end{aligned}$$

Conversely, suppose there are quaternion F-algebras $Q_1',\dots,Q_d'$ with conjugation involutions $\gamma_1,\dots,\gamma_d$ such that

$$(B,\tau)=(Q_1',\gamma_1)\otimes_F\cdots\otimes_F(Q_d',\gamma_d)\otimes_F(K,\iota).$$

Since B is split, the product $Q'_1 \otimes_F \cdots \otimes_F Q'_d$ is split by K, so we may find $b \in F^\times$ such that

$$Q'_1 \otimes_F \cdots \otimes_F Q'_d = (a,b)_F \quad \text{in } \mathrm{Br}(F).$$

Embed $K \hookrightarrow (a,b)_F$ and pick an involution θ on $(a,b)_F$ that restricts to ι on K and that is orthogonal if d is even and symplectic if d is odd. (So, in the latter case θ is the conjugation involution.) We then have an embedding

$$(B,\tau) \hookrightarrow (A,\sigma) := (Q'_1,\gamma_1) \otimes_F \cdots \otimes_F (Q'_d,\gamma_d) \otimes_F \big((a,b)_F,\theta\big).$$

By Theorem 3.1 we have $e_i(\sigma) = 0$ for $i = 1,\dots,d$, hence $e_i(\tau) = 0$ for $i = 2,\dots,d$ by Lemma 4.1.

To prove (c), let $B = \mathrm{End}_K V$ with $\dim_K V = 2^{d-1}$ and consider unitary involutions $\tau = \mathrm{ad}_h$ and $\tau' = \mathrm{ad}_{h'}$ on B with $e_i = 0$ for $i = 2,\dots,d-1$. The corresponding quadratic forms q_h and $q_{h'}$ satisfy $e_i(q_h) = e_i(q_{h'}) = 0$ for $i = 1,\dots,d-1$; hence, Theorem 3.1 shows that q_h and $q_{h'}$ are similar if and only if $e_d(q_h) = e_d(q_{h'})$. Therefore, τ and τ' are isomorphic if and only if $e_d(\tau) = e_d(\tau')$. □

4.2 *The Discriminant Algebra*

Since the group $\mathrm{PGU}_{n,K}$ is connected, the procedure that yields the discriminant of orthogonal involutions in Sect. 3.3 does not apply here. The group $\mathrm{PGU}_{n,K}$ is not simply connected however, so we may obtain cohomological invariants of degree 2 as in the orthogonal case. The simply connected cover of $\mathrm{PGU}_{n,K}$ is the special unitary group:

$$\mathrm{SU}_{n,K} := \{u \in \mathrm{U}_{n,K} \mid \det(u) = 1\}.$$

Its center is a twisted version of the group of nth roots of unity:

$$\mu_{n,K} := \{z \in K^\times \mid N_{K/F}(z) = 1 = z^n\}.$$

Henceforth, we assume that the characteristic of F does not divide n, so that $\mu_{n,K}$ is a smooth algebraic group. Its group of rational points over F_s is isomorphic to the group of nth roots of unity in F_s, with a twisted Galois action that disappears after scalar extension to K. From the exact sequence

$$1 \to \mu_{n,K} \to \mathrm{SU}_{n,K} \to \mathrm{PGU}_{n,K} \to 1, \tag{4.3}$$

we obtain a connecting map in cohomology:

$$\partial\colon H^1(F,\mathrm{PGU}_{n,K}) \to H^2(F,\mu_{n,K}).$$

The features of this map are significantly different according to whether n is odd or even.

4.2.1 The Odd Degree Case

When n is odd, the scalar extension map

$$\mathrm{res}_{K/F}\colon H^2(F,\mu_{n,K}) \to H^2(K,\mu_n)$$

is injective, and identifies $H^2(F,\mu_{n,K})$ with the kernel of the corestriction map

$$\mathrm{cor}_{K/F}\colon H^2(K,\mu_n) \to H^2(F,\mu_n),$$

see [29, (30.12)]. Comparing the exact sequence (4.3) with the corresponding exact sequence after scalar extension to K, which is

$$1 \to \mu_n \to \mathrm{SL}_n \to \mathrm{PGL}_n \to 1,$$

it is easy to see that the cohomology class in $H^1(F,\mathrm{PGU}_{n,K})$ represented by an algebra with involution (B,τ) is mapped by ∂ to the Brauer class $[B] \in H^2(K,\mu_n)$.

4.2.2 The Even Degree Case

Let $n = 2m$. Besides the restriction map $\mathrm{res}_{K/F}$, we may also consider the map defined by raising to the mth power:

$$m\colon H^2(F,\mu_{n,K}) \to H^2(F,\mu_2).$$

The following description of $H^2(F,\mu_{n,K})$ is due to Colliot-Thélène–Gille–Parimala [10, Proposition 2.10].

Proposition 4.4. *The map* $(\mathrm{res}_{K/F}, m)\colon H^2(F,\mu_{n,K}) \to H^2(K,\mu_n) \times H^2(F,\mu_2)$ *is injective. Its image is the group of pairs* (ξ,η) *such that* $\xi^m = \mathrm{res}_{K/F}(\eta)$ *and* $\mathrm{cor}_{K/F}(\xi) = 0$.

Let (B,τ) be a central simple K-algebra of degree n with unitary involution, and let $\Delta(B,\tau) \in H^2(F,\mu_{n,K})$ be the image under ∂ of the corresponding cohomology class in $H^1(F,\mathrm{PGU}_{n,K})$. As in the case where n is odd, we have

$$\mathrm{res}_{K/F}\,\Delta(B,\tau) = [B],$$

which is an obvious invariant that gives no information on the involution τ. The other component of $\Delta(B,\tau)$ under the map of Proposition 4.4 is more interesting; let

$$e_2(\tau) = \Delta(B,\tau)^m \in H^2(F).$$

This cohomology class turns out to be the Brauer class of a central simple F-algebra $D(B,\tau)$ of degree $\binom{n}{m}$ first considered by Tits [53, Sect. 6.3] and by Tamagawa [51]. When $B = \mathrm{End}_K V$ and $\tau = \mathrm{ad}_h$ for some hermitian form h, the algebra $D(B,\tau)$ is Brauer equivalent to the quaternion algebra $(a, \mathrm{disc}\, h)_F$. Therefore, $D(B,\tau)$ is called the *discriminant algebra* of (B,τ) in [29, Sect. 10], and the e_2-invariant defined earlier coincides with the e_2-invariant of unitary involutions on split algebras defined in Sect. 4.1.

Theorem 4.5. *Let τ be a unitary involution on a central simple K-algebra B of even degree:*

(a) If $\deg B = 2$, then τ is hyperbolic if and only if $e_2(\tau) = 0$.
(b) If $\deg B = 4$, then $e_2(\tau) = 0$ if and only if there is a decomposition

$$(B,\tau) = (B_1,\tau_1) \otimes_K (B_2,\tau_2)$$

for some subalgebras B_1, $B_2 \subset B$ of degree 2.
(c) If $\deg B = 2$, unitary involutions on B are classified by their e_2-invariant.

Proof. If $\deg B = 2$, then $D(B,\tau)$ is the quaternion F-algebra such that

$$(B,\tau) = (D(B,\tau),\gamma) \otimes_F (K,\iota),$$

where γ is the conjugation involution (see [29, p. 129]). Therefore, τ is hyperbolic if $D(B,\tau)$ is split, and $D(B,\tau)$ determines τ uniquely. Part (b) is due to Karpenko–Quéguiner [26]. It is based on the coincidence of Dynkin diagrams $A_3 = D_3$, which can be used to show that every central simple algebra of degree 4 with unitary involution is isomorphic to the Clifford algebra of a canonical orthogonal involution on its discriminant algebra (see [29, Sect. 15.D]). □

4.3 Higher Invariants

The same method as in Sect. 3.5 allows one to derive from Rost's invariant for $\mathrm{SU}_{n,K}$ a relative invariant of unitary involutions on a given central simple algebra B over $K = F(\sqrt{a})$. Suppose $\deg B = n$ is even and not divisible by the characteristic, and let τ_0 be a unitary involution on B with $e_2(\tau_0) = 0$. By Proposition 4.4, the cohomology class in $H^1\big(F,\mathrm{PGU}(B,\tau_0)\big)$ corresponding to a unitary involution τ on B with $e_2(\tau) = 0$ lifts to some $\xi \in H^1\big(F,\mathrm{SU}(B,\tau_0)\big)$. The Rost invariant $R(\xi)$ lies in $H^3(F,\mu_d^{\otimes 2})$, where d is the Dynkin index of $\mathrm{SU}(B,\tau_0)$, determined in [17, (12.6), p. 142]:

$$d = \begin{cases} \exp B & \text{if } n \text{ is a 2-power and } \exp B = n \text{ or } n/2,\\ 2\exp B & \text{otherwise.}\end{cases}$$

In view of the description of the Rost invariant on the center of $\mathrm{SU}(B,\tau_0)$ given by Merkurjev–Parimala–Tignol [40], one should be able to define

$$e_3(\tau/\tau_0) = R(\xi) + B_B^3 \in H^3(F,\mu_d^{\otimes 2})/B_B^3,$$

where

$$B_B^3 = \mathrm{cor}_{K/F}\bigl([B]\cdot H^1(K,\mu_d)\bigr).$$

As far as I know, this invariant has not been investigated yet.

Although the case where the degree n is odd does not pertain to the line of investigation developed so far in this text, it is worth mentioning that a similar construction based on the Rost invariant is better documented in this case: consider the F-vector space $\mathrm{Sym}(\tau)$ of τ-symmetric elements in B and the quadratic form

$$Q_\tau\colon \mathrm{Sym}(\tau) \to F, \quad x \mapsto \mathrm{Trd}_B(x^2).$$

Assuming $\deg B = n$ is odd (and not divisible by the characteristic), it is shown in [29, (31.45)] that the Rost invariant of $\mathrm{SU}(B,\tau_0)$ yields a relative invariant of unitary involutions on B defined by

$$f_3(\tau/\tau_0) = e_3(Q_\tau - Q_{\tau_0}) \in H^3(F).$$

By a result of Garibaldi–Gille [16, Proposition 7.2], we may in fact define an *absolute* invariant by

$$f_3(\tau) = e_3\left(Q_\tau - \langle 1\rangle - \frac{n-1}{2}\langle 2,2a\rangle\right) \in H^3(F),$$

so that $f_3(\tau/\tau_0) = f_3(\tau) - f_3(\tau_0)$. (The form $\langle 1\rangle + \frac{n-1}{2}\langle 2,2a\rangle$ is Witt equivalent to the form Q_τ for τ the adjoint involution of the n-dimensional hermitian form of maximal Witt index.) The absolute invariant f_3 was first investigated in the particular case where $\deg B = 3$ by Haile–Knus–Rost–Tignol [20]. It classifies the unitary involutions on a given central simple algebra of degree 3 up to isomorphism (see [29, Sect. 19.B and (30.21)]).

There is also an absolute invariant of degree 4 defined just for $\deg B = 4$ and $K = F(\sqrt{-1})$ by Rost–Serre–Tignol [46]: letting n_D denote the norm form of the quaternion F-algebra Brauer equivalent to the discriminant algebra $D(B,\tau)$, the invariant is

$$f_4(\tau) = e_4(Q_\tau - n_D) \in H^4(F).$$

It vanishes if and only if B is generated by two elements $x, y \in \mathrm{Sym}(\tau)$ such that x^4, $y^4 \in F^\times$ and $yx = ixy$, where $i = \sqrt{-1} \in K$. If B is split and $\tau = \mathrm{ad}_h$ with

$$h = \langle a_1,a_2,a_3,a_4\rangle_K,$$

we have

$$f_4(\tau) = (-1)\cdot(-a_1a_2)\cdot(-a_1a_3)\cdot(-a_1a_4).$$

Note that the fourfold Pfister form $\langle\langle -1,-a_1a_2,-a_1a_3,-a_1a_4\rangle\rangle$ is indeed an invariant of the hermitian form h: in the notation of Garibaldi et al. [17, p. 67], we have

$$\langle\langle -1,-a_1a_2,-a_1a_3,-a_1a_4\rangle\rangle = 2 + \lambda_2^2(h) + \lambda_2^4(h).$$

5 Symplectic Involutions

Let n be an even integer, $n = 2m$, and let s_n be the following skew-symmetric matrix of order n:

$$s_n = \mathrm{diag}\big(\underbrace{\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)}_{m}\big).$$

Define a symplectic involution $\sigma\colon M_n(F) \to M_n(F)$ by

$$\sigma(m) = s_n^{-1} \cdot m \cdot s_n \quad \text{for } m \in M_n(F).$$

The symplectic group is the automorphism group of the bilinear form with Gram matrix s_n:

$$\mathrm{Sp}_n(F) := \{u \in \mathrm{GL}_n(F) \mid u^{\mathrm{t}} s_n u = s_n\} = \{u \in \mathrm{GL}_n(F) \mid \sigma(u) = u^{-1}\}.$$

As in the orthogonal and symplectic cases, the group of similitudes is defined by

$$\mathrm{GSp}_n(F) := \{g \in \mathrm{GL}_n(F) \mid \sigma(g)g \in F^\times\};$$

its projective version is

$$\mathrm{PGSp}_n(F) := \mathrm{Aut}(M_n(F), \sigma) = \mathrm{GSp}_n(F)/F^\times.$$

Galois cohomology (see [29, (29.22)]) yields a bijection:

$$\boxed{\begin{array}{l}\text{isomorphism classes of central}\\ \text{simple } F\text{-algebras of degree } n\\ \text{with symplectic involution}\end{array}} \quad \longleftrightarrow \quad H^1(F, \mathrm{PGSp}_n).$$

As pointed out in Sect. 2, symplectic involutions on split central simple algebras are adjoint to nonsingular skew-symmetric bilinear forms. Since every such form is hyperbolic, all the symplectic involutions on a split central simple algebra are hyperbolic (and conjugate). The classification problem thus arises only when the index is at least 2.

5.1 The Case of Index 2

Let A be a central simple F-algebra of degree n and index 2, that is, A is Brauer equivalent to a quaternion F-algebra Q. As in Sect. 3.2, we may represent A as

$$A = \mathrm{End}_Q V$$

for some right Q-vector space V with $\dim_Q V = n/2$. Every symplectic involution on A is adjoint to some hermitian form h on V with respect to the conjugation involution

γ on Q. As in Sect. 4.1, a result of Jacobson yields a reduction to quadratic forms since the map

$$q_h \colon V \to F, \quad x \mapsto h(x,x)$$

is a quadratic form on V viewed as an F-vector space, which determines h uniquely (see [48, Theorem 10.1.7, p. 352]). The invariants of ad_h are the invariants of the similarity class of h, which are also the invariants of the similarity class of q_h. If $e_i(q_h)$ is defined for some i, let

$$e_i(\mathrm{ad}_h) = e_i(q_h) \in H^i(F).$$

The correspondence between the symplectic involution ad_h and the orthogonal involution adjoint to q_h was used by MacDonald [36, Theorem 4.7] to determine all the invariants of symplectic involutions on central simple algebras A with $\mathrm{ind} A = 2$ and $\deg A \equiv 2 \bmod 4$. This correspondence can also be described directly, as the next lemma shows.

Lemma 5.1. *Let A be a central simple F-algebra Brauer equivalent to a quaternion F-algebra Q. Let σ be a symplectic involution on A and let γ be the conjugation involution on Q. Then $\sigma \otimes \gamma$ is an orthogonal involution on the split algebra $A \otimes_F Q$. If $(A,\sigma) = (\mathrm{End}_Q V, \mathrm{ad}_h)$ for some hermitian form h, then there is a canonical isomorphism*

$$(A \otimes_F Q, \sigma \otimes \gamma) \simeq (\mathrm{End}_F V, \mathrm{ad}_{q_h})$$

which carries $x \otimes y \in A \otimes_F Q$ to the map $v \mapsto x(v)\gamma(y)$. Therefore, for any integer $i \geq 1$, the invariant $e_i(\sigma)$ is defined if and only if $e_i(\sigma \otimes \gamma)$ is defined, and then

$$e_i(\sigma) = e_i(\sigma \otimes \gamma).$$

Proof. The lemma follows by a straightforward verification. □

Let $m = n/2$ and let $(v_\alpha)_{\alpha=1}^m$ be an orthogonal Q-base of V with respect to h, in which h has the diagonalization

$$h = \langle \lambda_1, \dots, \lambda_m \rangle_Q.$$

We have $\lambda_\alpha \in F^\times$ for all α. If $(1,i,j,k)$ is a quaternion F-base of Q with $i^2 = a$ and $j^2 = b$, then $(v_\alpha, v_\alpha i, v_\alpha j, v_\alpha k)_{\alpha=1}^m$ is an F-base of V in which q_h has the diagonal form

$$q_h = \langle\langle a,b \rangle\rangle \otimes \langle \lambda_1, \dots, \lambda_m \rangle.$$

Therefore,

$$e_1(\mathrm{ad}_h) = 0, \quad e_2(\mathrm{ad}_h) = \begin{cases} [Q] & \text{if } m \text{ is odd,} \\ 0 & \text{if } m \text{ is even,} \end{cases} \tag{5.2}$$

and, if m is even,

$$e_3(\mathrm{ad}_h) = [Q] \cdot \big((-1)^{m/2}\lambda_1, \dots, \lambda_m\big) \in H^3(F).$$

Note that the involution ad_h always decomposes: if $V_0 \subset V$ denotes the F-span of $(v_\alpha)_{\alpha=1}^m$, then $V = V_0 \otimes_F Q$ and

$$(\mathrm{End}_Q V, \mathrm{ad}_h) = (\mathrm{End}_F V_0, \mathrm{ad}_{\langle\lambda_1,\dots,\lambda_m\rangle}) \otimes_F (Q,\gamma).$$

Theorem 5.3. *Let σ be a symplectic involution on a central simple algebra of index 2, and let d be an arbitrary integer, $d \geq 2$:*

(a) If $\deg A < 2^d$, we have $e_i(\sigma) = 0$ for all $i = 2,\dots,d$ if and only if σ is hyperbolic.
(b) If $\deg A = 2^d$, we have $e_i(\sigma) = 0$ for all $i = 2,\dots,d$ if and only if (A,σ) decomposes into a tensor product of quaternion algebras with involution:

$$(A,\sigma) = (Q_1,\sigma_1) \otimes_F \cdots \otimes_F (Q_d,\sigma_d). \tag{5.4}$$

(c) If $\deg A = 2^{d-1}$, symplectic involutions on A with $e_i = 0$ for $i = 2,\dots,d-1$ are classified by their e_d-invariant.

Proof. Using the same notation as in Lemma 5.1, part (a) readily follows from Theorem 3.1 since $e_i(\sigma) = e_i(\sigma\otimes\gamma)$ and σ is hyperbolic if and only if $\sigma\otimes\gamma$ is hyperbolic.

If $\deg A = 2^d$ and $e_i(\sigma) = 0$ for $i = 2,\dots,d$, then q_h is a $(d+1)$-Pfister form

$$q_h = \langle\langle a,b,\lambda_1,\dots,\lambda_{d-1}\rangle\rangle \quad \text{for some } \lambda_1,\dots,\lambda_{d-1} \in F^\times,$$

and we have a decomposition

$$(A,\sigma) \simeq (M_2(F), \mathrm{ad}_{\langle\langle\lambda_1\rangle\rangle}) \otimes_F \cdots \otimes_F (M_2(F), \mathrm{ad}_{\langle\langle\lambda_{d-1}\rangle\rangle}) \otimes_F (Q,\gamma).$$

Conversely, if we have a decomposition (5.4), then

$$(A\otimes_F Q, \sigma\otimes\gamma) \simeq (Q_1,\sigma_1) \otimes_F \cdots \otimes_F (Q_{d-1},\sigma_{d-1}) \otimes_F (Q,\gamma).$$

By Theorem 3.1, we have $e_i(\sigma\otimes\gamma) = 0$ for $i = 2,\dots,d$, hence $e_i(\sigma) = 0$ for $i = 2,\dots,d$ by Lemma 5.1.

Similarly, part (c) reduces to the split orthogonal case by Lemma 5.1. □

5.2 *Invariant of Degree 2*

The group PGSp_n is connected, so there is no analogue of the discriminant of orthogonal involutions as defined in Sect. 3.3. The simply connected cover of PGSp_n is the symplectic group, whose center is μ_2. The exact sequence

$$1 \to \mu_2 \to \mathrm{Sp}_n \to \mathrm{PGSp}_n \to 1 \tag{5.5}$$

yields a connecting map in cohomology:

$$\partial\colon H^1(F, \mathrm{PGSp}_n) \to H^2(F).$$

The cohomology class corresponding to an algebra with involution (A, σ) is mapped by ∂ to the Brauer class $[A]$, which does not yield any information on σ. Yet, we have a result analogous to Theorems 3.6 and 4.5.

Theorem 5.6. *Let σ be a symplectic involution on a central simple F-algebra A of even degree:*

(a) If $\deg A = 2$*, then σ is unique. It is hyperbolic if and only if A is split.*
(b) If $\deg A = 4$*, there is a decomposition*

$$(A, \sigma) = (Q_1, \sigma_1) \otimes_F (Q_2, \sigma_2)$$

for some quaternion subalgebras Q_1, $Q_2 \subset A$.

Part (a) is clear. Part (b) was first observed by Rowen [47, Theorem B]. For a proof based on the coincidence of Dynkin diagrams $B_2 = C_2$, see [54, p. 131] or [29, (16.16)].

5.3 The Discriminant

Quéguiner-Mathieu's construction of Sect. 3.5 has an analogue for symplectic involutions, showing that there is no absolute invariant of degree 3 for symplectic involutions on central division algebras of degree 4. Start with an arbitrary division algebra A of degree 4 with symplectic involution σ over a field F, and suppose there is a functorial invariant $e_3(\sigma) \in H^3(F)$. Let

$$e_3(\sigma) = \sum_i (a_i) \cdot (b_i) \cdot (c_i) \quad \text{for some } a_i,\, b_i,\, c_i \in F^\times.$$

Let K be the function field of the product of the quadrics:

$$x_0^2 - a_i x_1^2 - b_i x_2^2 + a_i b_i x_3^2 - c_i x_4^2 = 0.$$

We have $e_3(\sigma)_K = 0$, hence $e_3(\sigma_K) = 0$, but A_K is a division algebra by a theorem of Merkurjev [13, Corollary 30.10]. It is a tensor product of quaternion algebras by Theorem 5.6; let Q_1, Q_2 be quaternion K-algebras such that $A_K \simeq Q_1 \otimes_K Q_2$. The difference of the norm forms $n_{Q_1} - n_{Q_2}$ is Witt equivalent to a six-dimensional quadratic form φ known as an *Albert form* of A_K. Let L be the function field of the projective quadric $\varphi = 0$. Over L, the quaternion algebras Q_1, Q_2 have isomorphic maximal subfields, hence A_L is not division. It is not split either, since the function field of a quadric does not split any algebra of index 4, hence $\operatorname{ind} A_L = 2$. Since $e_3(\sigma_L) = 0$, Theorem 5.3(a) shows that σ_L is hyperbolic. In view of the coincidence of Dynkin diagrams $B_2 = C_2$, this property translates into a condition on a five-dimensional quadratic F-form q such that[4] $A \simeq C_0(q)$ under an isomorphism that carries σ to the canonical involution of $C_0(q)$: the form q_L is isotropic (see [29, (15.21)]). However, q_K is anisotropic and is not a Pfister neighbor since A_K is a division algebra (see [29, p. 270, Exercise 8]). We obtain a contradiction because Hoffmann [21] has shown that such a form cannot become isotropic by scalar extension to the function field of a six-dimensional quadratic form.

On the other hand, as in the orthogonal case (see Sect. 3.5), the Rost invariant of Sp_n can be used to define a relative invariant of symplectic involutions on central simple algebras of degree $n \equiv 0 \bmod 4$. In the symplectic case, this relative invariant has an easy description.

Let σ_0 be a fixed symplectic involution on a central simple F-algebra A of even degree $n = 2m$. If m is odd, the index of A is 1 or 2. As pointed out at the beginning of this section, the split case is uninteresting since every symplectic involution is hyperbolic. If $\operatorname{ind} A = 2$, then (5.2) yields $e_2(\sigma_0) = [A] \neq 0$, hence there is no e_i-invariant for $i \geq 3$. Therefore, *throughout this section we assume that m is even*. On the vector space $\mathrm{Sym}(\sigma_0)$ of symmetric elements, the reduced norm has a square root given by a polynomial map Nrp analogous to the Pfaffian of skew-symmetric matrices under the transpose involution. The map

$$\mathrm{Nrp}\colon\ \mathrm{Sym}(A,\sigma_0) \to F$$

is a form of degree m such that $\mathrm{Nrp}(1) = 1$, $\mathrm{Nrd}(s) = \mathrm{Nrp}(s)^2$ and

$$\mathrm{Nrp}\big(as\sigma_0(a)\big) = \mathrm{Nrp}(s)\,\mathrm{Nrd}(a) \quad \text{for } s \in \mathrm{Sym}(\sigma_0) \text{ and } a \in A.$$

Every symplectic involution σ on A has the form $\sigma = \mathrm{Int}(s) \circ \sigma_0$ for some unit $s \in \mathrm{Sym}(\sigma_0)$ uniquely determined up to a scalar factor. Since $\mathrm{Nrp}(\lambda s) = \lambda^m \,\mathrm{Nrp}(s)$ for $\lambda \in F$, and since m is even, the square class $\big(\mathrm{Nrp}(s)\big) \in H^1(F)$ is uniquely determined by σ. We may thus set

$$e_3(\sigma/\sigma_0) = \big(\mathrm{Nrp}(s)\big) \cdot [A] \in H^3(F).$$

If σ' is a symplectic involution on A such that (A,σ) and (A,σ') are isomorphic, then σ and σ' are conjugate so there exists $a \in A^\times$ such that

$$\sigma' = \mathrm{Int}(a) \circ \sigma \circ \mathrm{Int}(a)^{-1} = \mathrm{Int}\big(as\sigma_0(a)\big) \circ \sigma_0.$$

Since $\mathrm{Nrp}\big(as\sigma_0(a)\big) = \mathrm{Nrp}(s)\,\mathrm{Nrd}(a)$ and $\big(\mathrm{Nrd}(a)\big) \cdot [A] = 0$, we have

$$\big(\mathrm{Nrp}(as\sigma_0(a))\big) \cdot [A] = \big(\mathrm{Nrp}(s)\big) \cdot [A],$$

[4] This condition determines q uniquely up to a scalar factor (see [29, Sect. 15.C]).

hence

$$e_3(\sigma'/\sigma_0) = e_3(\sigma/\sigma_0).$$

Therefore, $e_3(\sigma/\sigma_0)$ depends only on the isomorphism class of σ: it is an invariant of symplectic involutions on A.

Alternatively, as pointed out by Garibaldi, the invariant $e_3(\sigma/\sigma_0)$ may be obtained by mimicking the argument in Sect. 3.5, using the following twisted version of (5.5):

$$1 \to \mu_2 \to \mathrm{Sp}(A,\sigma_0) \to \mathrm{PGSp}(A,\sigma_0) \to 1.$$

The involution σ defines a cohomology class $\xi \in H^1\big(F, \mathrm{PGSp}(A,\sigma_0)\big)$ that can be lifted to $H^1\big(F, \mathrm{Sp}(A,\sigma_0)\big)$. The Rost invariant of the lift is the invariant $e_3(\sigma/\sigma_0)$. Note that in this case the Rost invariant does not depend on the choice of the lift of ξ since it vanishes on cocycles that come from the center of $\mathrm{Sp}(A,\sigma_0)$ (see [40]). Therefore, we do not have to factor out $H^3(F)$ by a subgroup depending on A to obtain a well-defined relative invariant.

Theorem 5.7. *If* $\deg A = 4$*, then the symplectic involutions* σ *and* σ_0 *are conjugate if and only if* $e_3(\sigma/\sigma_0) = 0$.

This theorem was proved by Knus–Lam–Shapiro–Tignol [28] with a slightly different definition of the invariant (see also [29, Sect. 16.B]). It also follows from the exceptional isomorphism $B_2 = C_2$ together with Garibaldi [14, Lemma 1.2].

If the Schur index $\operatorname{ind} A$ divides $(1/2)\deg A$, then A carries hyperbolic involutions. Taking for σ_0 a hyperbolic involution, we may consider $e_3(\sigma/\sigma_0)$ as an absolute invariant. It coincides with the e_3-invariant of Sect. 5.1 when $\operatorname{ind} A = 2$, as was shown by Berhuy–Monsurrò–Tignol [7, Example 2].

If $\deg A \equiv 0 \bmod 8$, the invariant e_3 can be turned into an absolute invariant by reduction to the case where $\operatorname{ind} A$ divides $(1/2)\deg A$, as was shown by Garibaldi–Parimala–Tignol [18].

Theorem 5.8. *If* $n \equiv 0 \bmod 8$*, there is a unique invariant* e_3 *of central simple algebras of degree* n *with symplectic involution with values in* H^3 *such that for any extension* K *of* F *and any symplectic involutions* σ, σ_0 *on a central simple* K*-algebra* A *of degree* n*:*

(i) $e_3(\sigma) = 0$ *if* σ *is hyperbolic.*
(ii) $e_3(\sigma/\sigma_0) = e_3(\sigma) - e_3(\sigma_0)$.

Proof. Let A be a central simple F-algebra of degree 8. If A is not division, then it carries a hyperbolic involution σ_0. On the set of isomorphism classes of symplectic involutions on A, the unique map e_3 satisfying the conditions of the theorem is given by

$$e_3(\sigma) = e_3(\sigma/\sigma_0).$$

Now, suppose A is division and decomposes into a tensor product of quaternion subalgebras:

$$A = Q_1 \otimes_F Q_2 \otimes_F Q_3.$$

Then $Q_1 \otimes Q_2$ is division, and remains division over the generic splitting field F_{Q_3} of Q_3. Let X be the projective quadric defined by the vanishing of an Albert form of $Q_1 \otimes Q_2$. Over the function field $F(X)$, the product $Q_1 \otimes Q_2$ is not division, hence we may find $e_3(\sigma_{F(X)}) \in H^3(F(X))$. Similarly, since Q_3 splits over F_{Q_3}, we may find $e_3(\sigma_{F_{Q_3}}) \in H^3(F_{Q_3})$. One may check that $e_3(\sigma_{F(X)})$ is unramified over F, that is, it is in the kernel of all the residue maps corresponding to points of codimension 1 on X. Arason [1, (5.6)] proved that the scalar extension map $H^3(F) \to H^3_{\mathrm{nr}}(F(X))$ is injective, and Kahn [25] showed that its cokernel is $\mathbb{Z}/2\mathbb{Z}$, the nontrivial element being represented by the relative invariant $e_3(\rho_{F(X)}/\rho_0)$, where ρ is any symplectic involution on $Q_1 \otimes Q_2$ and ρ_0 is a hyperbolic symplectic involution on $(Q_1 \otimes Q_2)_{F(X)}$. Since $Q_1 \otimes Q_2$ remains division after scalar extension to F_{Q_3}, the form φ is anisotropic over F_{Q_3}, and we have a commutative diagram where the vertical maps are given by scalar extension:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^3(F) & \longrightarrow & H^3_{\mathrm{nr}}(F(X)) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
 & & H^3(F_{Q_3}) & \longrightarrow & H^3_{\mathrm{nr}}(F_{Q_3}(X)) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0.
\end{array}$$

By uniqueness of e_3 over $F_{Q_3}(X)$, we must have

$$e_3\left(\sigma_{F_{Q_3}}\right)_{F_{Q_3}(X)} = e_3(\sigma_{F(X)})_{F_{Q_3}(X)} = e_3\left(\sigma_{F_{Q_3}(X)}\right),$$

hence a diagram chase shows that $e_3(\sigma_{F(X)})$ is the image of a unique element $e_3(\sigma) \in H^3(F)$. Thus, e_3 is well defined and unique on the set of isomorphism classes of symplectic involutions on tensor products of three quaternion algebras. The proof in the general case relies on the same arguments, using induction on the minimal number of terms in a decomposition of $[A]$ into a sum of Brauer classes of quaternion algebras. See [18, Sect. 2]. □

The e_3-invariant of symplectic involutions has the same property regarding tensor decompositions as the invariants e_1 and e_2 of orthogonal involutions (see Theorems 3.6(b) and 3.10(b)) and the invariant e_2 of unitary involutions (Theorem 4.5(b)), as was shown in Garibaldi et al. [18].

Theorem 5.9. *Let σ be a symplectic involution on a central simple F-algebra of degree* 8. *There is a decomposition*

$$(A,\sigma) = (Q_1,\sigma_1) \otimes_F (Q_2,\sigma_2) \otimes_F (Q_3,\sigma_3)$$

for some quaternion subalgebras Q_1, Q_2, $Q_3 \subset A$ if and only if $e_3(A,\sigma) = 0$.

Appendix: Trace Form Invariants

Besides those that are explicitly defined in terms of the trace form (at the end of Sect. 4.3), several invariants defined earlier[5] have an alternative description in terms of the trace form. Throughout this appendix, we use the following notation: for σ an involution of arbitrary type on a central simple algebra A, we let Q_σ denote the quadratic form

$$Q_\sigma\colon \operatorname{Sym}(\sigma) \to F, \quad x \mapsto \operatorname{Trd}_A(x^2),$$

where F is the subfield fixed under σ in the center of A.

Suppose first σ is orthogonal and $\deg A = n = 2m$. Lewis [33, Theorem 1] and Quéguiner [44, Sect. 2.2] computed

$$\det Q_\sigma = 2^m \det \sigma.$$

(See also [29, (11.5)].) The Witt–Clifford invariant of Q_σ was computed by Quéguiner [44, Sect. 2.3]; it turns out to depend only on the discriminant of σ, the Brauer class of A, and the residue of m modulo 8. Therefore, if σ and σ_0 are two orthogonal involutions with the same discriminant on A, then $Q_\sigma - Q_{\sigma_0} \in I^3F$. The e_3-invariant of that form was computed in a particular case in [9, Lemma 4]. Note that $e_3(Q_\sigma - Q_{\sigma_0})$ lies in $H^3(F)$ whereas $e_3(\sigma/\sigma_0)$ lies in $H^3(F, \mu_4^{\otimes 2})/B_A^3$.

Suppose next τ is a unitary involution on a central simple algebra B of degree n over a field $K = F(\sqrt{a})$. Then by Quéguiner [44, Lemma 13] (see also [29, (11.16)])

$$\det Q_\tau = (-a)^{n(n-1)/2} \cdot F^{\times 2} \in F^\times / F^{\times 2}.$$

If $n = 2m$, the Witt–Clifford invariant $e_2(Q_\tau)$ is related to the Brauer class $e_2(\tau)$ of the discriminant algebra $D(B, \tau)$ as follows:

$$e_2(Q_\tau) = e_2(\tau) + (-a) \cdot (2^m (-1)^{m(m-1)/2}),$$

see [44, Sect. 3.4] or [29, (11.17)].

Finally, assume σ is a symplectic involution on a central simple F-algebra A of degree $n = 2m$. Then by Lewis [33, Theorem 1] or Quéguiner [44, Sect. 2.2] $\det Q_\sigma = 1$, and by Quéguiner [44, Sect. 2.3]

$$e_2(Q_\sigma) = \begin{cases} 0 & \text{if } m \equiv 0,\, 1 \bmod 8, \\ [A] & \text{if } m \equiv 2,\, 7 \bmod 8, \\ [A] + (-1) \cdot (-1) & \text{if } m \equiv 3,\, 6 \bmod 8, \\ (-1) \cdot (-1) & \text{if } m \equiv 4,\, 5 \bmod 8. \end{cases}$$

[5] Essentially the first nontrivial invariant in each of the orthogonal, unitary, and symplectic case.

If σ, σ_0 are symplectic involutions on A, then by Berhuy et al. [7, Theorem 4] we have

$$e_3(Q_\sigma - Q_{\sigma_0}) = \begin{cases} e_3(\sigma/\sigma_0) & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd.} \end{cases}$$

In a different direction, note that the trace form is also used to define the *signature* of an involution (see [34], [43], or [29, Sect. 11]).

Acknowledgements The text was substantially improved as a result of comments by Karim Becher during the conference and by Skip Garibaldi on a preliminary version, for which I am very grateful. Partial support from the F.R.S.–FNRS (Belgium) is gratefully acknowledged.

References

1. Arason, J.K.: Cohomologische Invarianten quadratischer Formen. J. Algebra **36**(3), 448–491 (1975)
2. Bayer-Fluckiger, E., Parimala, R.: Galois cohomology of the classical groups over fields of cohomological dimension ≤ 2. Invent. Math. **122**(2), 195–229 (1995)
3. ———: Classical groups and the Hasse principle. Ann. Math. **147**(3), 651–693 (1998)
4. Bayer-Fluckiger, E., Parimala, R., Quéguiner-Mathieu, A.: Pfister involutions. Proc. Indian Acad. Sci. Math. Sci. **113**(4), 365–377 (2003)
5. Becher, K.J.: A proof of the Pfister factor conjecture. Invent. Math. **173**(1), 1–6 (2008)
6. Berhuy, G.: Cohomological invariants of quaternionic skew-Hermitian forms. Arch. Math. (Basel) **88**(5), 434–447 (2007)
7. Berhuy, G., Frings, C., Tignol, J.P.: The discriminant of a symplectic involution. Pacific J. Math. **209**(2), 201–218 (2003)
8. ———: Galois cohomology of the classical groups over imperfect fields. J. Pure Appl. Algebra **211**(2), 307–341 (2007)
9. Berhuy, G., Monsurrò, M., Tignol, J.P.: Cohomological invariants and *R*-triviality of adjoint classical groups. Math. Z. **248**(2), 313–323 (2004)
10. Colliot-Thélène, J.-L., Gille, P., Parimala, R.: Arithmetic of linear algebraic groups over 2-dimensional geometric fields. Duke Math. J. **121**(2), 285–341 (2004)
11. Dejaiffe, I.: Somme orthogonale d'algèbres à involution et algèbre de Clifford. Commun. Algebra **26**(5), 1589–1612 (1998)
12. ———: Formes antihermitiennes devenant hyperboliques sur un corps de déploiement. C.R. Acad. Sci. Paris Sér. I Math. **332**(2), 105–108 (2001)
13. Elman, R., Karpenko, N., Merkurjev, A.: The algebraic and geometric theory of quadratic forms. *American Mathematical Society Colloquium Publications*, vol. 56. American Mathematical Society, Providence, RI (2008)
14. Garibaldi, S.: The Rost invariant has trivial kernel for quasi-split groups of low rank. Comment. Math. Helv. **76**, 684–711 (2001)
15. ———: Orthogonal involutions on algebras of degree 16 and the Killing form of E_8 (with an appendix by Kirill Xainoulline). In: Quadratic Forms – Algebra, Arithmetic, and Geometry. *Contemporary Mathematics*, vol. 493, pp. 131–162. American Mathematical Society, Providence, RI (2009)
16. Garibaldi, S., Gille, P.: Algebraic groups with few subgroups. J. Lond. Math. Soc. **80**, 405–430 (2009)
17. Garibaldi, S., Merkurjev, A., Serre, J.P.: Cohomological invariants in Galois cohomology. *University Lecture Series*, vol. 28. American Mathematical Society, Providence, RI (2003)

18. Garibaldi, S., Parimala, R., Tignol, J.P.: Discriminant of symplectic involutions. Pure Appl. Math. Q. **5**(1), 349–374 (2009)
19. Garibaldi, S., Quéguiner-Mathieu, A.: Pfister's theorem for orthogonal involutions of degree 12. Proc. Am. Math. Soc. **137**(4), 1215–1222 (2009)
20. Haile, D.E., Knus, M.A., Rost, M., Tignol, J.P.: Algebras of odd degree with involution, trace forms and dihedral extensions. Israel J. Math. B **96**, 299–340 (1996)
21. Hoffmann, D.W.: Isotropy of 5-dimensional quadratic forms over the function field of a quadric. In: K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992). *Proceedings of the Symposium on Pure Mathematics*, vol. 58, pp. 217–225. American Mathematical Society, Providence, RI (1995)
22. ———: Similarity of quadratic forms and half-neighbors. J. Algebra **204**(1), 255–280 (1998)
23. Jacobson, N.: Clifford algebras for algebras with involution of type D. J. Algebra **1**, 288–300 (1964)
24. ———: Some applications of Jordan norms to involutorial simple associative algebras. Adv. Math. **48**(2), 149–165 (1983)
25. Kahn, B.: Lower $\mathscr{H}$-cohomology of higher-dimensional quadrics. Arch. Math. (Basel) **65**(3), 244–250 (1995)
26. Karpenko, N., Quéguiner, A.: A criterion of decomposability for degree 4 algebras with unitary involution. J. Pure Appl. Algebra **147**(3), 303–309 (2000)
27. Karpenko, N.A.: On anisotropy of orthogonal involutions. J. Ramanujan Math. Soc. **15**(1), 1–22 (2000)
28. Knus, M.A., Lam, T.Y., Shapiro, D.B., Tignol, J.P.: Discriminants of involutions on biquaternion algebras. In: K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992). *Proceedings of the Symposium on Pure Mathematics*, vol. 58, pp. 279–303. American Mathematical Society, Providence, RI (1995)
29. Knus, M.A., Merkurjev, A., Rost, M., Tignol, J.P.: The book of involutions. *American Mathematical Society Colloquium Publications*, vol. 44. American Mathematical Society, Providence, RI (1998); with a preface in French by J. Tits
30. Knus, M.A., Parimala, R., Sridharan, R.: Pfaffians, central simple algebras and similitudes. Math. Z. **206**(4), 589–604 (1991)
31. Laghribi, A.: Isotropie de certaines formes quadratiques de dimensions 7 et 8 sur le corps des fonctions d'une quadrique. Duke Math. J. **85**(2), 397–410 (1996)
32. Lam, T.Y.: Introduction to quadratic forms over fields. *Graduate Studies in Mathematics*, vol. 67. American Mathematical Society, Providence, RI (2005)
33. Lewis, D.W.: A note on trace forms and involutions of the first kind. Exposition. Math. **15**(3), 265–272 (1997)
34. Lewis, D.W., Tignol, J.P.: On the signature of an involution. Arch. Math. (Basel) **60**(2), 128–135 (1993)
35. ———: Classification theorems for central simple algebras with involution. Manuscripta Math. **100**(3), 259–276 (1999); with an appendix by R. Parimala
36. MacDonald, M.L.: Cohomological invariants of odd degree Jordan algebras. Math. Proc. Camb. Philos. Soc. **145**(2), 295–303 (2008)
37. Mammone, P., Shapiro, D.B.: The Albert quadratic form for an algebra of degree four. Proc. Am. Math. Soc. **105**(3), 525–530 (1989)
38. Masquelein, A., Quéguiner-Mathieu, A., Tignol, J.P.: Quadratic forms of dimension 8 with trivial discriminant and Clifford algebra of index 4. Arch. Math. (Basel) **93**(2), 129–138 (2009)
39. Merkurjev, A.S.: Simple algebras and quadratic forms. Izv. Akad. Nauk SSSR Ser. Mat. **55**(1), 218–224 (1991)
40. Merkurjev, A.S., Parimala, R., Tignol, J.P.: Invariants of quasitrivial tori and the Rost invariant. Algebra i Analiz **14**(5), 110–151 (2002)
41. Parimala, R., Sridharan, R., Suresh, V.: Hermitian analogue of a theorem of Springer. J. Algebra **243**(2), 780–789 (2001)
42. Pfister, A.: On the Milnor conjectures: history, influence, applications. Jahresber. Deutsch. Math.-Verein. **102**(1), 15–41 (2000)

43. Quéguiner, A.: Signature des involutions de deuxième espèce. Arch. Math. (Basel) **65**(5), 408–412 (1995)
44. ———: Cohomological invariants of algebras with involution. J. Algebra **194**(1), 299–330 (1997)
45. Quéguiner-Mathieu, A.: Invariants cohomologiques: des formes quadratiques aux algèbres à involution. In: Théorie des nombres (Besançon, 2002). *Publications mathmatiques de l'UFR Sciences et techniques de Besançon*, p. 12. University of Franche-Comté, Besançon (2002)
46. Rost, M., Serre, J.P., Tignol, J.P.: La forme trace d'une algèbre simple centrale de degré 4. C.R. Math. Acad. Sci. Paris **342**(2), 83–87 (2006)
47. Rowen, L.H.: Central simple algebras. Israel J. Math. **29**(2–3), 285–301 (1978)
48. Scharlau, W.: Quadratic and Hermitian forms. *Grundlehren der mathematischen Wissenschaften*, vol. 270. Springer, Berlin (1985)
49. Serre, J.P.: Cohomologie galoisienne. *Lecture Notes in Mathematics*, vol. 5, 5th edn. Springer, Berlin (1994)
50. Sivatski, A.S.: Applications of Clifford algebras to involutions and quadratic forms. Commun. Algebra **33**(3), 937–951 (2005)
51. Tamagawa, T.: Representation theory and the notion of the discriminant. In: Algebraic number theory. *Kyoto International Symposium on Research Institute for Mathematical Sciences, University of Kyoto, Kyoto, 1976*, pp. 219–227. Japan Society for the Promotion of Science, Tokyo (1977)
52. Tits, J.: Formes quadratiques, groupes orthogonaux et algèbres de Clifford. Invent. Math. **5**, 19–41 (1968)
53. ———: Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque. J. Reine Angew. Math. **247**, 196–220 (1971)
54. ———: Théorie des groupes. Ann. Collège France **91**, 125–138 (1992) (1990/1991)

Witt Groups of Varieties and the Purity Problem

Kirill Zainoulline

Summary We provide a general algorithm used to prove purity for functors with transfers. As a basic example we consider the Witt group of an algebraic variety.

1 The Witt Ring of a Field

Symmetric bilinear spaces. Let k be a field of characteristic $\neq 2$. A *symmetric bilinear space* over k is a pair (V,b) consisting of a vector space V and a symmetric isomorphism $b\colon V \to V^{\#}$ into its dual $V^{\#} = \mathrm{Hom}_k(V,k)$.

Observe that the map b defines a symmetric bilinear form $B\colon V \times V \to k$ via $B(x,y) := b(x)(y)$. Given a basis $\{e_1, e_2, \ldots, e_n\}$ of V and a symmetric bilinear space there is a symmetric matrix

$$M_b := \Big(b(e_i)(e_j)\Big)_{i,j=1,\ldots,n} = \Big(B(e_i,e_j)\Big)_{i,j=1,\ldots,n}.$$

By definition, the map $b\colon V \to V^{\#}$ is an isomorphism if and only if M_b is invertible.

Isometries. Assume we are given two symmetric bilinear spaces (V,b) and (V',b'). An *isometry* $\varphi\colon (V,b) \to (V',b')$ between them is an isomorphism $\varphi\colon V \to V'$ of vector spaces such that the square

---

Kirill Zainoulline
Department of Mathematics and Statistics, University of Ottawa, 585 King Edward, Ottawa, ON, Canada
e-mail: kirill@uottawa.ca

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_9,

$$
\begin{tikzcd}
V \arrow[r, "\varphi"] \arrow[d, "b"] & V' \arrow[d, "b'"] \\
V^{\#} & V'^{\#} \arrow[l, "\varphi^{\#}"']
\end{tikzcd}
$$

commutes. For the respective matrices M_b and $M_{b'}$, it means that

$$M_{b'} = C_\varphi^t \cdot M_b \cdot C_\varphi,$$

where C_φ is the transformation matrix corresponding to φ.

Hyperbolic spaces. We define the hyperbolic space of V as

$$H(V) := \left(V \oplus V^{\#}, \begin{pmatrix} 0 & id \\ id & 0 \end{pmatrix} \right).$$

A symmetric bilinear space isometric to $H(V)$ is called *hyperbolic*.

The Witt ring. We define the *orthogonal sum* and the *tensor product* of symmetric bilinear spaces as

$$(V,b) \perp (V',b') := (V \oplus V', b \oplus b'),$$
$$(V,b) \otimes (V',b') := (V \otimes V', b \otimes b').$$

The orthogonal sum and the tensor product respect isometries.

Let $KO(k)$ denote the *Grothendieck group* of isometry classes of symmetric bilinear spaces with respect to the orthogonal sum. Let H be the subgroup of $KO(k)$ generated by the classes of hyperbolic spaces. The *Witt group* of k is defined to be the quotient

$$W(k) := KO(k)/H.$$

The tensor product of spaces turns $W(k)$ into a commutative ring with a unit $1 = (k, id)$, where k is a vector space of rank 1.

Properties:

- Let l/k be a field extension. The base change induces a ring homomorphism $i^*\colon W(k) \to W(l)$. Hence, the assignment $l/k \mapsto W(l)$ is a covariant functor from the category of field extensions to the category of commutative rings.
- Let l/k be a finite field extension and $s\colon l \to k$ be a nontrivial k-linear map. Then the composite $s \circ B$, where B is a bilinear form over l, defines a bilinear form over k and, moreover, induces a well-defined group homomorphism $s_*\colon W(l) \to W(k)$ called a Scharlau *transfer*.
- There is the *projection formula*:

$$s_*(i^*(\alpha) \cdot \beta) = \alpha \cdot s_*(\beta) \quad \text{for } \alpha \in W(k) \text{ and } \beta \in W(l).$$

  In particular, the composite $s_* \circ i^*\colon W(k) \to W(k)$ is given by multiplication by $s_*(1)$.

Relations with quadratic forms. By a *quadratic form* q over k, we mean a homogeneous polynomial of degree 2 over k

$$q(x) = \sum_{i,j=1,\dots,n} a_{ij}x_ix_j \quad \text{with } a_{ij} \in k.$$

Assume we are given a symmetric bilinear space (V,b). Let M_b be the symmetric matrix corresponding to the space (V,b) and the chosen basis $\{e_1,e_2,\dots,e_n\}$. We can associate to M_b a quadratic form

$$q(x) = x^t \cdot M_b \cdot x.$$

In the opposite direction, let $q(x)$ be a quadratic form over k. Then we may define a symmetric matrix M_q as

$$M_q := \left(\frac{1}{2}(a_{ij}+a_{ji})\right)_{ij}$$

and, hence, a map $b\colon V \to V^{\#}$ by $b(e_i)(e_j) := (M_q)_{ij}$. If b is an isomorphism, then q is called *nonsingular*.

We have just provided a bijection

$$\boxed{\begin{array}{c}\textit{isometry classes}\\ \textit{of nonsingular}\\ \textit{quadratic forms}\end{array}} \leftrightarrow \boxed{\begin{array}{c}\textit{isometry classes of}\\ \textit{symmetric bilinear spaces}\end{array}}$$

which is compatible with the orthogonal sum and the tensor product of spaces. Hence, to compute the Witt group we can use the language of quadratic forms. The following two properties turn out to be very important for computations:

- *Diagonalization.* Any quadratic form q over k can be diagonalized. Namely, there exists an isometry such that q transforms into a diagonal form

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 \quad \text{where } a_i \in k.$$

  We denote such a form as $\langle a_1,a_2,\dots,a_n\rangle$. In particular, a hyperbolic space corresponds to the form $\langle 1,-1,1,-1,\dots,1,-1\rangle$.
- *Witt decomposition.* Any nonsingular quadratic form q can be written uniquely (up to an isometry) as an orthogonal sum of a maximal hyperbolic subspace H and the so called anisotropic part of q

$$q = q_{an} \perp H.$$

Examples.

- $W(\mathbb{C}) = \mathbb{Z}/2$ or, more generally, $W(k) = \mathbb{Z}/2$ whenever k is quadratically closed, that is, any element of k is a square. Indeed, in this case any form can be diagonalized to $\langle 1,1,\dots,1\rangle$
- $W(\mathbb{R}) = \mathbb{Z}$ (use the signature)

- $W(\mathbb{F}_p) = \begin{cases} \mathbb{Z}/2[k^*/k^{*2}] & \text{if } p \equiv 1 \mod 4 \\ \mathbb{Z}/4 & \text{if } p \equiv 3 \mod 4 \end{cases}$

2 The Witt Ring of a Variety

The affine case. Let R be a commutative ring with unit, $1/2 \in R$. The previous definition of the Witt ring perfectly works if one replaces

a field k	*by*	*a ring R*
a k-vector space V	*by*	*a finitely generated projective R-module P*
an isomorphism b	*by*	*an isomorphism of R-modules* $b\colon P \to P^{\#}$

In this way, we obtain the definition of the Witt ring of a commutative ring R. Let $X = \mathrm{Spec}(R)$ be the associated affine scheme. Then we define

$$W(X) := W(R).$$

The Euler trace. We extend the notion of the Scharlau transfer to the affine case as follows.

Let T/S be a finite flat extension of commutative rings. Let $s\colon T \to S$ be an S-linear map such that the induced map

$$\lambda\colon T \to \mathrm{Hom}_S(T,S)$$

defined by $\lambda(x)(y) := s(xy)$ is an isomorphism.

Then to every symmetric bilinear space (P,B) over T, we associate the bilinear form $(P_S, s \circ B)$, where P_S denotes P considered as an S-module. This bilinear form gives rise to a symmetric bilinear space over S and, moreover, induces a generalized Scharlau transfer

$$s_*\colon W(T) \to W(S).$$

Example. Let k be a field and let T/S be a finite extension of smooth, purely d-dimensional k-algebras. Let Ω_S and Ω_T be the modules of Kähler differentials of S and T over k and let $\omega_S = \bigwedge^d \Omega_S$ and $\omega_T = \bigwedge^d \Omega_T$.

Assume ω_S and ω_T are trivial. Then there exists an isomorphism of T-modules

$$\lambda\colon T \xrightarrow{\cong} \mathrm{Hom}_S(T,S)$$

which induces an S-linear map $\varepsilon\colon T \to S$ via $\varepsilon(x) := \lambda(1)(x)$, called an *Euler trace*. Observe that from ε we get back λ as $\lambda(x)(y) := \varepsilon(xy)$.

The general case. Let X be a scheme with structure sheaf $\mathscr{O}_X$, $1/2 \in \Gamma(\mathscr{O}_X)$. A symmetric bilinear space over X is a pair $(\mathscr{E}, b)$, consisting of a vector bundle $\mathscr{E}$ and an isomorphism $b\colon \mathscr{E} \to \mathscr{E}^{\#}$, where $\mathscr{E}^{\#} = \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{E}, \mathscr{O}_X)$ such that $b^{\#} = b$ (we identify $\mathscr{E}$ with its double dual $\mathscr{E}^{\#\#}$).

An isometry $\varphi\colon (\mathscr{E},b) \to (\mathscr{E}',b')$ of symmetric bilinear spaces is an $\mathscr{O}_X$-linear isomorphism such that $\varphi^\# \circ b' \circ \varphi = b$. The orthogonal sum and the tensor product are defined in an obvious way.

If we now introduce hyperbolic spaces $H(\mathscr{E})$ in the same manner as before and then take the quotient, the result will *not* be the Witt group of X but a finer version of it. To obtain the correct definition we have to use the notion of a *metabolic* space instead of hyperbolic. This was first observed by Knebusch [11]. Roughly speaking, the reason is that

$$\textit{metabolic} \;=\; \textit{locally hyperbolic}.$$

Metabolic spaces. Let $(\mathscr{E},b)$ be a symmetric bilinear space over X and let $\mathscr{F}$ be a subbundle of $\mathscr{E}$, that is, a locally direct summand of $\mathscr{E}$.

For a subbundle $\mathscr{F}$ of $\mathscr{E}$ we define its *orthogonal complement* $\mathscr{F}^\perp$ as the kernel of the composite $i^\# \circ b$, where $i^\#\colon \mathscr{E}^\# \to \mathscr{F}^\#$ is the dual of the inclusion $i\colon \mathscr{F} \to \mathscr{E}$. Clearly, $i^\#$ is an epimorphism and b induces an isomorphism $\mathscr{E}/\mathscr{F}^\perp \to \mathscr{F}^\#$. In particular, $\mathscr{F}^\perp$ is again a subbundle of $\mathscr{E}$.

A subbundle $\mathscr{F}$ of $\mathscr{E}$ is called a *lagrangian* of $\mathscr{E}$ if $\mathscr{F} = \mathscr{F}^\perp$. A symmetric bilinear space is called *metabolic* if it contains a lagrangian.

Observe that in the field case, that is, $X = \mathrm{Spec}(k)$, the orthogonal complement of a subspace U of (V,b) coincides with

$$U^\perp = \{x \in V \mid B(x,y) = 0 \text{ for all } y \in U\},$$

where B is the corresponding bilinear form.

The Witt group. It is defined to be the quotient of the Grothedieck group $KO(X)$ of isometry classes of symmetric bilinear spaces over X modulo the subgroup M generated by metabolic spaces, that is,

$$W(X) := KO(X)/M.$$

As before, the tensor product turns $W(X)$ into a ring. Note that in the affine case this definition gives the previously defined Witt ring.

Examples.

- $W(\mathbb{A}^n_X) = W(X)$, where X is affine – Karoubi [10]
- $W(\mathbb{P}^n_k) = W(k)$ for $n = 1$ follows from the description of vector bundles over the projective line and for $n \geq 2$ – Arason [1]
- For an irreducible smooth quasiprojective complex curve C

$$W(C) = \mathbb{Z}/2 \oplus \mathrm{Disc}(C),$$

where $\mathrm{Disc}(C)$ is the group of isometry classes of symmetric bilinear spaces of rank 1. (This follows from [9].) In particular, if C is projective of genus g, then

$$W(C) = (\mathbb{Z}/2)^{1+2g}.$$

For conic, elliptic, and hyperelliptic curves, see Parimala [18].

- For an irreducible smooth quasiprojective complex surface X

$$W(X) = \mathbb{Z}/2 \oplus \mathrm{Disc}(X) \oplus {}_2\mathrm{Br}(X).$$

For real projective surfaces, see Sujatha [21]. For affine threefolds, see Parimala [19].

One of the main technical tools is the exact sequence

$$W(X) \to W(k(X)) \xrightarrow{\partial_x} \bigoplus_{x \in X^{(1)}} W(k(x)),$$

where X is an integral regular scheme over k, $k(X)$ is its quotient field, $k(x)$ is the residue field at a point x of codimension 1, and ∂_x is a second residue homomorphism which depends on the choice of a local parameter. The exactness of this sequence at the $W(k(X))$-term is called *purity* and is the main subject of these lectures.

Purity for the Witt groups is known for the following cases:

- X is a regular integral noetherian scheme of dimension at most 2 by Colliot-Thélène and Sansuc [8].
- X is a regular integral noetherian affine scheme of dimension 3 by Ojanguren, Parimala, Sridharan, Suresh [15].
- $X = \mathrm{Spec}(R)$, where R is a local regular ring containing a field by Ojanguren and Panin [14].

Triangular Witt groups. A vast generalization of the notion of the Witt group of a scheme was provided by Balmer [2]. He introduced and studied the notion of the Witt group $\mathscr{W}$ of a *triangulated category with duality*. For triangular Witt groups the following computations were obtained:

- $\mathscr{W}(\mathbb{P}_X(\mathscr{E}))$, $\mathscr{W}(\text{quadric})$ by Nenashev [12], Walter
- $\mathscr{W}(\text{Grassmannian})$ by Balmer and Calmès [4]

3 Purity

Let A be a smooth algebra over an infinite field k and let K be its quotient field. Let $R = A_{\mathfrak{q}}$ be the localization of A at a prime ideal $\mathfrak{q} \in \mathrm{Spec}(A)$. Such a ring R is called a *local regular ring of geometric type*.

Let $F : A\text{-Alg} \to Ab$ be a covariant functor from the category of A-algebras to the category of Abelian groups. From now on

- the local regular ring of geometric type R
- the covariant functor F

will be the main objects of our discussion.

Definition 1. (cf. [6, 2.1.1]) For every prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$, consider the group homomorphism $F(R_{\mathfrak{p}}) \to F(K)$ induced by the canonical inclusion of $R_{\mathfrak{p}}$ into its quotient field K.

We say that an element $\alpha \in F(K)$ is *unramified at a prime ideal* $\mathfrak{p}$ if it is in the image of $F(R_{\mathfrak{p}})$. We say that an element $\alpha \in F(K)$ is *unramified over* R if it is unramified at every prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ of height 1.

Definition 2. (cf. [6, 2.1.4.(b)]) We say that *purity* holds for the functor F over R if every unramified element of $F(K)$ belongs to the image of $F(R)$ in $F(K)$. In other words, the following equality holds between subgroups of $F(K)$:

$$\bigcap_{ht\ \mathfrak{p}=1} \mathrm{im}\{F(R_{\mathfrak{p}}) \to F(K)\} = \mathrm{im}\{F(R) \to F(K)\}.$$

The subgroup of unramified elements (the left-hand side of the equality) will be denoted by $F_{nr}(K)$.

Remark. Purity is a particular case of the following more general problem, called the Gersten conjecture: Given a cohomology theory $F = H^*$ over R, show that the *Gersten complex*

$$0 \to H^*(R) \to H^*(K) \to \bigoplus_{x \in U^{(1)}} H^{*-1}(k(x)) \to \bigoplus_{x \in U^{(2)}} H^{*-2}(k(x)) \to \cdots$$

is exact.

Here H^* is a functor to the category of graded abelian groups which satisfies certain axioms (homotopy invariance, excision, localization, etc.) as in [7, Sect. 5] or [16, Sect. 2]. Observe that exactness at the $H^*(K)$-term gives purity.

For the Witt groups the Gersten conjecture was proven

- for a local regular ring of geometric type over an infinite field of characteristic not 2 – Balmer [3] and Schmid [20]
- for a local regular ring R containing a field of characteristic not 2 – Balmer, Gille, Panin, and Walter [5]

Remark. Purity is closely related to the following problem, called *injectivity*: Given a regular local ring R and a functor F from the category of R-algebras to the category of pointed sets, show that the induced map $F(R) \to F(K)$ has a trivial kernel.

If $F = H^1_{et}(-, G)$, where G is a smooth reductive group scheme over R, it is equivalent to the Grothendieck-Serre conjecture (see [8, 6.5, p. 124]) which is still open. For the Witt groups the injectivity is due to Ojanguren [13] and Pardon.

Our goal is to prove the following general fact (see [22]).

Theorem 3 (Purity Theorem). *Let R be a local regular ring of geometric type obtained by localizing a smooth k-algebra A. Let $F\colon A\text{-Alg} \to Ab$ be a functor with transfers described below. Then purity holds for F over R.*

As a corollary of the proof we obtain the following celebrated result.

Theorem 4 (Ojanguren, Panin). *Let R be a regular local ring containing a field k,* $\mathrm{char}(k) \neq 2$. *Then purity holds for the Witt functor $F = W$ over R.*

- The proof of Theorem 3 uses the same techniques as the original proof by Ojanguren–Panin.
- The Witt group formally does not satisfy the condition of being a functor with transfers. Nevertheless, since for all varieties appearing in the proof the canonical sheaves ω turn out to be trivial, the proof works after replacing transfers by Euler traces.

Functors with transfers. Let R be a local regular ring of geometric type obtained by localizing a smooth k-algebra A. Let $F\colon A\text{-Alg} \to Ab$ be a covariant functor. We say the F is a *functor with transfers* if it satisfies the following axioms:

(C) (Continuity) Roughly speaking, it says that F commutes with filtered direct limits of localizations. More precisely, for any A-algebra S essentially smooth over k and for any multiplicative system M in S the canonical map

$$\lim_{g \in M} F(S_g) \to F(M^{-1}S)$$

is an isomorphism, where $M^{-1}S$ denotes the localization of S with respect to M.

(T) (Structure of transfer maps) Let $F_R\colon R\text{-Alg} \to Ab$ denote the restriction of the functor F to the category of R-algebras via the canonical inclusion $A \hookrightarrow R$. For any finite étale R-algebra T, there exist homomorphisms

$$\mathrm{Tr}_R^T\colon F_R(T) \to F_R(R) \quad \text{and} \quad \mathrm{Tr}_K^{T\otimes_R K}\colon F_R(T \otimes_R K) \to F_R(K)$$

called transfer maps which satisfy the following conditions:

(a) $\mathrm{Tr}_R^R = id_R$ and for any finite étale R-algebras T_1 and T_2 the following relation holds

$$\mathrm{Tr}_R^{T_1 \times T_2}(x) = \mathrm{Tr}_R^{T_1}(x_1) + \mathrm{Tr}_R^{T_2}(x_2).$$

(b1) Let $R[t]$ denote a polynomial ring over R. For a finite $R[t]$-algebra S such that $S/(t)$ and $S/(t-1)$ are finite étale over R the following diagram commutes:

$$\begin{tikzcd}
F_R(S) \arrow[r] \arrow[d] & F_R(S/(t)) \arrow[d, "\mathrm{Tr}"] \\
F_R(S/(t-1)) \arrow[r, "\mathrm{Tr}"'] & F_R(R)
\end{tikzcd}$$

(b2) The transfer map $\mathrm{Tr}_K^{T\otimes_R K}$ satisfies conditions (a) and (b1) above and the following diagram induced by extension of scalars via the canonical inclusion $R \hookrightarrow K$ commutes:

$$\begin{tikzcd} F_R(T) \arrow[r] \arrow[d, "\mathrm{Tr}"'] & F_R(T\otimes_R K) \arrow[d, "\mathrm{Tr}"] \\ F_R(R) \arrow[r] & F_R(K) \end{tikzcd}$$

Observe that if F is *homotopy invariant*, that is, if the canonical inclusion induces an isomorphism $F_R(R') \simeq F_R(R'[t])$ for any R-algebra R', and transfer maps satisfy the general base change, that is, (b2) holds for any extension R'/R, then the condition (b1) follows automatically.

(E) (Finite monodromy) A certain technical condition which, roughly speaking, means that restrictions of F via canonical maps $A \to A\otimes_k A$, $a \mapsto a\otimes 1$ and $a \mapsto 1\otimes a$, become locally isomorphic in the étale topology. This condition holds automatically for the Witt group and for any functor defined over a field.

Examples. Let S be a k-algebra.

- $F = \mathbb{G}_m$, that is, $F\colon S \mapsto S^*$. Purity is equivalent to the exact sequence

$$R^* \to K^* \xrightarrow{\oplus v_\mathfrak{p}} \bigoplus_{ht\,\mathfrak{p}=1} \mathbb{Z}$$

- For the functors K_* of K-theory purity means that the sequence

$$K_*(R) \to K_*(K) \xrightarrow{\partial_\mathfrak{p}} \bigoplus_{ht\,\mathfrak{p}=1} K_{*-1}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p})$$

is exact.
- $F = \mathrm{coker}(\mu)$, where $\mu\colon G \to \mathbb{G}_m$ is a surjective morphism of group schemes and G is a linear algebraic group over k, $\mathrm{char}(k) = 0$, which is rational as a k-variety.
- $F = H^*_{et}(-,\mathscr{C})$, where $\mathscr{C}$ is a locally constant sheaf with finite stalks of $\mathbb{Z}/n$-modules over R, $(n,\mathrm{char}(k)) = 1$.
- $F = \mathrm{coker}(\mathrm{Nrd})$, where $\mathrm{Nrd}\colon \mathrm{GL}_{1,\mathscr{A}} \to \mathbb{G}_m$ is the reduced norm of an Azumaya algebra $\mathscr{A}$ over R.
- $F = \mathrm{coker}(\mathrm{Sn})$, where $\mathrm{Sn}\colon \mathrm{SO}_q \to H^1_{et}(-,\mu_2)$ is the spinor norm of a nonsingular quadratic form q defined over R.
- $F = \mathrm{coker}(\mathrm{Nrd})$, where $\mathrm{Nrd}\colon U(\mathscr{A},\sigma) \to U(Z,\sigma|_Z)$ is the reduced norm from the unitary group of an Azumaya algebra $\mathscr{A}$ with involution of the second kind σ over R to the unitary group of its center Z.

We also have the torsion versions of the previous cases. Here $d > 1$ and S is an R-algebra.

- $F\colon S \mapsto S^*/\mathrm{Nrd}(\mathscr{A}_S^*)\cdot(S^*)^d$
- $F\colon S \mapsto U(Z,\sigma)/\mathrm{Nrd}(U(\mathscr{A},\sigma))\cdot U(Z,\sigma)^d$

4 The Proof of the Purity Theorem

First, we discuss two main geometric ingredients of the proof: the Geometric Presentation Lemma and the Quillen trick.

Lemma 5 (Geometric Presentation Lemma). *Let R be a local essentially smooth k-algebra with maximal ideal $\mathfrak{m}$ over an infinite field k, and S an essentially smooth integral k-algebra, finite over the polynomial algebra $R[t]$. Suppose that $\varepsilon\colon S \to R$ is an R-augmentation and let $I = \ker \varepsilon$. Assume that $S/\mathfrak{m}S$ is smooth over the residue field $R/\mathfrak{m}$ at the maximal ideal $\varepsilon^{-1}(\mathfrak{m})/\mathfrak{m}S$. Then, given a regular function $f \in S$ such that $S/(f)$ is finite over R, we can find a $t' \in I$ such that:*

- *S is finite over $R[t']$.*
- *There is an ideal J comaximal with I such that $I \cap J = (t')$.*
- *The ideals J and $(t'-1)$ are comaximal with the ideal (f).*
- *$S/(t')$ and $S/(t'-1)$ are étale over R.*

Proof. We will only show how to construct this t' and establish the first property and the part of the last.

Replacing t by $t - \varepsilon(t)$ we may assume that $t \in I$. We denote by "bar" the reduction modulo $\mathfrak{m}$. By the assumptions made on S the quotient $\bar{S} = S/\mathfrak{m}S$ is smooth over the residue field $\bar{R} = R/\mathfrak{m}$ at its maximal ideal $\bar{I} = \varepsilon^{-1}(\mathfrak{m})/\mathfrak{m}S$.

Choose an $\alpha \in S$ such that $\bar{\alpha}$ is a local parameter of the localization of $\bar{S}$ at $\bar{I}$. By the Chinese Remainder theorem we may assume that $\bar{\alpha}$ does not vanish at the zeros of $\bar{f}$ different from $\bar{I}$.

Without changing $\bar{\alpha}$ we may replace α by $\alpha - \varepsilon(\alpha)$ and assume that $\alpha \in I$. Since S is integral over $R[t]$, there exists a relation of integral dependence

$$\alpha^n + p_1(t)\alpha^{n-1} + \cdots + p_n(t) = 0. \qquad (*)$$

For any $r \in k^\times$ and any N larger than the degree of each $p_i(t)$ we put

$$t' = \alpha - rt^N.$$

By the equation $(*)$, t is integral over $R[t']$. Hence S, which is integral over $R[t]$, is integral over $R[t']$ and the first property is proven.

By Bertini's theorem we may choose α such that the algebra $\bar{S}/(\bar{\alpha})$ is étale over $\bar{R}$. Consider the fiber product diagram

$$\begin{tikzcd} \bar{S}[u]/(\bar{\alpha} - u\bar{t}^N) \arrow[r] & \bar{S}/(t') \\ k[u] \arrow[u, "\pi"] \arrow[r, "u\mapsto r"] & k \arrow[u] \end{tikzcd}$$

Since the fiber of π at $u = 0$ is étale, the fibers of π at almost all rational points $u \in k^\times$ are étale. In other words, $\bar{S}/(\bar{t}')$ is étale over k and, hence, over $\bar{R}$ for almost all $r \in k^\times$.

By assumption S and $R[t']$ are smooth. Since S is finite over $R[t']$, S is finitely generated projective as an $R[t']$-module and, hence, $S/(t')$ is free as an R-module. In particular, $S/(t')$ is flat over R. Finally, the fact that $\bar{S}/(\bar{t}')$ is étale over $\bar{R}$ implies that $S/(t')$ is étale over R. $\square$

Observe that in the original statement of the geometric presentation lemma by Panin–Ojanguren the last condition (that the fibers are étale) was missing. Hence, our lemma (see [22, Theorem 6.1]) provides a slightly stronger version. This difference becomes important when one looks for transfer maps related with certain group schemes (e.g., the spinor norm case discussed in [23]).

The following fact, which is due to Quillen, can be viewed as a generalization of Noether's Normalization Lemma.

Lemma 6 (Quillen's trick). *Let A be a smooth finite-type algebra of dimension d over a field k. Let $f \in A$ be a regular function. Let $\mathscr{I}$ be a finite subset of* $\mathrm{Spec}(A)$.

Then there exist functions $x_1,\dots,x_d$ in A algebraically independent over k such that if $\mathfrak{i}\colon W = k[x_1,\dots,x_{d-1}] \to A$ denotes the inclusion, then

- *$A/(f)$ is finite over W.*
- *A is smooth over W at the points of $\mathscr{I}$.*
- *The inclusion $\mathfrak{i}$ factors as $\mathfrak{i}\colon W \hookrightarrow W[x_d] \to A$, where the last map is finite.*

A generalization of this lemma involving some support condition was proven recently by Panin and the author in [17].

Proof of the Purity Theorem. Let $R = A_{\mathfrak{q}}$ be a localization of a smooth k-algebra A at a prime ideal $\mathfrak{q}$ and let K be its quotient field. We have to prove that any unramified element $\alpha \in F_{nr}(K)$ belongs to the image of the canonical map $i_K^*\colon F(R) \to F(K)$. We give only a brief sketch of the proof.

The proof consists of three steps.

Step 1. We may choose $f \in A$ in such a way that the element α is the image of some element α_f by means of the canonical map $F(A_f) \to F_{nr}(K)$. By applying Quillen's trick to the algebra A, the function f and the subset $\mathscr{I} = \{\mathfrak{q}\}$ we obtain the commutative diagram

$$\begin{tikzcd} A \arrow[r, "a\mapsto a\otimes 1"] & A\otimes_W R \\ W \arrow[u] \arrow[r, "\mathfrak{i}"] & R \arrow[u, "r\mapsto 1\otimes r"'] \end{tikzcd}$$

where $\mathfrak{i}\colon W \to A \to A_{\mathfrak{q}}$ is the respective inclusion of the ring of polynomials W. Let

$$\varphi\colon F(A_f) \to F((A\otimes_W R)_f)$$

be the map induced by the upper horizontal arrow.

Step 2. Let $S = A \otimes_W R$. It is easy to check that S/R and $f = f \otimes 1 \in S$ satisfy the hypothesis of the Geometric Presentation Lemma. Applying that lemma (with $t = x_d$) we then construct $t' \in R[t]$ and the ideal J. Let

$$\psi\colon F(S_f) \to F(R)$$

be the map defined by $\psi = \mathrm{Tr}_1 \circ p_1^* - \mathrm{Tr}_J \circ p_J^*$, where $p_1\colon S_f \to S/(t'-1)$, $p_J\colon S_f \to S/J$ are the quotient maps and Tr_1, Tr_J are the respective transfers.

This is a key point of the proof: There is no map $F(S_f) \to F(R)$ which comes from a regular one, however, by the Geometric Presentation Lemma one can define its substitute ψ using transfers.

Step 3. Consider the commutative diagram

$$\begin{tikzcd}
F(A_f) \arrow[r, "\varphi"] & F(S_f) \arrow[r, "i_K^*"] \arrow[d, "\psi"'] & F((S \otimes_R K)_f) \arrow[d, "\psi_K"] \\
& F(R) \arrow[r, "i_K^*"] & F(K)
\end{tikzcd}$$

where the square is obtained by the base change and the maps φ and ψ were defined before. By commutativity, the image of $\alpha' = \psi(\varphi(\alpha_f))$ in $F(K)$ coincides with $\psi_K(\beta)$, where $\beta = i_K^*(\varphi(\alpha_f))$. By the homotopy invariance *(b2)* we obtain that

$$\psi_K(\beta) = \mathrm{Tr}_1 \circ p_1^*(\beta) - \mathrm{Tr}_J \circ p_J^*(\beta) = \mathrm{Tr}_0 \circ p_0^*(\beta) - \mathrm{Tr}_J \circ p_J^*(\beta),$$

and by the additivity *(a)* the latter coincides with the image of the augmentation map $\varepsilon_K^*(\beta)$. Here $\varepsilon_K\colon (S \otimes_R K)_f \to K$ is given by the usual multiplication.

On the other hand, one can show that $\varepsilon_K(\beta) = \varepsilon_K(i_K^*(\varphi(\alpha_f))) = \alpha$. Therefore, α is the image of α' by means of the canonical map i_K^*, and the proof is finished. $\square$

References

1. Arason, J.Kr. Der Wittring projektiver Räume. Math. Ann. 253 (1980), 205–212
2. Balmer, P. Derived Witt groups of a scheme. J. Pure Appl. Algebra 141(2) (1999), 101–129
3. ______. Witt cohomology, Mayer–Vietoris, homotopy invariance and the Gersten conjecture. *K*-Theory 23(1) (2001), 15–30
4. Balmer, P., Calmès, B. Witt groups of Grassmann varieties. Preprint (2008), 28pp
5. Balmer, P., Gille, S., Panin, I., Walter, C. The Gersten conjecture for Witt groups in the equicharacteristic case. Doc. Math. 7 (2002), 203–217
6. Colliot-Thélène, J.-L. Birational invariants, purity and the Gersten conjecture, in K-Theory and Algebraic Geometry: Connections with Quadratic Forms and Division Algebras, AMS Summer Research Institute, Santa Barbara 1992, eds. W. Jacob and A. Rosenberg, Proceedings of Symposia in Pure Mathematics 58, Part I (1995) 1–64
7. Colliot-Thélène, J.-L., Hoobler, R., Kahn, B. The Bloch–Ogus–Gabber theorem, in Algebraic K-Theory, 31-94, Fields Institute Communications 16, American Mathematics Society, Providence, RI, 1997

8. Colliot-Thélène, J.-L., Sansuc, J.-J. Fibrés quadratiques et composantes connexes réelles. Math. Ann. 244 (1979), 105–134
9. Elman, R., Lam, T.Y. Quadratic forms over formally real fields and pythagorean fields. Am. J. Math. 94 (1972), 1155–1194
10. Karoubi, M. Localisation de formes quadratiques II. Ann. Sci. Éc. Norm. Sup. 4e série 8 (1975), 99–155
11. Knebusch, M. Symmetric bilinear forms over algebraic varieties, in Conference on Quadratic Forms 1976 (Proceedings of a Conference, Queen's University, Kingston, ON, 1976), pp. 103–283. Queen's Papers in Pure and Applied Mathematics, No. 46, Queen's University, Kingston, ON, 1977
12. Nenashev, A. On the Witt groups of projective bundles and split quadrics: geometric reasoning. J. K-Theory 3(3) (2009), 533–546
13. Ojanguren, M. Quadratic forms over regular rings. J. Indian Math. Soc. 44 (1980), 109–116
14. Ojanguren, M., Panin, I. A purity theorem for the Witt group. Ann. Sci. École Norm. Sup. (4) 32(1) (1999), 71–86
15. Ojanguren, M., Parimala, R., Sridharan, R., Suresh, V. Witt groups of the punctured spectrum of a 3-dimensional regular local ring and a purity theorem. J. Lond. Math. Soc., II. Ser. 59(2) (1999), 521–540
16. Panin, I., Zainoulline, K. Variations on the Bloch–Ogus theorem. Doc. Math. 8 (2003), 51–67
17. ———. Gersten resolution with support. Manuscripta Math. 128(4) (2009), 443–452
18. Parimala, R. Witt groups of conics, elliptic, and hyperelliptic curves. J. Number Theory 28 (1988), 69–93
19. ———. Witt groups of affine three-folds. Duke Math. J. 57 (1989), 947–954
20. Schmid, M. Wittringhomologie. Ph.D. Thesis, Universität Regensburg, 1998
21. Sujatha, R. Witt groups of real projective surfaces. Math. Ann. 288(1) (1990), 89–101
22. Zainoulline, K. The purity problem for functors with transfers, K-Theory J. 22(4) (2001), 303–333
23. ———. On Knebusch's norm principle for quadratic forms over semi-local rings. Math. Zeitsch. 251(2) (2005), 415–425

Further Reading (Books)

24. Baeza, R. Quadratic forms over semi-local rings, Lecture Notes in Mathematics, Vol. 655, Springer, Berlin, 1978
25. Knus, M.-A. Quadratic and Hermitian forms over rings. Grundlehren der Mathematischen Wissenschaften, Vol. 294, Springer, Berlin, 1991
26. Knus, M.-A., Merkurjev, A., Rost, M., Tignol, J.-P. The Book of Involutions. AMS Colloquium Publications, Vol. 44, AMS, Providence, RI, 1998
27. Lam, T.Y. The algebraic theory of quadratic forms. Lecture Notes Series, W.A. Benjamin, Reading, MA, 1980
28. Scharlau, W. Quadratic and Hermitian forms. Grundlehren der Mathematischen Wissenschaften, Vol. 270, Springer, Berlin, 1985

Part II
Invited Articles

Some Extensions and Applications of the Eisenstein Irreducibility Criterion

Anuj Bishnoi and Sudesh K. Khanduja

Summary Some generalizations of the classical Eisenstein and Schönemann Irreducibility Criteria and their applications are described. In particular some extensions of the Ehrenfeucht–Tverberg irreducibility theorem, which states that a difference polynomial $f(x) - g(y)$ in two variables is irreducible over a field K provided the degrees of f and g are coprime, are also given.

The discussion of irreducibility of polynomials has a long history. The most famous irreducibility criterion for polynomials with coefficients in the ring $\mathbb{Z}$ of integers proved by Eisenstein [9] in 1850 states as follows:

Eisenstein Irreducibility Criterion. *Let $F(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ be a polynomial with coefficient in the ring $\mathbb{Z}$ of integers. Suppose that there exists a prime number p such that a_0 is not divisible by p, a_i is divisible by p for $1 \le i \le n$, and a_n is not divisible by p^2, then $F(x)$ is irreducible over the field $\mathbb{Q}$ of rational numbers.*

Sometimes this criterion is not directly applicable to a given polynomial $F(x)$ but it may be applicable to $F(x+c)$ for some c, e.g., consider the p-th cyclotomic polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1 = (x^p - 1)/(x-1)$. On changing x to $x+1$, it becomes $x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}$ and hence is irreducible over $\mathbb{Q}$ by the above criterion. This slick proof of the irreducibility for the p-th cyclotomic polynomial was given by Eisenstein, though its irreducibility was proved by Gauss in 1799 and used by him in one of his proofs of Quadratic Reciprocity Law. Over the years, this criterion has witnessed many variations and generalizations using prime ideals, valuations and Newton polygons (see [15], [18, Sects. 3.1, 5.1]).

Anuj Bishnoi
Department of Mathematics, Panjab University, Chandigarh-160014, India,
e-mail: anuj.bshn@gmail.com

Sudesh K. Khanduja (corresponding author)
Department of Mathematics, Panjab University, Chandigarh-160014, India,
e-mail: skhand@pu.ac.in

2010 Mathematics subject classification. 12E05, 12J10, 12J25.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_10,

In 1906, Dumas [7] proved the following generalization of this criterion.

Dumas Criterion. *Let $F(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ be a polynomial with coefficients in $\mathbb{Z}$. Suppose there exists a prime p whose exact power p^{r_i} dividing a_i (where $r_i = \infty$ if $a_i = 0$), $0 \leq i \leq n$, satisfy $r_0 = 0$, $(r_i/i) > (r_n/n)$ for $1 \leq i \leq n-1$ and $\gcd(r_n,\ n)$ equals 1. Then $F(x)$ is irreducible over $\mathbb{Q}$.*

Note that Eisenstein's criterion is a special case of Dumas Criterion with $r_n = 1$. In 1923, Dumas criterion was extended to polynomials over more general fields namely, fields with discrete valuations by Kürschák (cf. [14]). Indeed, it was the Hungarian Mathematician Joseph Kürschák who formulated the formal definition of the notion of valuation of a field in 1912.

Definition. A real valuation v of a field K is a mapping $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ satisfying (i) $v(x) = \infty$ if and only if $x = 0$; (ii) $v(xy) = v(x) + v(y)$; and (iii) $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x,\ y$ in K. $v(K^*)$ is called the value group of v. A valuation is said to be discrete if $v(K^*)$ is isomorphic to $\mathbb{Z}$.

Eisenstein-Dumas-Kürschák Irreducibility Criterion. *Let v be a valuation of a field K with value group $\mathbb{Z}$. Let $F(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ be a polynomial with coefficients from K. If $v(a_0) = 0$, $v(a_i)/i > v(a_n)/n$ for $1 \leq i \leq n-1$ and $v(a_n)$ is coprime to n, then $F(x)$ is irreducible over $\mathbb{Q}$.*

In 1931, Wolfgang Krull generalized the notion of valuation by defining a valuation of a field K to be a mapping:

$$v : K \xrightarrow{\text{onto}} G \cup \{\infty\},$$

where G is a totally ordered (additively written with infinity greater than each element of G) abelian group and v satisfies properties (i), (ii) and (iii) of a real valuation. The pair (K, v) is called a valued field and G is called the value group of v.

In 1997, Khanduja and Saha [13] generalized the Eisenstein–Dumas–Kürschák criterion to polynomials with coefficients from any valued field (K, v).

Theorem 1. *Let v be a Krull valuation of any rank of a field K with value group G and $F(x) = a_0x^s + a_1x^{s-1} + \cdots + a_s$ be a polynomial over K. If $v(a_0) = 0$, $v(a_i)/i \geq v(a_s)/s$ for $1 \leq i \leq s$ and there does not exit any integer $d > 1$ dividing s such that $v(a_s)/d \in G$, then $F(x)$ is irreducible over K.*

Example. Let $F(X,Y) = g(Y)X^s + h(Y)$ be a polynomial over a field L in independent variables X, Y. If $g(Y), h(Y)$ have no common factors and $\deg g(Y) - \deg h(Y)$ is coprime to s, then $F(X,Y)$ is irreducible over L, for we can regard $F(X,Y)/g(Y)$ as a polynomial in X with coefficients over the field $K = L(Y)$ with valuation on K defined by $v(a(Y)/b(Y)) = \deg b(Y) - \deg a(Y)$ and apply Theorem 1.

The following criterion which is more general than the Eisenstein Irreducibility Criterion was proved by Schönemann [19] in 1846.

Classical Schönemann Irreducibility Criterion. *If a polynomial $F(x)$ belonging to $\mathbb{Z}[x]$ has the form $F(x) = f(x)^s + pM(x)$, where p is a prime number, $f(x)$ belonging to $\mathbb{Z}[x]$ is a monic polynomial which is irreducible modulo p, $f(x)$ is co-prime to $M(x)$ modulo p, and the degree of $M(x)$ is less than the degree of $F(x)$, then $F(x)$ is irreducible in $\mathbb{Q}[x]$.*

Eisenstein's Criterion is easily seen to be a particular case of Schönemann Criterion by setting $f(x) = x$.

In 1997, Khanduja and Saha [13] gave a generalization of classical Schönemann Irreducibility Criterion using the theory of prolongations of a valuation defined on K to a simple transcendental extension of K which was initiated by MacLane and developed further by Popescu et al. in [2]. In 2008, Ron Brown [5] gave a different proof of Saha's result.

Notation. 1. Let v be a valuation of a field K with valuation ring $R_v = \{x \in K \mid v(x) \geq 0\}$ having maximal ideal $\mathscr{M}_v = \{x \in K \mid v(x) > 0\}$; $R_v/\mathscr{M}_v$ is called the residue field of v.

2. For any element ξ in R_v, $\bar{\xi}$ will denote its v-residue, i.e., the image of ξ under the canonical homomorphism from R_v onto $R_v/\mathscr{M}_v$. For any polynomial $g(x) \in R_v[x]$, $\bar{g}(x)$ will have similar meaning.

3. We shall denote by v^x the Gaussian valuation of the field $K(x)$ of rational functions in an indeterminate x which extends v and is defined on $K[x]$ by:

$$v^x\left(\sum_i a_i x^i\right) = \min_i\{v(a_i)\}, \qquad a_i \in K.$$

4. If $g(x)$ is a fixed monic polynomial with coefficients in an integral domain R, then each $F(x)$ belonging to $R[x]$ can be uniquely represented as a finite sum $F(x) = \sum_{i\geq 0} F_i(x)g(x)^i$, where for any i, the polynomial $F_i(x) \in R[x]$ has degree less than that of $g(x)$. This representation of $F(x)$ will be referred to as the $g(x)$-expansion of $F(x)$.

With the above notations, Khanduja and Saha [13] proved:

Generalized Schönemann Irreducibility Criterion. *Let v be a valuation of a field K with valuation ring R_v, residue field $R_v/\mathscr{M}_v$ and value group G_v. Let $f(x) \in R_v[x]$ be such that the polynomial $\bar{f}(x)$ is irreducible over $R_v/\mathscr{M}_v$. Assume that the $f(x)$-expansion of $F(x) \in K[x]$ is given by $F(x) = \sum_{i=0}^{s} F_i(x)(f(x))^i$ satisfies $F_s(x) = 1$,*

$$\frac{v^x(F_i(x))}{s-i} \geq \frac{v^x(F_0(x))}{s} > 0 \quad \textit{for } 0 \leq i \leq s-1,$$

and there does not exist any number $d > 1$ dividing s such that $v^x(F_0(x))/d \in G_v$, then $F(x)$ is irreducible over K.

In 2001, Bhatia and Khanduja [3] generalized Eisenstein's Irreducibility Criterion in a different direction.

Theorem 2. *Let v be a valuation of a field K with value group the set of integers. Let $g(x) = x^m + a_1x^{m-1} + \cdots + a_m$ be a polynomial with coefficients in K such that $v(a_i)/i > v(a_m)/m$ for $1 \leq i \leq m-1$. Let r denote $\gcd(v(a_m), m)$ and b be an element of K with $v(b) = v(a_m)/r$. Suppose that the polynomial $z^r + \overline{(a_m/b^r)}$ in the indeterminate z is irreducible over the residue field of v. Then $g(x)$ is irreducible over K.*

Example. Let p be a prime congruent to 3 modulo 4. The polynomial $x^4 + px^3 + p^2x^2 + p^2$ is irreducible over $\mathbb{Q}$.

Using Theorem 2, Bhatia and Khanduja [3] have proved:

Theorem 3. *Let $F(x,y) = cx^n + F_1(y)x^{n-1} + \cdots + F_n(y)$ be a polynomial having coefficients in a field K such that $F_n(y)$ is a nonzero polynomial with leading coefficient c_0 and degree d. Suppose that*

$$\frac{\deg F_i(y)}{i} < \frac{d}{n} \quad \text{for } 1 \leq i \leq n-1.$$

If r denotes $\gcd(d,n)$ and if the polynomial $z^r + c_0/c$ is irreducible over K, then so is $F(x,y)$.

The following theorem, which generalizes a well known result of Ehrenfeucht and Tverberg is an immediate consequence of Theorem 3.

Theorem 4. *Let $f(x)$ and $g(y)$ be nonconstant polynomials with coefficients in a field K. Let c and c_0 denote, respectively, the leading coefficients of $f(x)$ and $g(y)$ and n, m their degrees. If $\gcd(m,n) = r$ and if $z^r - (c_0/c)$ is irreducible over K, then so is $f(x) - g(y)$.*

The result of Theorem 4 has its roots in a theorem of Ehrenfeucht. In 1956, Ehrenfeucht [8] proved that a polynomial $f_1(x_1) + \cdots + f_n(x_n)$ with complex coefficients is irreducible provided the degrees of $f_1(x_1), \ldots, f_n(x_n)$ have greatest common divisor one. In 1964, Tverberg [20] extended this result by showing that if $n \geq 3$ then $f_1(x_1) + \cdots + f_n(x_n)$ belonging to $K[x_1, \ldots, x_n]$ is irreducible over any field K of characteristic zero in case the degree of each f_i is positive. He also proved that a bivariate polynomial $f_1(x_1) + f_2(x_2)$ is irreducible over a field of arbitrary characteristic when the degrees of f_1 and f_2 are coprime.

A polynomial of the form $f(x) - g(y)$ in two variables is called a difference polynomial and a polynomial of the type given in Theorem 3 is called a generalized difference polynomial.

Definition. A polynomial $P(x,y)$ is said to be a generalized difference polynomial (with respect to x) of the type (n,m) if $P(x,y) = cx^m + \sum_{i=1}^{m} P_i(y)x^{m-i}$, where $c \in K^*$, $m \geq 1$, $n = \deg P_m(y) \geq 1$ and $\deg P_i(y) < ni/m$ for $1 \leq i \leq m-1$.

It is known that contrary to appearances, the property of being a generalized difference polynomial is actually symmetric in x and y. Note that every difference polynomial is a generalized difference polynomial. In fact, Bhatia and Khanduja [3] considered irreducibility conditions on more general polynomials called quasi-difference polynomials given by $F(x,y) = cx^e + \sum_{i=1}^{e} P_i(y)x^{e-i},\ c \in K^*,\ e \geq 1$, such that there exists t with $1 \leq t \leq e$ satisfying $\deg_y F(x,y) = \deg P_t(y) = d$ and $\deg P_i(y) < di/t$ for $i \neq t,\ 1 \leq i \leq e$. Also every generalized difference polynomial of the type (d,e) (with respect to x) is a quasi-difference polynomial of the same type, but the converse is not true, e.g., the polynomial $F(x,y) = cx^4 + c_1x^3y + c_2x^2(y^4+y) + c_3x(y^4+y^3) + c_4y^4$ with the coefficients c and c_2 nonzero is a quasi-difference polynomial of the type $(4,2)$ with respect to x that is not a generalized difference polynomial as $d=4$, $e=4$ and $\deg P_i(y) > di/e$ for $i=2$.

In 1990, Panaitopol and Stefănescu [16] proved that a quasi-difference polynomial of the type (d,t) with d and t coprime is irreducible over $K(x)$. It may be pointed out that the irreducibility criterion for a quasi-difference polynomial of the type (d,t) with d and t not necessarily coprime given in [3] extends the criterion of Panaitopol and Stefănescu.

Theorem 5. *Let $P(x,y) = cx^e + P_1(y)x^{e-1} + \cdots + P_e(y)$ be a quasi-difference polynomial of the type (d,t) with respect to x over a field K. Let c_0 denote the leading coefficient of $P_t(y)$ and r the gcd of d and t. If the polynomial $x^r + cc_0^{-1}$ is irreducible over k, then $P(x,y)$ is irreducible over $K(x)$.*

As regards generalized difference polynomials, recently Engler jointly with Khanduja [11] has given an elementary proof of the number of irreducible factors of a generalized difference polynomial by means of the following theorem.

Theorem 6. *Let $P(x,y) = a_0x^m + P_1(y)x^{m-1} + \cdots + P_m(y)$ be a generalized difference polynomial of the type (n,m) with respect to x over a field K. Let r be the greatest common divisor of m and n, and let b_0 be the leading coefficient of $P_m(y)$. Then the number of irreducible factors of $P(x,y)$ over K (counting multiplicities if any) does not exceed the number of K-irreducible factors of the polynomial $x^r + b_0/a_0$.*

Proof. Let

$$P(x,y) = a_0F_1(x,y)\cdots F_s(x,y) \tag{1}$$

be a factorization of $P(x,y)$ as a product of irreducible factors over K. Let x be given the weight n and y the weight m. Let $H_i(x,y)$ denote the sum of those monomials occurring in $F_i(x,y)$ which have the highest weight, then $H_i(x,y)$ is a nonconstant polynomial. Denote b_0/a_0 by $-b$. Keeping in mind the definition of a generalized difference polynomial and comparing the terms of highest weight on both sides of (1), it can be easily seen that:

$$x^m - by^n = H_1(x,y)\cdots H_s(x,y). \tag{2}$$

Let ξ be a primitive r_1-th root of unity, where $r = p^t r_1$ and p does not divide r_1. The integers m/r and n/r will be denoted by m_1 and n_1, respectively. Choose c belonging to the algebraic closure $\widetilde{K}$ of K such that $c^r = b$. Rewrite (2) as:

$$\prod_{i=1}^{r}(x^{m_1} - c\xi^i y^{n_1}) = H_1(x,y)\cdots H_s(x,y). \tag{3}$$

The desired result follows from (3) because a polynomial of the type $x^j - ay^k$ is irreducible over $\widetilde{K}$ when j and k are co-prime.

For polynomials with rational coefficients, the following theorem gives a better estimate than the one given by Theorem 6.

Theorem 7. *Let $P(x,y)$ be a generalized difference polynomial of the type (n,m) over the field $\mathbb{Q}$ of rational numbers. Let r be the greatest common divisor of m and n. Then the number of irreducible factors (counting multiplicities) of $P(x,y)$ over $\mathbb{Q}$ does not exceed the number of positive integers dividing r.*

Proof. Let $b = -b_0/a_0$ be as in the proof of Theorem 6. Fix a complex number c satisfying $c^r = b$ and a primitive d-th root of unity to be denoted by ζ_d for any number d dividing r. Define a polynomial $P_d(x)$ with complex coefficients by:

$$P_d(x) = \prod_{1\le i\le d,(i,d)=1}(x - c\zeta_d^i).$$

Then

$$x^r - b = \prod_{d|r} P_d(x). \tag{4}$$

Observe that if $x - c\zeta_d$ is a factor of a polynomial $h(x)$ belonging to $\mathbb{Q}[x]$, then so is $x - \sigma(c\zeta_d)$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}^{alg}/\mathbb{Q})$ and hence so is $P_d(x)$. It now follows from (4) that the number of $\mathbb{Q}$-irreducible factors of $x^r - b$ does not exceed the number of divisors of r. This proves the theorem in view of Theorem 6.

The following corollary is an immediate consequence of the above theorem.

Corollary. *Let $f(x)$ and $h(y)$ be polynomials having coefficients in $\mathbb{Q}$. Assume that* $\deg f(x)$ *is a prime number. Then $f(x) - f(h(y))$ is a product of two irreducible factors over $\mathbb{Q}$. In particular the polynomial $f(x) - f(y)/x - y$ is irreducible over $\mathbb{Q}$.*

The above corollary sheds some light on a problem posed by Cassels [6] which asks for what polynomials f is the polynomial $f(x) - f(y)/x - y$ reducible over $\mathbb{Q}$.

Definition. A polynomial with coefficients from a valued field (K,v) which satisfies the hypothesis of Theorem 1 is called an Eisenstein–Dumas polynomial with respect to v. A polynomial satisfying the hypothesis of Generalized Schönemann Irreducibility Criterion (stated before Theorem 2) will be referred to as a Generalized Schönemann polynomial with respect to v and $f(x)$.

The following natural question arises:

When is a translate $g(x+a)$ of a given polynomial $g(x)$ with coefficients in a valued field (K,v) an Eisenstein-Dumas polynomial with respect to v?

Recently, we have characterized such polynomials using distinguished pairs defined later. Indeed we have also dealt with the following more general problem in [4].

Let $g(x)$ belonging to $R_v[x]$ be a monic polynomial over a henselian valued field (K,v) of arbitrary rank with $\bar{g}(x) = \phi(x)^e$, where $\phi(x)$ is an irreducible polynomial over $R_v/\mathscr{M}_v$, and let θ be a root of $g(x)$. What are the necessary and sufficient conditions so that $g(x)$ is a Generalized Schönemann polynomial with respect to v and some polynomial $f(x) \in R_v[x]$ with $\bar{f}(x) = \phi(x)$?

Definition. Let v be a henselian valuation of a field K and let $\tilde{v}$ be the unique prolongation of v to the algebraic closure $\widetilde{K}$ of K. A pair (θ,α) of elements of $\widetilde{K}$ is called a distinguished pair (more precisely a (K,v)-distinguished pair) if the following three conditions are satisfied:

(i) $[K(\theta):K] > [K(\alpha):K]$,
(ii) $\tilde{v}(\theta-\beta) \leqslant \tilde{v}(\theta-\alpha)$ for every β in $\widetilde{K}$ with $[K(\beta):K] < [K(\theta):K]$, and
(iii) whenever β belonging to $\widetilde{K}$ is such that $[K(\beta):K] < [K(\alpha):K]$, then $\tilde{v}(\theta-\beta) < \tilde{v}(\theta-\alpha)$.

Properties of distinguished pairs have been studied extensively in [17] and [1].

In [4], we have proved

Theorem 8. *Let v be a henselian valuation of arbitrary rank of a field K with value group G. Let $g(x)$ belonging to $R_v[x]$ be a monic polynomial of degree e having a root θ. Then for an element a of K, $g(x+a)$ is an Eisenstein–Dumas polynomial with respect to v if and only if (θ,a) is a distinguished pair and $K(\theta)/K$ is a totally ramified extension of degree e.*

The following result, which generalizes a result of Juras [12] proved in 2006, has been quickly deduced from the earlier theorem.

Theorem 9. *Let $g(x) = \sum_{i=0}^{e} a_i x^i$ be a monic polynomial with coefficients in a henselian valued field (K,v). Suppose that the characteristic of the residue field of v does not divide e. If there exists an element b belonging to K such that $g(x+b)$ is an Eisenstein–Dumas polynomial with respect to v, then so is $g(x-a_{e-1}/e)$.*

Theorem 8 can be used to construct examples of totally ramified extensions $K(\theta)/K$ such that no translate of the minimal polynomial of θ over K is an Eisenstein–Dumas polynomial with respect to v.

Notation. For α separable over K of degree > 1, $\omega_{\mathrm{K}}(\alpha)$ will stand for the Krasner's constant defined by:

$$\omega_{\mathrm{K}}(\alpha) = \max\left\{\tilde{v}(\alpha-\alpha') \mid \alpha' \neq \alpha \text{ runs over } K\text{-conjugates of } \alpha\right\}.$$

Example. Let K be the field of 2-adic numbers with the usual valuation v_2 given by $v_2(2) = 1$. The prolongation of v_2 to the algebraic closure of K will be denoted by v_2 again. Consider $\theta = 2 + 2(2^{-1/2}) + 2^2(2^{-1/2^2})$ and $\theta_1 = 2 + 2(2^{-1/2})$. It will be shown that $K(\theta) = K(2^{1/4})$ and (θ, θ_1) is a distinguished pair. Note that the Krasner's constant $\omega_K(\theta_1) = 3/2$ and $v_2(\theta - \theta_1) = 7/4 > \omega_K(\theta_1)$. Therefore, by Krasner's Lemma [10, Theorem 4.1.7], $K(\theta_1) \subseteq K(\theta)$ and hence $2^2(2^{-1/4}) = \theta - \theta_1$ belongs to $K(\theta)$ as asserted. To show that (θ, θ_1) is a distinguished pair, we first verify that whenever γ belonging to $\widetilde{K}$ satisfies $v_2(\theta - \gamma) > v_2(\theta - \theta_1) = 7/4$, then $\deg \gamma \geqslant 4$. If γ is as above, we have by the strong triangle law

$$v_2(\theta_1 - \gamma) = \min\{v_2(\theta_1 - \theta), v_2(\theta - \gamma)\} = 7/4 > \omega_K(\theta_1) = 3/2.$$

So by Krasner's Lemma, $K(\theta_1) \subseteq K(\gamma)$ and hence $v_2(K(\gamma))$ contains $v_2(\theta_1 - \gamma) = 7/4$ which implies that $[K(\gamma) : K] \geqslant 4$. Therefore

$$7/4 = v_2(\theta - \theta_1) = \max\left\{ v_2(\theta - \beta) \mid \beta \in \widetilde{K} \text{ and } \deg \beta < 4 \right\}.$$

Also for any $b \in \widetilde{K}$ with $\deg b < \deg \theta_1$, we have $b \in K$ and clearly $v_2(\theta_1 - b) \leqslant 1/2 < v_2(\theta - \theta_1)$. So (θ, θ_1) is a distinguished pair. As can be easily checked, θ is a root of $g(x) = x^4 - 8x^3 + 20x^2 - 80x + 4$ which must be irreducible over K. By Theorem 8, no translate of $g(x)$ can be an Eisenstein–Dumas polynomial with respect to v_2 because (θ, θ_1) is a distinguished pair with $\theta_1 \notin K$ and consequently (θ, a) cannot be a distinguished pair for any a in K. Moreover, if p is a prime number different from 2, then no translate of $g(x)$ can be an Eisenstein–Dumas polynomial with respect to the p-adic valuation v_p, for otherwise in view of Theorem 9, $g(x+2) = x^4 - 4x^2 - 64x - 124$ would be an Eisenstein–Dumas polynomial with respect to v_p, which is not so.

Acknowledgements The first author gratefully acknowledges the financial support of CSIR (grant no. 09/135(0539)/2008-EMR-I).

References

1. K. Aghigh and S. K. Khanduja, On chains associated with elements algebraic over a henselian valued field, *Algebra Colloq.* 12:4 (2005) 607–616.
2. V. Alexandru, N. Popescu and A. Zaharescu, A theorem of characterizaton of residual transcendental extension of a valuation, *J. Math. Kyoto Univ.* 28 (1988) 579–592.
3. S. Bhatia and S. K. Khanduja, Difference polynomials and their generalizations, *Mathematika* 48 (2001) 293–299.
4. A. Bishnoi and S. K. Khanduja, On Eisenstein-Dumas and generalized Schönemann polynomials, *Comm. Algebra* (2010).
5. R. Brown, Schönemann Polynomials in Henselian extension fields, *Indian J. Pure Appl. Math.* 39(5) (2008) 403–410.

6. J. W. S. Cassels, *Factorization of polynomials in several variables.* Proceedings of the 15th Scandinavian congress; Oslo, 1968, Springer Lecture Notes in Mathematics, 118 (1970), 1–17.
7. G. Dumas, Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels, *J. de Math. Pures et Appliquées,* 6 (1906) 191–258.
8. A. Ehrenfeucht, Kryterium absolutnej nierozkladalnosci wielomianow, *Prace Math.,* 2 (1956) 167–169.
9. G. Eisenstein, Über die Irreduzibilität und einige andere Eigenschaften der Gleichungen, *J. für die Reine und Angew. Math.,* 39 (1850) 160–179.
10. A. J. Engler and A. Prestel, *Valued Fields*, Springer-Verlag, Berlin, 2005.
11. A. J. Engler and S. K Khanduja, On irreducible factors of the polynomial $f(x) - g(y)$, *Int. J. Math.* 21(4) (2010) 407–418, http://dx.doi.org/10.1142/S0129167X10006082.
12. M. Juráš, Eisenstein-Dumas criterion for irreducibility of polynomials and projective transformations of the independent variable, *JP J. Algebra Number Theory Appl.*, 6(2) (2006) 221–236.
13. S. K. Khanduja and J. Saha, On a generalization of Eisenstein's irreducibility criterion, *Mathematika,* 44 (1997) 37–41.
14. J. Kürschák, Irreduzible Formen, *J. für die Reine und Angew. Math.,* 152 (1923) 180–191.
15. S. MacLane, The Schönemann-Eisenstein irreducibility criterion in terms of prime ideals, *Trans. Am. Math. Soc.,* 43 (1938) 226–239.
16. L. Panaitopol and D. Stefănescu, On the generalized difference polynomials, *Pacific J. Math.,* 143(2) (1990) 341–348.
17. N. Popescu and A. Zaharescu, On the structure of the irreducible polynomials over local fields, *J. Number Theory,* 52 (1995) 98–118.
18. P. Ribenboim, *The Theory of Classical Valuations*, Springer Verlag, Berlin, 1999.
19. T. Schönemann, Von denjenigen Moduln, welche Potenzen von Primzahlen sind, *J. für die Reine und Angew. Math.*, 32 (1846) 93–105.
20. H. Tverberg, A remark on Ehrenfeucht's criterion for irreducibility of polynomials, *Prace Mat.,* 8 (1964) 117–118.

On the Kernel of the Rost Invariant for E_8 Modulo 3

Vladimir Chernousov

Summary We show that the kernel of the Rost invariant for a split group of type E_8 is trivial modulo 3.

1 Introduction

Let F be a field and let G be a simple simply connected algebraic group over F. With these data one can associate two natural functors $f, g\colon \textbf{Fields} \to \textbf{Sets}$, where **Fields** denotes the category of field extensions of F and **Sets** denotes the category of sets, given by $f(K/F) = H^1(K, G)$ and $g(K/F) = H^3(K, \mathbb{Q}/\mathbb{Z}(2))$.

In the 1990s, Rost constructed a natural transformation between f and g which nowadays is called the Rost invariant of G and it is denoted by $\mathscr{R}_G$. Thus for every field extension K/F we have a natural (functorial) mapping of pointed sets $\mathscr{R}_{G,K}\colon H^1(K,G) \to H^3(K, \mathbb{Q}/\mathbb{Z}(2))$. By abuse of language, instead of $\mathscr{R}_{G,K}$ we will use the abbreviated notation $\mathscr{R}_G$ whenever there is no danger of confusion.

For applications it is important to describe the kernel of $\mathscr{R}_G$. If G is split or quasi-split over F and has small rank then the kernel is trivial by [Gar] (see also [Ch03]). In particular, $\mathrm{Ker}\mathscr{R}_G = 1$ for all groups G of exceptional types but E_8, i.e., for every field extension K/F we have $\mathrm{Ker}\mathscr{R}_{G,K} = 1$. For type E_8 the situation is much more difficult and not much information is available. For instance, we know that the kernel of the Rost invariant is not trivial. Indeed, if $F = \mathbb{Q}$ and $K = \mathbb{R}$ then one checks that the class $[\xi] \in H^1(K,G)$ corresponding to the compact form of E_8 belongs to the kernel of the Rost invariant.

Vladimir Chernousov
Department of Mathematics, University of Alberta, Edmonton, Alberta T6G 2G1, Canada,
e-mail: chernous@math.ualberta.ca

2010 Mathematics subject classification. 20G07, 20G10, 20G15, 20G41.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_11,

In this paper, we address the (slightly simpler) problem of describing the kernel of $\mathscr{R}_G$ modulo a prime number p where G is a split group over F of type E_8. We say that a class $[\xi] \in H^1(K,G)$ is in the kernel of $\mathscr{R}_G$ modulo p if there is a finite field extension L/K of degree prime to p such that $\mathscr{R}_{G,L}([\xi_L]) = 1$. We also say that the kernel of the Rost invariant of G is trivial modulo p if every class $[\xi] \in H^1(K,G)$ which is in the kernel of $\mathscr{R}_G$ modulo p can be killed by a finite field extension L/K of degree prime to p.

Clearly, for all $p \neq 2,3,5$ the kernel of the Rost invariant of a split group of type E_8 is trivial modulo p because every torsor over K of type E_8 can be killed by a finite extension of K of degree dividing $2^6 3^2 5$ by [To] (for a simpler proof see also [Ch06]). If $p = 5$ then the main result in [Ch94] says that the kernel of the Rost invariant for E_8 modulo 5 is trivial. The aim of the paper is to consider the next case $p = 3$.

Theorem 1.1. *Let F be a field of characteristic $\neq 3$ and let G_0 be the split group of type E_8 over F. Then the kernel of the Rost invariant for G_0 is trivial modulo* 3.

2 Notation and Auxiliary Results

If F is a field we denote by F^s a separable closure of F. Let G be a reductive algebraic group defined over F and let $T \subset G$ be a maximal torus over F. We denote by $\Sigma = \Sigma(G,T)$ the corresponding root system and by W_Σ the corresponding Weyl group. For a prime number p we let $W_\Sigma(p)$ denote a p-Sylow subgroup of W_Σ. If Σ has type X (in the paper we consider mainly types $X = A_2, E_6, E_8$) we also write W_X (respectively $W_X(p)$) instead of W_Σ (respectively $W_\Sigma(p)$).

Note that $\mathrm{Gal}\,(L/F)$, where L/F is a minimal splitting extension of T has a natural embedding into the automorphism group $\mathrm{Aut}\,\Sigma$ of Σ. If G is a group of inner type, for example of type E_8, then the image of $\mathrm{Gal}\,(L/F)$ is contained in the Weyl group $W_\Sigma \subset \mathrm{Aut}\,(\Sigma)$.

If $\Sigma_1 \subset \Sigma$ is a root subsystem we denote by $G_{\Sigma_1} \subset G$ the subgroup generated by unipotent root subgroups $U_{\pm\alpha} \subset G$ for all roots $\alpha \in \Sigma_1$. Note that G_{Σ_1} is not necessarily defined over the ground field F because Σ_1 is not necessarily stable by $\mathrm{Gal}\,(L/F)$.

We say that an F-defined subgroup $H \subset G$ is standard if there exists a maximal torus $T \subset G$ defined over F and a root subsystem $\Sigma_1 \subset \Sigma(G,T)$ such that $H = G_{\Sigma_1}$. Note that in this case T normalizes H.

2.1 Split Groups

Assume, additionally, that G is a simple simply connected group split over F and that $T \subset G$ is a split maximal torus. Let $\mathfrak{g}$ be the Lie algebra of G. A choice of Borel subgroup $B \subset G$ containing T determines an ordering of Σ, hence the system of simple roots $\Pi = \{\alpha_1, \dots, \alpha_n\}$. Let Σ^+ (respectively Σ^-) be the set of positive (respectively negative) roots and let B^- be the Borel subgroup opposite to B with respect to T. We pick a Chevalley basis [St67]

$$\{H_{\alpha_1}, \dots, H_{\alpha_n}, X_\alpha, \alpha \in \Sigma\}$$

in $\mathfrak{g}$ corresponding to the pair (T, B). This basis is unique up to signs and automorphisms of $\mathfrak{g}$ which preserve B and T (see [St67], Sect. 1, Remark 1).

Let $\widehat{T}$ and T_* denote the corresponding group of characters and cocharacters of T. There exists a natural pairing $T_* \times \widehat{T} \to \mathbb{Z}$. We may view the root system Σ as a subset in $\widehat{T}$. For each root $\alpha \in \Sigma$ Steinberg in his book [St67] associates the cocharacter in T_* denoted by h_α. Thus, h_α is a homomorphism $h_\alpha : G_m \to T$. For instance, if $G = \mathrm{SL}_n$ and $\alpha = \varepsilon_i - \varepsilon_j$ then $h_\alpha(t)$ is a diagonal matrix with t in the ith column and t^{-1} in the jth. The image of h_α coincides with $T_\alpha = T \cap G_\alpha$. If all roots in Σ have the same length then for every sum $\alpha = \beta + \gamma$, where α, β, and γ are roots we have $h_\alpha = h_\beta h_\gamma$.

As G is a simply connected group, the following relations hold in G (cf. [St67], Lemma 28 b), Lemma 20 c)):

(A) $T = T_{\alpha_1} \times \cdots \times T_{\alpha_n}$; hence T_* is generated by $h_{\alpha_1}, \dots, h_{\alpha_n}$.
(B) For any two roots $\alpha, \beta \in \Sigma$ we have

$$h_\alpha(t)\, X_\beta\, h_\alpha(t)^{-1} = t^{\langle \beta, \alpha \rangle} X_\beta,$$

where $\langle \beta, \alpha \rangle = 2(\beta, \alpha)/(\alpha, \alpha)$.

If $\Delta \subset \Pi$, we let G_Δ denote the subgroup generated by $U_{\pm\alpha}$, $\alpha \in \Delta$.

2.2 Steinberg's Theorem

We state now two theorems which are due to Steinberg [St65]. Although they are not formulated explicitly in [St65], their proofs can be easily obtained from the arguments contained in [St65], Sect. 10 (see also [PR, Propositions 6.18, 6.19, p. 338–339] and [Ch03, Theorems 3.1, 3.2]).

Let G_0 be a simple (not necessary simply connected) linear algebraic group split or quasi-split over F. Let $\xi \in Z^1(F, G_0)$ be a cocycle and let $G = {}^{\xi}G_0$ be the corresponding twisted group.

Theorem 2.1. *For any maximal torus $S \subset G$ over F there is an F-embedding $S \hookrightarrow G_0$ such that the class $[\xi]$ lies in the image of $H^1(F, S) \to H^1(F, G_0)$.*

Theorem 2.2. *In the notation earlier assume that G_0 is a simple simply connected group split over F and that G is isotropic over F. Then ξ is equivalent to a cocycle with coefficients in a proper semisimple simply connected F-split subgroup H_0 in G_0 which is standard and isomorphic over F^{s} to a semisimple anisotropic kernel of G.*

As a simple corollary of these two results we have the following:

Proposition 2.3. *In the earlier notation let $T_0 \subset G_0$ be a maximal F-split torus. If $S \subset G$ is a maximal torus over F with a minimal splitting extension L/F then ξ is equivalent to cocycle in $Z^1(L/F, N_{G_0}(T_0)(L))$.*

Proof. Let $i\colon S \hookrightarrow G_0$ be an embedding given by Theorem 2.1. Passing to an equivalent cocycle we may assume that $\xi = (a_\sigma)$ takes values in $i(S)$. As S is L-split we may additionally assume that $\xi \in Z^1(L/F, i(S)(L))$. We remind the reader that any two maximal L-split tori in G_0 are conjugate by an element in $G_0(L)$. Hence there exists $a \in G_0(L)$ such that $ai(S)a^{-1} = T_0$. As $i(S)$ and T_0 are F-defined, it is easy to see that $a^{-\sigma}a \in N_{G_0}(i(S))(L)$ for every $\sigma \in \mathrm{Gal}\,(F^s/F)$. Consider an equivalent cocycle $\xi' = (aa_\sigma a^{-\sigma}) \in Z^1(L/F, G_0(L))$. It takes values in

$$a(i(S)(L)a^{-\sigma}a)a^{-1} \subset aN_{G_0}(i(S))(L)a^{-1} = N_{G_0}(T_0)(L)$$

as required. □

3 The Rost Invariant and its Properties

In this section for later use we state (without proofs) two properties of the Rost invariant. For proofs we refer to [KMRT] (Sect. 31), [GMS]. We note that an explicit formula for $\mathscr{R}_G$ is known in a few cases only.

3.1 *Inner Type* A_{p-1}

Let A be a central simple algebra over F of degree p, where p is prime and let $G = \mathbf{SL}(1, A)$. One has:

$$H^1(F, G) = F^\times / \mathrm{Nrd}\,(A^\times).$$

Assume that $\mathrm{char}(F) \neq p$. Then the formula for the Rost invariant $\mathscr{R}_G$ is given (up to a sign) by

$$\mathscr{R}_G\colon F^\times/\mathrm{Nrd}\,(A^\times) \longrightarrow H^3(F, \mu_p^{\otimes 2}), \quad \mathscr{R}_G\,(x\mathrm{Nrd}\,(A^\times)) = (x) \cup [A].$$

In particular, we have the following:

Proposition 3.1. *In the earlier notation one has* $\mathrm{Ker}\,\mathscr{R}_{G,F} = 1$.

Indeed, this follows immediately from

Theorem 3.2. ([MS], Theorem 12.2) *If A is a central simple algebra over F of prime degree p, and p is different from the characteristic of F, then $(x) \cup [A] = 0$ if and only if $x \in \mathrm{Nrd}A^\times$.*

3.2 The Rost Multipliers

Let G, H be almost simple simply connected linear algebraic groups over F and let $\rho : H \hookrightarrow G$ be an F-embedding. The restriction $\mathscr{R}_G$ at $\rho(H)$ gives a cohomological invariant of H, hence is equal to $n_\rho \mathscr{R}_H$ for a positive integer n_ρ (see [KMRT], Sect. 31). The smallest such integer is called the Rost multiplier of the embedding ρ.

Proposition 3.3. *Let $\rho : H \hookrightarrow G$ be an F-embedding such that $\rho(H)$ is a standard subgroup normalized by a maximal torus T. Assume that all roots in $\Sigma = \Sigma(G,T)$ have the same length. Then $n_\rho = 1$; in particular, for every field extension K/F and every class $[\xi] \in H^1(K,H)$ one has $\mathscr{R}_G(\rho([\xi])) = \mathscr{R}_H([\xi])$.*

Proof. Let $\Sigma_1 \subset \Sigma(G,T)$ be a subsystem such that $\rho(H) = G_{\Sigma_1}$. Let S be the connected component of $T \cap \rho(H)$. Clearly S is a maximal torus in $\rho(H)$ and there is a natural embedding of the root systems

$$\Sigma(\rho(H), S) \hookrightarrow \Sigma(G,T).$$

Hence the coroots of $\rho(H)$ are also the coroots of G (we used the fact that all roots of the root system $\Sigma = \Sigma(G,T)$ have the same length). The rest of the proof follows from [GMS, Proposition 7.9, p. 122]. $\square$

4 Reduction to Special Cocycles

In what follows we assume $\operatorname{char}(F) \neq 3$ and G_0 is the split group of type E_8 over F. Let $T_0 \subset G_0$ be a maximal split torus over F. For the proof of Theorem 1.1 we may assume without loss of generality that F has no finite extension of degree prime to 3. In particular, this implies that F is perfect (because $\operatorname{char} F \neq 3$) and F contains a primitive cube root of unity.

Now consider a cocycle $\xi \in Z^1(F, G_0)$ that is in the kernel of the Rost invariant $\mathscr{R}_{G_0,F}$. Take a finite extension L/F of minimal possible degree killing ξ. As F has no finite extensions of degree prime to 3 we have $[L:F] = 3^n$. Consider a chain

$$F = L_0 \subset L_1 \subset \cdots \subset L_n = L$$

of subfields such that L_i/L_{i-1} is a Galois extension of degree 3. To prove that ξ is trivial we apply induction on n. By induction ξ_{L_1} is trivial, hence up to equivalence $\xi \in Z^1(L_1/F, G_0(L_1))$. Thus, we may henceforth assume that ξ is killed by a Galois extension $L = L_1$ of F of degree 3. In what follows σ denotes a fixed generator of $\operatorname{Gal}(L/F)$.

We say that a cocycle $\eta \in Z^1(F, G_0)$ is *special* if the twisted group ${}^{\eta}G_0$ is F-anisotropic (in particular η is not trivial) and there exists a finite Galois extension L/F of degree 3 such that η is equivalent to a cocycle in $Z^1(L/F, N_{G_0}(T_0)(L))$. The proof of Theorem 1.1 consists in showing that

(a) If $[\xi] \neq 1$ then ξ is equivalent to a special cocycle; and
(b) The kernel of the Rost $\mathscr{R}_{G_0,F}$ invariant does not contain special cocycles.

Clearly (a) and (b) imply that $\operatorname{Ker}\mathscr{R}_{G_{0,F}} = 1$.

Let us start with (a). We first reduce to the anisotropic case.

Proposition 4.1. *Let $[\xi] \in \operatorname{Ker}\mathscr{R}_{G_0}$ and let $G = {}^{\xi}G_0$ be the twisted group. If G is F-isotropic then $[\xi] = 1$.*

Proof. Let H_0 be the subgroup in G_0 given by Theorem 2.2. We may assume that ξ takes values in H_0. Since H_0 is proper, rank of H_0 is at most 7. Note that H_0 is simply connected since so is G_0. By Proposition 3.3, we know that $\mathscr{R}_{H_0}([\xi]) = \mathscr{R}_{G_0}([\xi]) = 1$. Furthermore for all split or quasi-split F-groups of rank ≤ 7 the Rost invariant has trivial kernel by [Gar], hence $[\xi] = 1$. □

Thus, for the proof of Theorem 1.1 we may assume that ξ is F-anisotropic, i.e., the twisted group $G = {}^{\xi}G_0$ is F-anisotropic. To complete the reduction to special cocycles we need the following

Proposition 4.2. *Let $\theta \in Z^1(F, G_0)$ be a cocycle such that the twisted group ${}^{\theta}G_0$ is F-anisotropic and split over a cubic Galois extension L/F. Then $G = {}^{\theta}G_0$ contains a maximal F-torus $S \subset G$ which is split over L.*

Proof. We apply the same argument as in [Ch03], Proposition 5.2. Namely, let $P \subset G$ be a maximal parabolic subgroup over L corresponding to the root α_8. It has dimension 191. Now consider the connected component C of the intersection $\mathscr{P} \cap \sigma(\mathscr{P}) \cap \sigma^2(\mathscr{P})$. As F is perfect and G is F-anisotropic, C is a reductive group over F of dimension at least 77. Let $C^{(1)} = [C, C] = C_1 \cdots C_s$ be the decomposition of the semisimple part of C into an almost direct product of the simple components over F^s. It easily follows from $\dim C \geq 77$ that $C^{(1)}$ contains a simple component, say C_1, of type not A_n. As in [Ch03] we may additionally assume that C_1 is defined over F. Because F has no quadratic extensions, C_1 is not of type B_n, C_n, G_2. By a dimension argument, it also cannot be of type D_n or F_4. So only one of the following cases can occur.

Case: C_1 is of type E_7. From $C_1 \subset C \subset P$ we conclude that C_1 is the semisimple part of a Levi subgroup of P. In particular, $C_G(C_1)$ contains a 1-dimensional torus which is split over L (the center of the Levi subgroup). Thus, by dimension consideration $C_G(C_1)$ is an F-defined reductive group of rank 1. But any such group is split over F. This contradicts our assumption that G is F-anisotropic.

Case: C_1 is a group of type E_6. As earlier we find that $C_G(C_1)$ is a reductive group of rank 2 which is isotropic over L and hence split over L. By classification results, every such group contains a maximal torus, say S_1, defined over F and splitting over L. Now consider the reductive group $C_G(S_1)$. Its semisimple part has rank at most 6 and contains C_1. Hence its semisimple part is precisely C_1. As S_1 is split over L so is C_1. By [Ch03], C_1 contains a maximal F-defined torus S_2 splitting over L. Then the torus $S = S_1 \cdot S_2$ is maximal and splits over L. □

Propositions 2.3 and 4.2 complete the proof of (a).

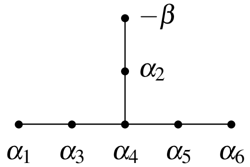
To prove (b), we assume the contrary. We fix a cocycle $\xi \in Z^1(L/F, N_{G_0}(T_0)(L))$ that is special and in the kernel of $\mathscr{R}_{G_0}$. In the next sections we construct cocycles $\xi = \xi_0, \xi_1, \xi_2, \xi_3$ such that ξ_i is equivalent to ξ_{i-1} for every $i = 1,2,3$ and ξ_3 takes values in a standard simply connected subgroup $H \subset G_0$ of inner type A_2. This will contradict our assumption that ξ is in the kernel of the Rost invariant because, by Proposition 3.3, $\mathscr{R}_H([\xi_3]) = \mathscr{R}_{G_0}([\xi_3])$ and by Proposition 3.1 the kernel of the Rost invariant of H is trivial.

Remark 4.3. We will construct ξ_3 explicitly and this will provide us with an explicit formula for the Rost invariant for all special cocycles.

For the construction of ξ_1 and ξ_2 we need information about 3-Sylow subgroups in W_{E_8} and about descent data for groups of the form $\mathbf{SL}(1,A)$ where A is a central simple algebra over F of degree 3.

5 3-Sylow Subgroups of the Weyl Group W_{E_8}

We first recall an explicit description of a 3-Sylow subgroup of the Weyl group W_{E_6}. For the proof we refer to [Ch03]. Let Σ_{E_6} be a root system of type E_6. Fix a basis $\Pi = \{\alpha_1, \dots, \alpha_6\}$ of Σ_{E_6} and denote by β the highest root. The extended Dynkin diagram of type E_6 is of the form



It follows from the picture that Σ_{E_6} contains a root subsystem Σ_1 of type $A_2 \times A_2 \times A_2$ generated by roots $\{\alpha_1, \alpha_3\}$, $\{\alpha_5, \alpha_6\}$, and $\{\alpha_2, -\beta\}$. Since the Weyl group W_{A_2} of type A_2 is isomorphic to S_3 it contains a unique 3-Sylow subgroup which is cyclic of order 3. Let v_1, v_2, v_3 be elements in $W_{\Sigma_1} \simeq S_3 \times S_3 \times S_3$ given by:

$$\alpha_3 \xrightarrow{v_1} \alpha_1 \xrightarrow{v_1} -(\alpha_1+\alpha_3) \xrightarrow{v_1} \alpha_3, \quad \alpha_5 \xrightarrow{v_2} \alpha_6 \xrightarrow{v_2} -(\alpha_5+\alpha_6) \xrightarrow{v_1} \alpha_5,$$
$$\text{and} \quad -\beta \xrightarrow{v_3} \alpha_2 \xrightarrow{v_3} \beta - \alpha_2 \xrightarrow{v_3} -\beta. \tag{5.1}$$

It is known that W_{E_6} contains an element v of order 3 permuting v_1, v_2, v_3. Hence, the subgroup in W_{E_6} generated by v_1, v_2, v_3, v has order 3^4. Since $W_{E_6}(3)$ has the same order we obtain

Lemma 5.2. *One has* $W_{E_6}(3) \simeq (\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes \mathbb{Z}/3.$

Later on we shall also need the description of the intersection

$$C = (G_{\{-\beta,\alpha_2\}} \times G_{\{\alpha_5,\alpha_6\}}) \cap G_{\{\alpha_1,\alpha_3\}}.$$

It is a central subgroup of order 3 of the following shape. It is easy to see that the images of the embeddings

$$\mu_3 \to G_{\{-\beta,\alpha_2\}}, \ \ x \to h_{-\beta}(x)\, h_{\alpha_2}(x^2)$$

and

$$\mu_3 \to G_{\{\alpha_5,\alpha_6\}}, \ \ x \to h_{\alpha_5}(x)\, h_{\alpha_6}(x^2)$$

are the centers of the groups in question.

Lemma 5.3. *The image of* $\varphi\colon \mu_3 \to G_{\{-\beta,\alpha_2\}} \times G_{\{\alpha_5,\alpha_6\}}$ *given by* $x \to (x, x^2)$, *i.e.,*

$$x \to h_{-\beta}(x) h_{\alpha_2}(x^2) h_{\alpha_5}(x^2) h_{\alpha_6}(x)$$

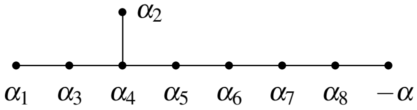
is contained in $G_{\{\alpha_1,\alpha_3\}}$ *and hence coincides with* C.

Proof. Using relation (B) in Sect. 2.1 it is straightforward to check that

$$\varphi(x) = h_{-\beta}(x) h_{\alpha_2}(x^2) h_{\alpha_5}(x^2) h_{\alpha_6}(x) = h_{\alpha_1}(x^2) h_{\alpha_3}(x),$$

so the result follows. $\square$

Now consider the root system Σ_{E_8} of type E_8. Let us fix its basis $\alpha_1,\dots,\alpha_8$. The extended Dynkin diagram is of the form



Here α is the highest root. From the picture we conclude that Σ_{E_8} contains a root subsystem Σ_2 of type $E_6 \times A_2$ generated by roots $\{\alpha_1,\dots,\alpha_6\}$ and $\{\alpha_8, -\alpha\}$. Recall that the order of a 3-Sylow subgroup $W_{E_8}(3)$ is 3^5. As $W_{\Sigma_2}(3) = W_{E_6}(3) \times W_{A_2}(3)$ has the same order we obtain

Lemma 5.4. *One has*

$$W_{E_8}(3) \simeq W_{E_6}(3) \times \mathbb{Z}/3 \simeq ((\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes \mathbb{Z}/3) \times \mathbb{Z}/3.$$

Finally, we describe a 3-Sylow subgroup of W_{E_8}. Consider the Weyl group W_{A_2} corresponding to the roots $\alpha_8, -\alpha$. Let $v_4 \in W_{A_2} \simeq S_3$ be the element given by:

$$\alpha_8 \xrightarrow{v_4} -\alpha \xrightarrow{v_4} \alpha - \alpha_8 \xrightarrow{v_4} \alpha_8, \tag{5.5}$$

From the earlier argument we know that the subgroup in W_{E_8} generated by v_1, v_2, v_3, v_4 and v is a 3-Sylow subgroup of W_{E_8}. We will call it a *standard* 3-*Sylow subgroup*.

6 Galois Descent Data for Groups of Type A_2

In this section F denotes an arbitrary field of characteristic $\neq 3$ containing a primitive cube root of unity ζ_3. Let A be a central simple algebra over F of degree 3 and let $G = \mathbf{SL}(1,A)$. Clearly G is an inner form of type A_2. We denote its Lie algebra by $\mathfrak{g}$: it consists of all elements in A with reduced trace zero.

One knows that A is a cyclic algebra, hence it is cyclic of the form $A = (a,b)_{\zeta_3}$ for some elements $a,b \in F^\times$, as defined in [GS, p. 36]. Let $L = F(\sqrt[3]{a})$ be a maximal subfield in A corresponding to a and let $T = R^{(1)}_{L/F}(G_m)$ be the maximal torus in G consisting of all elements in L with norm 1. It is defined over F and split over L.

We have $\mathrm{Gal}\,(L/F) = \mathbb{Z}/3$ and there is a natural embedding of $\mathrm{Gal}\,(L/F)$ into the Weyl group $W_{A_2} = S_3$. We identify $\mathrm{Gal}\,(L/F)$ with its image in W_{A_2}. We may assume that the presentation $A = (a,b)$ corresponds to a generator $\sigma \in \mathrm{Gal}\,(L/F)$ which is equal to the cycle (123) (under the identification $W_{A_2} = S_3$).

As $L \subset A$ we may identify $A_L = A \otimes_F L = M_3(L)$ in such a way that T_L corresponds to the set of diagonal matrices in $M_3(L)$. We choose the standard basis in the root system $\Sigma(G_L, T_L)$ of type A_2 and the standard Chevalley basis

$$\{H_{\alpha_1}, H_{\alpha_2}, X_{\pm\alpha_1}, X_{\pm\alpha_2}, X_{\pm(\alpha_1+\alpha_2)}\}$$

in $\mathfrak{g}_L = \mathfrak{g} \otimes_F L$. Recall that

$$X_{\alpha_1} = \begin{pmatrix} 0&1&0\\0&0&0\\0&0&0 \end{pmatrix}, \quad X_{\alpha_2} = \begin{pmatrix} 0&0&0\\0&0&1\\0&0&0 \end{pmatrix}, \quad \text{and} \quad X_{-(\alpha_1+\alpha_2)} = \begin{pmatrix} 0&0&0\\0&0&0\\1&0&0 \end{pmatrix}.$$

The algebra A viewed as a subalgebra in $A_L = M_3(L)$ is the invariant subset $A = M_3(L)^{\mathrm{Gal}\,(L/F)}$ where $\mathrm{Gal}\,(L/F)$ acts on $A_L = A \otimes_F L$ through the second factor. Because $\sigma = (123)$, it takes α_1 into α_2 and α_2 into $-(\alpha_1+\alpha_2)$, hence we have

$$X_{\alpha_1} \xrightarrow{\sigma} c_1 X_{\alpha_2} \xrightarrow{\sigma} c_2 X_{-(\alpha_1+\alpha_2)}$$

for some elements $c_1, c_2 \in L^\times$. We call them *structure constants* of G with respect to T.

Clearly $j = X_{\alpha_1} + c_1 X_{\alpha_2} + c_2 X_{-(\alpha_1+\alpha_2)}$ is invariant with respect to σ, hence $j \in A$. It is routine to check that $j^3 = c_1 c_2$ implying $c_1 c_2 \in F^\times$ (because j is Galois invariant). It is also straightforward to check that the conjugation by j on the set of diagonal matrices corresponds to the cycle (132), hence its restriction at $T(F)$ corresponds to σ^2 (note that we identified $A_L = M_3(L)$ in such a way that $T(F)$ is the Galois invariant subset of the set of all diagonal matrices with determinant 1).

It follows from the above argument that up to norms in $N_{L/F}(L^\times)$ we have $c_1 c_2 \equiv b^{-1} \equiv b^2$. In particular, we can restore the presentation $A = (a,b)$ if we know the Galois extension $L = F(\sqrt[3]{a})$ splitting a maximal torus $T \subset G$ and the structure constants c_1, c_2.

Lemma 6.1. *If $c_1c_2 \in (F^\times)^3$ then A is split.*

Proof. Indeed, we have $b = c^3$ for some $c \in F^\times$, so the result follows. □

Finally, for later use we want to describe explicitly cocycles with coefficients in T, i.e., the group $Z^1(L/F,T(L))$, in terms of standard generators of a Chevalley group $G_L = \mathrm{SL}_3$. As $\mathrm{Gal}\,(L/F) = \langle\sigma\rangle$ is cyclic every cocycle $\eta = (a_\tau) \in Z^1(L/F,T(L))$ is determined uniquely by an element $a_\sigma = h_{\alpha_1}(u)h_{\alpha_2}(v) \in T(L)$ satisfying the relation

$$a_\sigma \cdot \sigma(a_\sigma) \cdot \sigma^2(a_\sigma) = 1.$$

Lemma 6.2. *Let $u,v \in L^\times$. Then $a_\sigma = h_{\alpha_1}(u)h_{\alpha_2}(v)$ determines a cocycle if and only if $v\sigma(u) \in F^\times$.*

Proof. We know that σ acts on the character lattice $\widehat{T} = \langle\alpha_1,\alpha_2\rangle$ of T by $\sigma(\alpha_1) = \alpha_2$ and $\sigma(\alpha_2) = -\alpha_1 - \alpha_2$. Since $h_{\alpha_i} : G_m \to T$ is the cocharacter corresponding to α_i and since all roots have the same length we also have $\sigma(h_{\alpha_1}) = h_{\alpha_2}$ and $\sigma(h_{\alpha_2}) = h_{-\alpha_1-\alpha_2} = -h_{\alpha_1} - h_{\alpha_2}$. It is now routine to check that a_σ satisfies the equation $a_\sigma\sigma(a_\sigma)\sigma^2(a_\sigma) = 1$ if and only if $v\sigma(u) \in F^\times$. □

Corollary 6.3. *Every cocycle $(a_\sigma) \in Z^1(L/F,T(L))$ is equivalent to a cocycle of the form (b_σ), where $b_\sigma = h_{\alpha_1}(w)$ and $w \in F^\times$.*

Proof. Let $a_\sigma = h_{\alpha_1}(u)h_{\alpha_2}(v)$. It is easy to check that for an arbitrary element y in $L^\times$ a trivial cocycle $(h_{\alpha_1}(y)^{1-\sigma})$ is of the form $(h_{\alpha_1}(y)h_{\alpha_2}(\sigma(y)^{-1}))$. Hence taking $y = \sigma^2(v)$ we get that the cocycle (b_σ) where

$$b_\sigma = h_{\alpha_1}(y)h_{\alpha_1}(u)h_{\alpha_2}(v)h_{\alpha_1}(y)^{-\sigma}$$

is equivalent to (a_σ) and it is of the required form. □

7 Construction of ξ_1

In this section we keep the notation (introduced in Sect. 5) v_1,v_2,v_3,v_4,v for elements in the Weyl group W_{E_8} given by (5.1) and (5.5) and α, β for the highest roots in root systems of types E_8 and E_6. Recall that we assume ξ is special, i.e., $\xi \in Z^1(L/F,N_{G_0}(T_0))$ where L/F is a Galois extension of degree 3 and the twisted group $G = {}^\xi G_0$ is F-anisotropic. We denote by σ a generator of $\mathrm{Gal}\,(L/F)$ and by $\Sigma = \Sigma(G_0,T_0)$ the root system of G_0 with respect to T_0 with a basis $\alpha_1,\ldots,\alpha_8$.

A mapping $N_{G_0}(T_0) \to W_{E_8}$ induces

$$H^1(L/F,N_{G_0}(T_0)(L)) \to H^1(L/F,W_{E_8}) = \mathrm{Hom}(\mathrm{Gal}(L/F),W_{E_8})/\sim,$$

where $\sim$ is an equivalence relation given by conjugation. The map $N_{G_0}(T_0)(L) \to W_{E_8} = W_{E_8}(L)$ is surjective. So passing to an equivalent cocycle, if necessary, we may assume that the image $\overline{\xi}$ of ξ corresponds to a mapping $\overline{\xi} : \mathrm{Gal}\,(L/F) \to W_{E_8}$

whose image in W_{E_8} is contained in a standard 3-Sylow subgroup generated by v_1,v_2,v_3,v_4,v. It then follows that the standard subgroup $H_0 \subset G_0$ of type E_6 generated by roots $\alpha_1,\dots,\alpha_6$ is invariant with respect to twisting by ξ (because it is invariant with respect to conjugation by v_1,v_2,v_3,v_4,v).

Note that the twisted group ${}^{\xi}H_0$ is F-anisotropic because so is $G={}^{\xi}G_0$. Then, by [Ch03] Lemma 5.9, $\overline{\xi}(\sigma)$ is an element of order 3 in the subgroup generated by v_1,v_2,v_3,v_4, hence it is of the form $v_1^{\varepsilon_1}\cdots v_4^{\varepsilon_4}$, where $\varepsilon_i=0,1,2$. Furthermore, $\varepsilon_i\neq 0$ since otherwise G would be F-isotropic. Clearly v_i and v_i^2 are conjugate in W_{E_8}, hence up to equivalence we may assume that $\overline{\xi}(\sigma)=v_1\cdots v_4$. In other words, $\overline{\xi}$ viewed as a cocycle in $Z^1(L/F,W_{E_8})$ can be written (up to equivalence) in the form $\overline{\xi}=(\overline{a}_\sigma)$, where $\overline{a}_\sigma=v_1v_2v_3v_4$.

The root subsystem of Σ' generated by $\alpha_1,\alpha_3,\alpha_2,\beta,\alpha_5,\alpha_6,\alpha_8,\alpha$ has type $A_2\times A_2\times A_2\times A_2$ and this gives rise to a group $P=\mathrm{SL}_3\times\mathrm{SL}_3\times\mathrm{SL}_3\times\mathrm{SL}_3$ and a multiplication mapping $\varphi\colon P\to G_0$. Let $T_0'=\varphi^{-1}(T_0)$. It is a maximal F-split torus in P. Let $N'=N_P(T_0')$ and $W'=N'/T_0'$. We have a canonical mapping $N'\to W'\hookrightarrow W_{E_8}$. Let $u_1,u_2,u_3,u_4\in N'$ be standard liftings of v_1,v_2,v_3,v_4 represented by matrices

$$\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}.$$

Consider a cocycle $\eta'=(a_\sigma)\in Z^1(L/F,N'(L))$ where $a_\sigma=u_1u_2u_3u_4$ and its image η in $Z^1(L/F,N_{G_0}(T_0))$. As η' is trivial so is η. Twisting G_0 by η gives rise to a canonical bijection $\lambda: H^1(F,G_0)\to H^1(F,{}^{\eta}G_0)$ (see [Se]). As by construction ξ and η have the same image under $H^1(L/F,N_{G_0}(T_0)(L))\to H^1(L/F,W_{E_8})$, the image $\xi_1=\lambda(\xi)$ takes values in the twisted torus $S_1={}^{\eta}T_0$. Note that because η is trivial we may identify ${}^{\eta}G_0=G_0$ and this allows us to view S_1 as a maximal F-anisotropic torus in G_0 splitting by L.

We have thus proved that there is a maximal F-defined torus $S_1\subset G_0$ splitting over L such that ξ is equivalent to a cocycle ξ_1 with coefficients in S_1. By our construction S_1 being the image of ${}^{\eta'}(T_0')$ under φ is an almost direct product of four copies of $C=R^{(1)}_{L/F}(G_{m,L})$. In the next two sections we will describe the action of $\mathrm{Gal}\,(L/F)$ on the characters $\widehat{S_1}$ and cocharacters $(S_1)_*$ of S_1 and this will allow us to decompose S_1 as the direct product of four copies of C. This in turn immediately gives us a decomposition of ξ_1 as a product of four cocycles each of which, as we shall see, can be viewed as a cocycle in SL_3. The last property eventually will lead us to the proof of (b).

8 The Direct Product Decomposition of S_1

We keep the above notation. In particular, we deal with the maximal torus $S_1\subset G_0$ and the cocycle $\xi_1\in Z^1(L/F,S_1(L))$ constructed in the previous section. Let $\Sigma_1=\Sigma(G_0,S_1)$. Abusing notation we still denote its basis by $\alpha_1,\dots,\alpha_8$. As we saw earlier S_1 is F-anisotropic and hence the lattice $\widehat{S_1}$ contains no F-defined characters. This implies in turn that for every root $\alpha \in \Sigma_1$ we have $\alpha + \sigma(\alpha) + \sigma^2(\alpha) = 0$. Thus the σ-orbit

$$o(\alpha) = \{\,\alpha,\, \sigma(\alpha),\, \sigma^2(\alpha)\,\} \subset \Sigma_1$$

of α generates a root subsystem $\Sigma_{o(\alpha)} \subset \Sigma_1$ of rank at most 2. Because σ is an automorphism of $\Sigma_{o(\alpha)}$ of order 3 it immediately follows that $\Sigma_{o(\alpha)}$ is a root system of type A_2 with basis α, $\sigma(\alpha)$.

As usual we denote by:

$$\{\,H_{\alpha_1}, \ldots, H_{\alpha_8}, X_\alpha,\, \alpha \in \Sigma_1\,\}$$

a Chevalley basis of the Lie algebra $\mathfrak{g}_L$ of G_0 with respect to S_1.

Lemma 8.1. *Let $G_{o(\alpha)} \subset G_0$ be a standard subgroup corresponding to $\Sigma_{o(\alpha)}$. Then $G_{o(\alpha)} \simeq \mathrm{SL}_3$.*

Proof. We know that $G_{o(\alpha)}$ is a simple simply connected subgroup over F of type A_2. Hence it is of the form $\mathrm{SL}(1,A)$ where A is a central simple algebra over F of degree 3 and we need only to show that A is split.

Recall that the action of $\sigma \in \mathrm{Gal}\,(L/F)$ on the roots in Σ_1 is given by $v_1v_2v_3v_4 \in W_{E_8}$ and that the twisted action (by means of η) of σ on ${}^{\eta}G_0 = G_0$ and its Lie algebra is given by conjugation with the standard lifting $u_1u_2u_3u_4$ of $v_1v_2v_3v_4$ (see the above construction of η). It follows that σ acts via

$$X_\alpha \xrightarrow{\sigma} \varepsilon_1 X_{\sigma(\alpha)} \xrightarrow{\sigma} \varepsilon_2 X_{\sigma^2(\alpha)} = \varepsilon_2 X_{-\alpha-\sigma(\alpha)} \tag{8.2}$$

where $\varepsilon_1, \varepsilon_2 = \pm 1$. Thus the structure constants c_1, c_2 of A are ± 1. Because $-1 = (-1)^3$ is a cube, we are done by Lemma 6.1. □

The explicit action of $\sigma \in \mathrm{Gal}\,(L/F)$ on the roots α_1, α_2, α_3, α_5, α_6, α_8 is given by formulas (5.1) and (5.5). Let us describe its action on the remaining two simple roots α_4 and α_7.

Lemma 8.3. *One has*

$$\sigma(\alpha_4) = -\alpha_1 - \alpha_3 - \alpha_2 - 2\alpha_4 - \alpha_5 - \alpha_6$$

and

$$\sigma(\alpha_7) = \alpha_1 + 2\alpha_3 + 2\alpha_2 + 3\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7 + \alpha_8.$$

Proof. We know that $\sigma(\beta) = -\alpha_2$ and that $\beta = \alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6$. It follows that

$$\sigma(\alpha_1) + 2\sigma(\alpha_2) + 2\sigma(\alpha_3) + 3\sigma(\alpha_4) + 2\sigma(\alpha_5) + \sigma(\alpha_6) = -\alpha_2.$$

Substituting

$$\sigma(\alpha_1) = -\alpha_1 - \alpha_3, \quad \sigma(\alpha_3) = \alpha_1, \quad \sigma(\alpha_5) = \alpha_6,$$
$$\sigma(\alpha_6) = -\alpha_5 - \alpha_6, \quad \text{and} \quad \sigma(\alpha_2) = \beta - \alpha_2,$$

we easily get the result.

The argument for α_7 is similar. □

If $\alpha \in \Sigma$ is a root we set $S_{1,o(\alpha)} = G_{o(\alpha)} \cap S_1$. It is an F-defined maximal torus in $G_{o(\alpha)}$ isomorphic to $R^{(1)}_{L/F}(G_m)$.

Proposition 8.4. *The multiplication mapping*

$$S_{1,o(\alpha_4)} \times S_{1,o(\alpha_7+\alpha_6)} \times S_{1,o(\alpha_5)} \times S_{1,o(\alpha_2)} \longrightarrow S_1$$

is an F-isomorphism.

Proof. It is straightforward to check that

$$h_{\alpha_4}, h_{\sigma(\alpha_4)}, h_{\alpha_7+\alpha_6}, h_{\sigma(\alpha_7+\alpha_6)}, h_{\alpha_2}, h_{\sigma(\alpha_2)}, h_{\alpha_5}, h_{\sigma(\alpha_5)},$$

is a basis of the cocharacter lattice $(S_1)_*$ of S_1, so the result follows. □

9 Construction of ξ_2

We start with the following general formalism. Let G be an algebraic group (not necessary split) over F and let $S \subset G$ be a maximal F-torus splitting over a finite Galois extension L/F. Assume that we are given two cocycles $\eta_1 = (a_\sigma)$ and $\eta_2 = (b_\sigma)$ with coefficients in $S(L)$ such that η_2 viewed in $Z^1(L/F, G(L))$ is trivial, say $b_\sigma = g^{1-\sigma}$ for some element $g \in G(L)$.

Let now $\eta = \eta_1\eta_2$. As η_1, η_2 take values in a commutative group $S(L)$, η is a cocycle. Consider an inner conjugation $int(g)\colon G \to G$ given by $x \to g^{-1}xg$. We claim that the torus $S_1 = g^{-1}Sg$ is an F-defined maximal torus in G and the restriction of $int(g)$ to S is an F-defined isomorphism $S \to S_1$. Indeed, if $s \in S(L)$ then we have

$$\sigma(g^{-1}sg) = g^{-1}(g\sigma(g^{-1})\sigma(s)\sigma(g)g^{-1})g = g\sigma(s)g^{-1}.$$

(We used the fact that $g^{1-\sigma} \in S(L)$ implies that $int(g)$ is L-defined on S.)

Now take the cocycle

$$\eta_1' = (g^{-1}a_\sigma b_\sigma g^\sigma) = g^{-1}a_\sigma g,$$

which is equivalent to η and takes values in S_1. We say that the passage from η to η_1' is an untwisting of η, and we call the torus S_1 and the cocycle η_1' the *syndrome* of S and η with respect to g.

Lastly we note that if η_1 takes values in a subtorus $S' \subset S$ which is a maximal torus in a standard subgroup $S' \subset H \subset G$ over F then the syndrome of η can be viewed as a cocycle with coefficients in an F-defined $H_1 = g^{-1}Hg$ subgroup in G which will be called a *syndrome* of H.

Remark 9.1. (1) The restriction of $int(g)$ at H is not necessarily F-defined and the syndrome H_1 of H is not necessary isomorphic to H over F.

(2) Even if both η_1, η_2 are trivial when viewed as cocycles in $Z^1(F,G)$, the cocycle η is not necessarily trivial in G.

We come back to our torus $S_1 \subset G_0$ and our cocycle $\xi_1 \in Z^1(L/F, S_1(L))$. By Proposition 8.4, we may write ξ_1 as a product of four cocycles, say $\xi_1 = \theta_1\theta_2\theta_3\theta_4$ with coefficients in

$$S_{1,o(\alpha_5)},\, S_{1,o(\alpha_2)},\, S_{1,o(\alpha_7+\alpha_6)} \text{ and } S_{1,o(\alpha_4)},$$

respectively.

Using Lemma 8.3 one easily checks that the roots in $o(\alpha_7+\alpha_6)$ and $o(\alpha_4)$ are orthogonal to each other, in particular $G_{o(\alpha_7+\alpha_6)}$ and $G_{o(\alpha_4)}$ are commuting subgroups in G_0 each of type A_2 and their intersection is trivial. Hence the cocycle $\eta_2 = \theta_3\theta_4$ can be viewed as a cocycle in $Z^1(L/F, G_{0,o(\alpha_7+\alpha_6)} \times G_{0,o(\alpha_4)})$.

By Corollary 6.3, θ_3 and θ_4 can be written in the form $\theta_3 = (a_\sigma)$, $\theta_4 = (b_\sigma)$ where $a_\sigma = h_{\alpha_7+\alpha_6}(u_3)$ and $b_\sigma = h_{\alpha_4}(u_4)$ for some parameters $u_3, u_4 \in F^\times$. By Lemma 8.1, $G_{o(\alpha_7+\alpha_6)} \times G_{o(\alpha_4)}$ is isomorphic to $\mathrm{SL}_3 \times \mathrm{SL}_3$. Hence there is $g \in (G_{0,o(\alpha_7+\alpha_6)} \times G_{0,o(\alpha_4)})(L)$ such that $\theta_3\theta_4 = (g^{1-\sigma})$. We now denote by ξ_2 the syndrome of ξ_1 with respect to g.

10 Construction of ξ_3 and proof of (b)

It follows from the construction that ξ_2 lives in a syndrome subgroup

$$\widetilde{G}_{\{\alpha_5,\alpha_6\}} \times \widetilde{G}_{\{-\beta,\alpha_2\}} = g^{-1}(G_{o(\alpha_5)} \times G_{o(\alpha_2)})g < G_0$$

of type $A_2 \times A_2$. Hence it is of the form:

$$\widetilde{G}_{\{\alpha_5,\alpha_6\}} \times \widetilde{G}_{\{-\beta,\alpha_2\}} = \mathrm{SL}(1,T_1) \times \mathrm{SL}(1,T_2)$$

for some central simple algebras T_1, T_2 of degree 3.

Lemma 10.1. *We have $T_1 \simeq T_2 \simeq (a, u_3u_4^2)$.*

Proof. The Lie algebra of $\widetilde{G}_{\{\alpha_5,\alpha_6\}}$ has a Chevalley basis

$$\{\widetilde{H}_{\alpha_5}, \widetilde{H}_{\alpha_6}, \pm\widetilde{X}_{\alpha_5}, \pm\widetilde{X}_{\alpha_6}, \pm\widetilde{X}_{\alpha_5+\alpha_6}\},$$

where

$$\widetilde{H}_{\alpha_5} = g^{-1}H_{\alpha_5}g, \quad \widetilde{H}_{\alpha_6} = g^{-1}H_{\alpha_6}g,$$

and

$$\widetilde{X}_{\alpha_5} = g^{-1}X_{\alpha_5}g, \quad \widetilde{X}_{\alpha_6} = g^{-1}X_{\alpha_6}g, \quad \widetilde{X}_{\alpha_5+\alpha_6} = g^{-1}H_{\alpha_5+\alpha_6}g.$$

It follows that the action of $\sigma \in \mathrm{Gal}(L/F)$ on $\widetilde{X}_{\alpha_5}, \widetilde{X}_{\alpha_6}$ is the composition of the old action given by (8.2) and the twisting action by $g^{1-\sigma} = h_{\alpha_7+\alpha_6}(u_3)h_{\alpha_4}(u_4)$. For instance,

$$\sigma(\widetilde{X}_{\alpha_5}) = g^{-1}(g^{1-\sigma}\varepsilon X_{\alpha_6} g^{\sigma-1})g = \varepsilon u_3 \widetilde{X}_{\alpha_6}$$

where $\varepsilon = \pm 1$. Computing the second structure constant of T_1 we see that $T_1 = (a, u_3u_4^2)$. The argument for T_2 is similar. □

Proof of (b) *from* §4: By the above lemma the cocycle ξ_2 lives in $\mathrm{SL}(1,T_1) \times \mathrm{SL}(1,T_1)$, hence it can be presented by a pair of elements

$$[(a_1,a_2)] \in F^\times/\mathrm{Nrd}\, T_1 \times F^\times/\mathrm{Nrd}\, T_1.$$

Since ξ_2 is in the kernel of the Rost invariant, by (3.1) and (3.2) we have

$$\mathscr{R}_{G_0}([\xi_2]) = a_1 \cup T_1 + a_2 \cup T_1 = 0.$$

This implies that up to multiplication by a reduced norm we may assume $a_2 = a_1^2$. It then follows that ξ_2 is equivalent to a cocycle ξ_3 with coefficients in the image of the map $\varphi\colon \mu_3 \to \widetilde{G}_{\{\alpha_5,\alpha_6\}} \times \widetilde{G}_{\{-\beta,\alpha_2\}}$, $x \to (x,x^2)$ in Lemma 5.3. But $\mathrm{Im}\,\varphi$ is contained in a subgroup $\widetilde{G}_{\{\alpha_1,\alpha_3\}}$ of type A_2 and we know by Prop. 3.1 that the kernel of the Rost invariant for $\widetilde{G}_{\{\alpha_1,\alpha_3\}}$ is trivial and that the Rost multiplier for our subgroup $\widetilde{G}_{\{\alpha_1,\alpha_3\}}$ is one. On the other hand ξ_3 is in the kernel and nontrivial – a contradiction that completes the proof of (b). □

Acknowledgements The author was partially supported by the Canada Research Chairs Program and an NSERC research grant.

References

[Ch94] V. Chernousov, Remark on (mod 5)–Serre's invariant for groups of type E_8, Math. Zametki, **56** (1994), no. 1, 116–121.

[Ch03] ———, The kernel of the Rost invariant, Serre's Conjecture II and the Hasse principle for quasi-split groups ${}^{3,6}D_4, E_6, E_7$, Math. Annalen **326** (2003), 297– 330.

[Ch06] ———, Another proof of Totaro's theorem on E_8-torsors, Can. Math. Bull **49** (2006), 196–202.

[Gar] R. S. Garibaldi, The Rost invariant has trivial kernel for quasi-split groups of low rank, Comment. Math. Helvetici **76** (2001), 684–711.

[GMS] S. Garibaldi, A. Merkurjev, and J.-P. Serre, Cohomological invariants in Galois cohomology, University Lecture Series, vol. 28, Amer. Math. Soc., 2003.

[GS] P. Gille, T. Szamuely, Central simple algebras and Galois cohomology, Cambridge studies in advanced mathematics, vol. 101, 2006.

[KMRT] M. Knus, A. Merkurjev, M. Rost, J–P. Tignol, The Book of Involutions, **44** Colloquium publications: American Mathematical Society 1998.

[MS] A. Merkurjev, A. Suslin, K-cohomology of Severi-Brauer varieties and the norm residue homomorphism, Izv. Akad. Nauk SSSR **46** (1982), 1011–1046.

[PR] V. Platonov, A. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, London 1994.

[Se] J.-P. Serre, *Galois Cohomology*, Springer, Berlin 1997.

[St65] R. Steinberg, Regular elements of semisimple groups, Publ. Math. I.H.E.S. **25** (1965), 281–312.

[St67] ______, Lectures on Chevalley Groups, Yale University 1967.

[To] B. Totaro, Splitting fields for E_8-torsors, Duke Math. J **121** (2004), 425–455.

Une version du théorème d'Amer et Brumer pour les zéro-cycles

Jean-Louis Colliot-Thélène et Marc Levine

À Parimala

Résumé (anglais). M. Amer and A. Brumer have shown that, for two homogeneous quadratic forms f and g over a field k, the locus $f = g = 0$ has a non-trivial solution over k if and only if, for a variable t, the equation $f + tg = 0$ has a non-trivial solution over $k(t)$. We consider a modified version of this result. We show that the projective variety over k defined by $f_0 = \cdots = f_r = 0$, where the f_i are homogeneous forms over k of the same degree $d \geq 2$ in $n+1$ variables (with $n+1 \geq r+2$), has a 0-cycle of degree 1 over k if and only if the generic hypersurface $f_0 + t_1 f_1 + \cdots + t_r f_r = 0$ has a 0-cycle of degree 1 over $k(t_1, \ldots, t_r)$.

1 Introduction

Soit k un corps. Soient f et g deux formes *quadratiques* à coefficients dans k, en $n+1$ variables. Soit t une variable. On sait que le système de formes $f = g = 0$ a un zéro non trivial sur k si et seulement si la forme quadratique $f + tg$ sur le corps $k(t)$ a un zéro non trivial (M. Amer [1], A. Brumer [2], voir [4, III, Prop. 17.14]).

Dans cette note, dont une version primitive fut conçue à Boston en avril 1991, nous montrons que si l'on considère les zéro-cycles de degré 1 plutôt que les points rationnels, il existe en *tout degré* $d \geq 2$ une version de ce résultat pour un système

Jean-Louis Colliot-Thélène
C.N.R.S., Mathématiques, Bâtiment 425, Université Paris-Sud, F-91405 Orsay, France
e-mail: jlct@math.u-psud.fr

Marc Levine
Department of Mathematics, Northeastern University, 360 Huntington Avenue, Boston, MA 02115, USA and Universität Duisburg-Essen Fakultät Mathematik, Campus Essen, D-45117 Essen, Germany; e-mail: marc.levine@uni-due.de

Classification thématique AMS. 14C25

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_12,

de deux formes de même degré d (Théorème 1), et des versions pour un système quelconque de formes de même degré d (Théorèmes 2 et 3).

Pour K/k une extension de corps et X un k-schéma, on note $X_K = X \times_k K$. Une variété algébrique sur un corps k est un k-schéma séparé de type fini.

2 Indice et indice réduit

Définition 1. Soient k un corps et X une k-variété algébrique. À tout point fermé $P \in X$, de corps résiduel $k(P)$ on associe son degré $[k(P) : k] \in \mathbb{N}$. L'indice $I(X/k)$ de la k-variété X est par définition le plus grand commun diviseur (pgcd) des degrés des points fermés. C'est aussi le pgcd des degrés $[L : k]$ des extensions finies de corps L/k avec $X(L) \neq \emptyset$.

De façon évidente, on a $I(X/k) = 1$ si et seulement si X possède un zéro-cycle (cycle de dimension zéro) $\sum_P n_P P$ (avec $n_P \in \mathbb{Z}$) de degré $\sum_P n_P [k(P) : k] = 1$. On appelle indice réduit de X/k, et on note $I_{\mathrm{red}}(X/k)$ le produit des nombres premiers qui divisent $I(X/k)$. De façon triviale, $I(X/k) = 1$ si et seulement si $I_{\mathrm{red}}(X/k) = 1$.

Lemme 1. *Soient k un corps et X une k-variété.*

(a) Si $X = Y \cup Z$ est la réunion ensembliste de deux sous-k-variétés, alors on a $I(X/k) = \mathrm{pgcd}(I(Y/k),\ I(Z/k))$. En particulier, l'indice de X/k est égal à l'indice de sa sous-k-variété réduite.
(b) Si $X = Y \cup Z$ est la réunion ensembliste de deux sous-k-variétés, alors on a $I_{\mathrm{red}}(X/k) = \mathrm{pgcd}(I_{\mathrm{red}}(Y/k),\ I_{\mathrm{red}}(Z/k))$.
(c) Si $K = k(t_1, \ldots, t_n)$ est une extension transcendante pure de k, alors on a $I(X/k) = I(X_K/K)$ et $I_{\mathrm{red}}(X/k) = I_{\mathrm{red}}(X_K/K)$.

Preuve. Seul le point (c) requiert une explication. Soit $K = k(t)$. Si L/k est une extension finie de corps avec $X(L) \neq \emptyset$ alors $X_{k(t)}(L(t)) \neq \emptyset$. Ainsi $I(X_K/K)$ divise $I(X/k)$. Soit P un point fermé de X_K de degré n. On a donc une extension finie de corps L/K et une K-immersion fermée $\mathrm{Spec}\, L \hookrightarrow X_K$. Le corps L est le corps des fonctions d'une k-courbe normale C, finie sur $\mathrm{Spec}\, k[t]$. Il existe un ouvert non vide $U \subset \mathrm{Spec}\, k[t]$ tel que la restriction C_U/U soit finie de degré n, et qu'il existe une U-immersion fermée $C_U \hookrightarrow X \times_k U$. Si le corps k est infini, on choisit un k-point $R \in U(k)$. La fibre de C_U/U au-dessus de ce k-point est le spectre d'une k-algèbre finie de degré n qui admet une k-immersion dans X. Une telle situation définit un zéro-cycle effectif de degré n sur la k-variété X (voir [5, Appendices A1, A2, A3]). Si le corps k est fini, il existe un zéro-cycle $\sum n_i R_i$ tel que tous les points fermés R_i soient dans $U \subset \mathrm{Spec}\, k[t]$ et que $\sum_i n_i [k(R_i) : k] = 1$. A chaque R_i on associe par la méthode ci-dessus un zéro-cycle effectif z_i de degré $n[k(R_i) : k]$ sur la k-variété X. Le zéro-cycle $\sum_i n_i . z_i$ est alors de degré n sur la k-variété X. Ainsi $I(X/k)$ divise $I(X_K/K)$. L'énoncé sur les indices réduits résulte immédiatement de celui sur les indices. □

3 Système de deux formes

Théorème 1. *Soient k un corps, f et g deux formes de degré $d \geq 1$ en $n+1 \geq 3$ variables, non toutes deux nulles. Soient t une variable et $K = k(t)$.*

L'indice réduit de la K-hypersurface $W \subset \mathbb{P}^n_K$ définie par $f + tg = 0$ coïncide avec l'indice réduit de la k-variété $X \subset \mathbb{P}^n_k$ définie par $f = g = 0$.

En particulier, la K-hypersurface $f + tg = 0$ possède un zéro-cycle de degré 1 si et seulement si la k-sous-variété X de $\mathbb{P}^n_k$ définie par $f = g = 0$ possède un zéro-cycle de degré 1.

Preuve. Pour les k-variétés, on omet l'indice k. Si L/k est une extension finie de corps avec $X(L) \neq \emptyset$, alors $W(L(t)) \neq \emptyset$. Ainsi l'indice $I(W/K)$ divise $I(X/k)$, et donc l'indice réduit $I_{\mathrm{red}}(W/K)$ divise l'indice réduit $I_{\mathrm{red}}(X/k)$. D'après le lemme 1 (c), pour établir l'énoncé on peut remplacer le corps k par une extension transcendante pure. On supposera donc le corps k infini.

Supposons d'abord que les formes f et g n'ont pas de facteur commun non constant.

Soit $V = \mathbb{P}^n \setminus X$. Notons $I = I(X/k)$. De la suite exacte de localisation ([5, I. Prop. 1.8]) :

$$\mathrm{CH}_0(X) \to \mathrm{CH}_0(\mathbb{P}^n) \to \mathrm{CH}_0(V) \to 0$$

et du fait que le degré sur k définit un isomorphisme $\mathrm{CH}_0(\mathbb{P}^n) \simeq \mathbb{Z}$, on tire l'égalité $\mathrm{CH}_0(V) = \mathbb{Z}/I$. Soit $Z \subset \mathbb{P}^1 \times \mathbb{P}^n$ la k-variété définie par

$$\lambda f + \mu g = 0.$$

Via la projection $\mathbb{P}^1 \times \mathbb{P}^n \to \mathbb{P}^n$, c'est l'éclatée de $\mathbb{P}^n$ le long de l'intersection complète $X \subset \mathbb{P}^n$ ([5, Appendix A, Remark A.6]). Soit $U \subset \mathbb{P}^1 \times \mathbb{P}^n$ l'ouvert complémentaire de Z. La projection $q : \mathbb{P}^1 \times \mathbb{P}^n \to \mathbb{P}^n$ induit un morphisme $q_U : U \to V$ qui fait de U un fibré en droites affines sur V. On en déduit un isomorphisme $q_U^* : \mathbb{Z}/I = \mathrm{CH}_0(V) \xrightarrow{\cong} \mathrm{CH}_1(U)$. On a la suite exacte de localisation ([5, I. Prop. 1.8]) :

$$\mathrm{CH}_1(Z) \to \mathrm{CH}_1(\mathbb{P}^1 \times \mathbb{P}^n) \to \mathrm{CH}_1(U) \to 0.$$

Par ailleurs les poussettes associées à la projection $p : \mathbb{P}^1 \times \mathbb{P}^n \to \mathbb{P}^1$ et à la projection $q : \mathbb{P}^1 \times \mathbb{P}^n \to \mathbb{P}^n$ induisent un isomorphisme

$$(p_*, q_*) : \mathrm{CH}_1(\mathbb{P}^1 \times \mathbb{P}^n) \xrightarrow{\cong} \mathrm{CH}_1(\mathbb{P}^1) \oplus \mathrm{CH}_1(\mathbb{P}^n) = \mathbb{Z} \oplus \mathbb{Z}.$$

Notons

$$i : \mathrm{CH}_1(Z) \to \mathrm{CH}_1(\mathbb{P}^1 \times \mathbb{P}^n) \xrightarrow{\cong} \mathrm{CH}_1(\mathbb{P}^1) \oplus \mathrm{CH}_1(\mathbb{P}^n) = \mathbb{Z} \oplus \mathbb{Z}$$

l'application composée. Sur Z, on trouve les 1-cycles suivants.

Le corps k étant infini, et les formes f et g sans facteur commun, on trouve un cycle $z_1 = \mathbb{P}^1 \times R$, où R est un zéro-cycle effectif de degré d^2 sur X par intersection avec un espace linéaire de codimension 2 convenable. L'image par i de z_1 est $(d^2, 0)$.

L'hypothèse que f et g n'ont pas de facteur commun assure que la k-variété $X \subset \mathbb{P}^n$ est de codimension 2. Soient $\mathrm{Gr}(1,\mathbb{P}^n)$ la grassmannienne des droites dans $\mathbb{P}^n$ et $E \subset \mathrm{Gr}(1,\mathbb{P}^n) \times \mathbb{P}^n$ la variété d'incidence. Soient r_1, r_2 les deux projections induites sur E. L'image réciproque $r_2^{-1}(X)$ est de codimension au moins 2 dans E, le morphisme r_1 a ses fibres de dimension 1, donc l'adhérence de $r_1(r_2^{-1}(X))$ dans $\mathrm{Gr}(1,\mathbb{P}^n)$ est de codimension au moins 1. Le corps k étant infini, et la k-variété $\mathrm{Gr}(1,\mathbb{P}^n)$ k-birationnelle à un espace projectif, on peut donc trouver une k-droite $L = \mathbb{P}^1 \subset \mathbb{P}^n$ qui ne rencontre pas X. Soit $q_Z : Z \to \mathbb{P}^n$ la restriction de q à Z. Le morphisme q_Z induit un isomorphisme $Z \setminus q^{-1}(X) \xrightarrow{\cong} \mathbb{P}^n \setminus X$. Soit $z_2 \subset Z$ l'image réciproque de L par cet isomorphisme. Ceci définit un 1-cycle sur $Z \subset \mathbb{P}^1 \times \mathbb{P}^n$, dont l'image par i est $(d,1)$. En effet, ce 1-cycle est donné par $L \to \mathbb{P}^1 \times \mathbb{P}^n$, où la projection sur le second facteur est l'inclusion linéaire $l : L \subset \mathbb{P}^n$, et où la projection sur le premier facteur est donnée par $(-g(l), f(l))$ (on a noté ici l un système de $n+1$ formes linéaires en deux variables). Comme X ne rencontre pas l, le couple $(f(l), g(l))$ de formes homogènes de degré d n'a pas de zéro commun.

Soit $s = I(W/K)$. L'hypersurface $f + tg = 0$ sur le corps K possède un zéro-cycle de degré s. L'adhérence d'un tel zéro-cycle dans $Z \subset \mathbb{P}^1 \times \mathbb{P}^n$ définit un 1-cycle z_3 dont l'image par i est de la forme (s,a) pour un certain entier $a \in \mathbb{Z}$.

Le quotient de $\mathbb{Z} \oplus \mathbb{Z}$ par le groupe engendré par $(d^2,0), (d,1), (s,a)$ est annulé par l'entier $\mathrm{pgcd}(d^2,\ s - ad)$. De la suite de localisation on conclut que, pour un certain entier $a \in \mathbb{Z}$, l'entier $I = I(X/k)$ divise $\mathrm{pgcd}(d^2,\ I(W/K) - ad)$. Ainsi $I_{\mathrm{red}}(X/k)$ divise $I(W/K)$. Comme par ailleurs $I_{\mathrm{red}}(W/K)$ divise $I_{\mathrm{red}}(X/k)$, on conclut

$$I_{\mathrm{red}}(X/k) = I_{\mathrm{red}}(W/K).$$

Supposons maintenant que $f = h.f_1$ et $g = h.g_1$ avec f_1 et g_1 homogènes de même degré sans facteur commun non constant et h homogène non constant.

Soit $X \subset \mathbb{P}^n_k$, resp. $X_1 \subset \mathbb{P}^n_k$, resp. $X_2 \subset \mathbb{P}^n_k$ la k-variété définie par $f = g = 0$, resp. par $f_1 = g_1 = 0$, resp. par $h = 0$. Soit $W \subset \mathbb{P}^n_K$, resp. W_1/K la variété définie par $f + tg = 0$, resp. $f_1 + tg_1 = 0$. On a

$$I_{\mathrm{red}}(W/K) = \mathrm{pgcd}(I_{\mathrm{red}}(W_1/K),\ I_{\mathrm{red}}(X_{2,K}/K)) = \mathrm{pgcd}(I_{\mathrm{red}}(W_1/K),\ I_{\mathrm{red}}(X_2/k))$$

d'après le lemme 1 et

$$\mathrm{pgcd}(I_{\mathrm{red}}(W_1/K),\ I_{\mathrm{red}}(X_2/k)) = \mathrm{pgcd}(I_{\mathrm{red}}(X_1/k),\ I_{\mathrm{red}}(X_2/k)) = I_{\mathrm{red}}(X/k),$$

la première égalité résultant de $I_{\mathrm{red}}(W_1/K) = I_{\mathrm{red}}(X_1/k)$ établi ci-dessus, la seconde égalité provenant du lemme 1. Ceci achève la démonstration. □

Le théorème 1 se généralise à un nombre quelconque de formes. Il y a en fait deux généralisations. Nous aurons besoin du lemme suivant.

Lemme 2. *Soient k un corps, $f_0, f_1, \ldots, f_r$ des formes à coefficients dans k, de degré $d \geq 1$, en $n+1 \geq r+2$ variables $x_0, \ldots, x_n$. La k-variété $X \subset \mathbb{P}^n$ définie par l'annulation de ces formes contient un zéro-cycle effectif de degré d^{r+1}.*

Preuve. Par l'argument donné au lemme 1 (c), on peut supposer le corps k infini. Cette hypothèse sera utilisée de façon constante dans ce qui suit. Soient $g_0, g_1, \dots, g_r$ des formes de degré d, à coefficients dans k, dont l'annulation définit une sous-k-variété intersection complète et lisse $Y \subset \mathbb{P}^n$. Soit $\mathscr{X} \subset \mathbb{P}^n \times \mathbb{A}^1$ le sous-schéma fermé défini par l'idéal (homogène en les x_i)

$$(tg_0 + (1-t)f_0, \dots, tg_r + (1-t)f_r) \subset k[t][x_0, \dots, x_n].$$

Choisisons des formes linéaires $L_1, \dots, L_{n-r-1} \in k[x_0, \dots, x_n]$ telles que le sous-schéma de $\mathbb{P}^n$ défini par l'idéal $(g_0, \dots, g_r, L_1, \dots, L_{n-r-1})$ soit fini et étale sur k. Alors le sous-schéma fermé $\mathscr{C}'$ de $\mathscr{X}$ défini par l'idéal $(L_1, \dots, L_{n-r-1})$ est fini et étale de degré d^{r+1} au-dessus d'un voisinage ouvert U of 1 dans $\mathbb{A}^1$. Soit $\mathscr{C} \subset \mathscr{X}$ l'adhérence schématique de $\mathscr{C}' \cap \mathbb{P}^n_U$ dans $\mathscr{X}$. Le schéma $\mathscr{C}$ est propre sur $\mathbb{A}^1_k$ et comme un sous-schéma ouvert dense de $\mathscr{C}$ est quasi-fini sur $\mathbb{A}^1$, le morphisme $p : \mathscr{C} \to \mathbb{A}^1$ est fini. Comme $p^{-1}(U) \subset \mathscr{C}$ est étale sur U, donc réduit, son adhérence schématique $\mathscr{C}$ est aussi réduite, et chaque composante irréductible de $\mathscr{C}$ s'envoie surjectivement sur $\mathbb{A}^1$. Ainsi $\mathscr{C}$ est plat sur $\mathbb{A}^1$, et donc la fonction

$$a \to \dim_{k(a)} \mathscr{O}_{p^{-1}(a)}$$

est constante sur $\mathbb{A}^1$. En particulier, le 0-cycle associé au sous-schéma fermé $p^{-1}(0)$ de X a degré d^{r+1} sur k. □

4 Système de plusieurs formes, I

Voici la première généralisation du théorème 1.

Théorème 2. *Soient k un corps, et $f_0, f_1, \dots, f_r$, avec $r \geq 1$, des formes à coefficients dans k, de degré $d \geq 1$, en $n+1 \geq r+2$ variables. Soit $X \subset \mathbb{P}^n_k$ la k-variété définie par l'annulation de ces $r+1$ formes. Soient $t_1, \dots, t_r$ des variables indépendantes et $K = k(t_1, \dots, t_r)$. Soit $W \subset \mathbb{P}^n_K$ la K-variété définie par $f_1 - t_1 f_0 = \cdots = f_r - t_r f_0 = 0$. On a :*

$$I_{\text{red}}(X/k) = I_{\text{red}}(W/K).$$

En particulier, la K-variété W possède un zéro-cycle de degré 1 si et seulement si la k-variété X possède un zéro-cycle de degré 1.

Preuve. Pour les k-variétés, on omet l'indice k. Si L/k est une extension finie de corps avec $X(L) \neq \emptyset$, alors $W(L(t)) \neq \emptyset$. Ainsi l'indice $I(W/K)$ divise $I(X/k)$, et donc l'indice réduit $I_{\text{red}}(W/K)$ divise l'indice réduit $I_{\text{red}}(X/k)$. D'après le lemme 1 (c), pour établir l'énoncé on peut remplacer le corps k par une extension transcendante pure. On supposera donc le corps k infini.

Supposons d'abord que les formes f_i n'ont pas de facteur commun non constant.

Soient $V = \mathbb{P}^n \setminus X$ et $I = I(X/k)$. Comme au théorème 1, on a $\mathrm{CH}_0(V) = \mathbb{Z}/I$. Soit $Z \subset \mathbb{P}^r \times \mathbb{P}^n$ la k-variété définie par la proportionalité de $(\lambda_0, \dots, \lambda_r)$ et de

$(f_0,\dots,f_r)$, c'est-à-dire par le système d'équations $\lambda_i.f_j - \lambda_j.f_i = 0$ pour $i,j \in \{0,\dots,r\}$. La fibre de $Z \to \mathbb{P}^r$ au-dessus du point générique de $\mathbb{P}^r$ est W/K. Soit $U \subset \mathbb{P}^r \times \mathbb{P}^n$ l'ouvert complémentaire de Z. La projection $q : \mathbb{P}^r \times \mathbb{P}^n \to \mathbb{P}^n$ induit un morphisme $q_U : U \to V$. Soit $q_Z : Z \to \mathbb{P}^n$ le morphisme restriction de q à Z. Il induit un isomorphisme $q_Z^{-1}(V) \overset{\cong}{\to} V$. Les fibres de $q_U : U \to V$ au-dessus d'un point M de V sont donc le complémentaire d'un point dans un espace projectif $\mathbb{P}^r$. De façon plus globale, le morphisme $q_U : U \to V$ se décompose comme

$$U \to U_1 \to V$$

où $q_1 : U \to U_1$ est un fibré en droites affines et $q_2 : U_1 \to V$ est un fibré projectif de dimension relative $r-1$. Par image directe par morphisme propre on a un isomorphisme $q_{2*} : \mathrm{CH}_0(U_1) \overset{\cong}{\to} \mathrm{CH}_0(V) = \mathbb{Z}/I$. Par image inverse par morphisme plat, on a un isomorphisme $q_1^* : \mathrm{CH}_0(U_1) \overset{\cong}{\to} \mathrm{CH}_1(U)$. On a donc un isomorphisme $\mathrm{CH}_1(U) \overset{\cong}{\to} \mathbb{Z}/I$. On a la suite exacte de localisation

$$\mathrm{CH}_1(Z) \to \mathrm{CH}_1(\mathbb{P}^r \times \mathbb{P}^n) \to \mathrm{CH}_1(U) \to 0.$$

Par ailleurs les poussettes associées à la projection $p : \mathbb{P}^r \times \mathbb{P}^n \to \mathbb{P}^r$ et à la projection $q : \mathbb{P}^r \times \mathbb{P}^n \to \mathbb{P}^n$ induisent un isomorphisme

$$(p_*, q_*) : \mathrm{CH}_1(\mathbb{P}^r \times \mathbb{P}^n) \overset{\cong}{\to} \mathrm{CH}_1(\mathbb{P}^r) \oplus \mathrm{CH}_1(\mathbb{P}^n) = \mathbb{Z} \oplus \mathbb{Z}.$$

Notons

$$i : \mathrm{CH}_1(Z) \to \mathrm{CH}_1(\mathbb{P}^r \times \mathbb{P}^n) \overset{\cong}{\to} \mathrm{CH}_1(\mathbb{P}^r) \oplus \mathrm{CH}_1(\mathbb{P}^n) = \mathbb{Z} \oplus \mathbb{Z}$$

l'application composée. Sur Z, on trouve les 1-cycles suivants.

Un cycle $z_1 = \mathbb{P}^1 \times R$, où $\mathbb{P}^1 \subset \mathbb{P}^r$ est une droite et R est un zéro-cycle effectif de degré d^{r+1} sur X, dont l'existence est assurée par le lemme 2. L'image par i de z_1 est $(d^{r+1}, 0)$.

Soit $s = I(W/K)$. Il existe donc un zéro-cycle de degré s sur W/K, et un tel zéro-cycle s'étend en un r-cycle sur Z, cycle génériquement fini sur $\mathbb{P}^r$ de degré relatif s. Sa restriction au-dessus d'une droite générale $\mathbb{P}^1 \subset \mathbb{P}^r$ est un 1-cycle sur Z, dont l'image par i est de la forme (s,a) pour un certain entier $a \in \mathbb{Z}$.

Les formes homogènes $(f_0,\dots,f_r)$ définissent un k-morphisme $\sigma : V \to \mathbb{P}^r$. Elles définissent donc une section du morphisme $q_V : \mathbb{P}^r_V \to V$, restriction de q à $\mathbb{P}^r_V$, section dont l'image est dans Z : c'est l'isomorphisme inverse de l'isomorphisme $q_Z^{-1}(V) \overset{\cong}{\to} V$ mentionné plus haut. L'hypothèse que les f_i n'ont pas de diviseur commun non trivial assure que la k-variété $X \subset \mathbb{P}^n$ est de codimension au moins 2. Le corps k étant infini, par le même argument qu'au théorème 1, on peut donc trouver une k-droite $L = \mathbb{P}^1 \subset \mathbb{P}^n$ qui ne rencontre pas X. La restriction de σ à L est donc un morphisme $L \to Z \subset \mathbb{P}^r \times \mathbb{P}^n$, dont l'image est un 1-cycle sur Z. L'image de ce 1-cycle par i est $(d, 1)$.

Le quotient du groupe $\mathbb{Z} \oplus \mathbb{Z}$ par le groupe engendré par les trois éléments $(d^{r+1}, 0)$, (s,a) et $(d,1)$ est $\mathbb{Z}/J$, avec $J = \mathrm{pgcd}(d^{r+1},\ s-ad)$. De la suite de localisation on conclut que $I = I(X/k)$ divise $\mathrm{pgcd}(d^{r+1},\ I(W/K)-ad)$ pour un certain entier $a \in \mathbb{Z}$. Ainsi $I_{\mathrm{red}}(X/k)$ divise $I(W/K)$. Comme par ailleurs $I_{\mathrm{red}}(W/K)$ divise $I_{\mathrm{red}}(X/k)$, on obtient

$$I_{\mathrm{red}}(X/k) = I_{\mathrm{red}}(W/K).$$

Supposons maintenant que $f_i = h.g_i$ pour tout i avec les g_i homogènes de même degré sans facteur commun non constant et h homogène non constant.

Soit $X \subset \mathbb{P}^n_k$, resp. $X_1 \subset \mathbb{P}^n_k$, resp. $X_2 \subset \mathbb{P}^n_k$ la k-variété définie par l'annulation des f_i, resp. par l'annulation des g_i, resp. par $h = 0$. Soit $W \subset \mathbb{P}^n_K$, resp. W_1/K la variété définie par l'annulation des $f_i - t_i f_0$ $(i = 1, \ldots, r)$, resp. par l'annulation des $g_i - t_i g_0$ $(i = 1, \ldots, r)$. On a

$$I_{\mathrm{red}}(W/K) = \mathrm{pgcd}(I_{\mathrm{red}}(W_1/K),\ I_{\mathrm{red}}(X_{2,K}/K)) = \mathrm{pgcd}(I_{\mathrm{red}}(W_1/K),\ I_{\mathrm{red}}(X_2/k))$$

d'après le lemme 1 et

$$\mathrm{pgcd}(I_{\mathrm{red}}(W_1/K),\ I_{\mathrm{red}}(X_2/k)) = \mathrm{pgcd}(I_{\mathrm{red}}(X_1/k),\ I_{\mathrm{red}}(X_2/k)) = I_{\mathrm{red}}(X/k),$$

la première égalité résultant de $I_{\mathrm{red}}(W_1/K) = I_{\mathrm{red}}(X_1/k)$ établi ci-dessus, la seconde égalité provenant du lemme 1. Ceci achève la démonstration. $\square$

5 Système de plusieurs formes, II

Voici la seconde généralisation du théorème 1.

Théorème 3. *Soient k un corps, $f_0, f_1, \ldots, f_r$ des formes non toutes nulles, à coefficients dans k, de degré $d \geq 1$, en $n+1 \geq r+2$ variables. Soit $X \subset \mathbb{P}^n_k$ la k-variété définie par l'annulation de ces formes. Soient $w_1, \ldots, w_r$ des variables indépendantes et $L = k(w_1, \ldots, w_r)$. Soit $Y \subset \mathbb{P}^n_L$ l'hypersurface définie par l'équation $f_0 + w_1 f_1 + \cdots + w_r f_r = 0$. On a :*

$$I_{\mathrm{red}}(X/k) = I_{\mathrm{red}}(Y/L).$$

En particulier, la L-hypersurface Y possède un zéro-cycle de degré 1 si et seulement si la k-variété X possède un zéro-cycle de degré 1.

Preuve. Soit E_r l'énoncé de ce théorème pour r fixé et tout corps k. L'énoncé E_1 est le théorème 1. Supposons établi E_{r-1}.

Supposons $r \geq 2$. Soient $t_1, \ldots, t_r$ des variables indépendantes et $K = k(t_1, \ldots, t_r)$. D'après le théorème 2, on a $I_{\mathrm{red}}(X/k) = I_{\mathrm{red}}(W/K)$, où la K-variété $W \subset \mathbb{P}^n_K$ est définie par

$$f_1 - t_1 f_0 = \cdots = f_r - t_r f_0 = 0.$$

Soient $s_2,\dots,s_r$ des variables indépendantes et $F = K(s_2,\dots,s_r)$. D'après E_{r-1}, l'indice réduit de W sur $K = k(t_1,\dots,t_r)$ est égal à l'indice réduit sur F de l'hypersurface T définie dans $\mathbb{P}^n_F$ par

$$(f_1 - t_1 f_0) + s_2(f_2 - t_2 f_0) + \cdots + s_r(f_r - t_r f_0) = 0.$$

Ceci se réécrit

$$f_1 - (t_1 + s_2t_2 + \cdots + s_rt_r)f_0 + s_2f_2 + \cdots + s_rf_r = 0.$$

Soient $w_1 = -1/(t_1+s_2t_2+\cdots+s_rt_r)$ et, pour $i \geq 2$, $w_i = -s_i/(t_1+s_2t_2+\cdots+s_rt_r)$.

L'équation de l'hypersurface $T \subset \mathbb{P}^n_F$ s'écrit alors

$$f_0 + w_1f_1 + \cdots + w_rf_r = 0.$$

L'inclusion

$$k(w_1,\dots,w_r,t_2,\dots,t_r) \subset k(t_1,t_2,\dots,t_r,s_2,\dots,s_r) = F$$

est une égalité. L'extension $F = L(t_2,\dots,t_r)$ est transcendante pure. D'après le lemme 1, l'indice réduit sur L de l'hypersurface définie par

$$f_0 + w_1f_1 + \cdots + w_rf_r = 0$$

dans $\mathbb{P}^n_L$ est égal à l'indice réduit de cette hypersurface sur F. Ceci achève la démonstration. $\square$

Remarque. A. Pfister, J.W.S. Cassels et D. F. Coray (voir les références dans [3]) ont donné des exemples d'intersections complètes de trois quadriques $f_0 = f_1 = f_2 = 0$ dans $\mathbb{P}^n_k$ (sur un corps k de caractéristique différente de 2) qui possèdent un zéro-cycle de degré 1 sans posséder de point rationnel. La quadrique $f_0 + t_1f_1 + t_2f_2 = 0$ sur le corps $k(t_1,t_2)$ possède alors un zéro-cycle de degré 1. Comme c'est une quadrique, un théorème de Springer [6] assure que cette quadrique admet un point $k(t_1,t_2)$-rationnel. On voit ainsi que le théorème 3 ne vaut pas lorsque l'on remplace les zéro-cycles de degré 1 par des points rationnels : le théorème d'Amer et Brumer ne s'étend pas à un système de 3 formes.

Remerciements. Les auteurs savent gré au rapporteur de ses lectures attentives. Marc Levine remercie la NSF (grant number DMS-0801220) et la fondation Alexander von Humboldt.

Littérature

1. M. Amer, Quadratische Formen über Funtionenkörpern, Dissertation, Johannes Gutenberg Universität, Mainz 1976.
2. A. Brumer, Remarques sur les couples de formes quadratiques. C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 16, A679–A681.

3. D. F. Coray, On a problem of Pfister about intersections of three quadrics. Arch. Math. (Basel) **34** (1980), no. 5, 403–411.
4. R. Elman, N. Karpenko, and A. Merkurjev, The algebraic and geometric theory of quadratic forms, AMS Colloquium Publications, vol. **56**, American Mathematical Society, Providence, RI, 2008.
5. W. Fulton, Intersection theory, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band **2**, Springer-Verlag 1984.
6. T. A. Springer, Sur les formes quadratiques d'indice zéro. C. R. Acad. Sci. Paris **234** (1952) 1517–1519.

Quaternion Algebras with the Same Subfields

Skip Garibaldi and David J. Saltman

Summary Prasad and Rapinchuk asked if two quaternion division F-algebras that have the same subfields are necessarily isomorphic. The answer is known to be "no" for some very large fields. We prove that the answer is "yes" if F is an extension of a global field K so that F/K is unirational and has zero unramified Brauer group. We also prove a similar result for Pfister forms and give an application to tractable fields.

1 Introduction

Gopal Prasad and Andrei Rapinchuk asked the following question in Remark 5.4 of their paper [PR]:[1]

If two quaternion division algebras over a field F have the same maximal subfields, are the algebras necessarily isomorphic? (1.1)

The answer is "no" for some fields F, see Sect. 2 below. The answer is "yes" if F is a global field by the Albert-Brauer-Hasse-Minkowski Theorem [NSW, 8.1.17]. Prasad and Rapinchuk note that the answer is unknown even for fields like $\mathbb{Q}(x)$. We prove that the answer is "yes" for this field.

Skip Garibaldi
Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322, USA,
e-mail: skip@mathcs.emory.edu

David J. Saltman
Center for Communications Research-Princeton, 805 Bunn Drive, Princeton, NJ 008540, USA,
e-mail: saltman@idaccr.org

2010 Mathematics subject classification. Primary: 16K20. Secondary: 11E04, 11E72.

[1] The reference [40] in [PR] should point to this paper.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_13,

Theorem 1.2. *Let F be a field of characteristic $\neq 2$ that is transparent. If D_1 and D_2 are quaternion division algebras over F that have the same maximal subfields, then D_1 and D_2 are isomorphic.*

The term "transparent" is defined in Sect. 6 below. Every retract rational extension of a local, global, real-closed, or algebraically closed field is transparent; in particular $K(x_1,\ldots,x_n)$ is transparent for every global field K of characteristic $\neq 2$ and every n. There are many other examples.

The theorem can be viewed as a statement about symbols in the Galois cohomology group $H^2(F,\mathbb{Z}/2\mathbb{Z})$. We also state and prove an analogue for symbols in Galois cohomology of $H^d(F,\mathbb{Z}/2\mathbb{Z})$ – i.e., d-Pfister quadratic forms – in Theorem 9.1 later.

Notation. A *global field* is a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$ for some prime p. A *local field* is a completion of a global field with respect to a discrete valuation.

We follow [Lam 05] for notation on quadratic forms, except that we define the symbol $\langle\langle a_1,\ldots,a_d\rangle\rangle$ to be the d-Pfister form $\otimes_{i=1}^d\langle 1,-a_i\rangle$. For a Pfister form φ, we put φ' for the unique form such that $\varphi\cong\langle 1\rangle\oplus\varphi'$.

2 An Example

Example 2.1. Several people (in no particular order: Markus Rost, Kelly McKinnie, Adrian Wadsworth, Murray Schacher, Daniel Goldstein, etc.) noted that some hypothesis on the field F is necessary for the conclusion of the theorem to hold. Here is an example to illustrate this.

Let F_0 be a field of characteristic $\neq 2$ that has quaternion division algebras Q_1, Q_2 that are not isomorphic. Replacing F_0 if necessary by the function field of a generalized Severi-Brauer variety, we may assume that $Q_1\otimes Q_2$ has index 2 and so that Q_1 and Q_2 both contain a maximal subfield $F_0(\sqrt{b})$. Write $\varphi_i := \langle\langle a_i,b\rangle\rangle$ for the norm form of Q_i. The Albert form $\varphi_1-\varphi_2$ has anisotropic part similar to $\gamma=\langle\langle a_1a_2,b\rangle\rangle$.

Fix an extension E/F_0 and a proper quadratic extension $E(\sqrt{c})$ contained in Q_i but not Q_{i+1}, with subscripts taken modulo 2. Equivalently, $-c$ is represented by φ_i' but not by φ_{i+1}'. Put $q_{i,c} := \langle c\rangle\oplus\varphi_{i+1}'$; it is anisotropic. Further, its determinant c is a nonsquare, so $q_{i,c}$ is not similar to φ_i, φ_{i+1}, nor γ. All three of those forms remain anisotropic over the function field $E(q_{i,c})$ of $q_{i,c}$ by [Lam 05, X.4.10(3)]. That is, $Q_1\otimes E(q_{i,c})$ and $Q_2\otimes E(q_{i,c})$ are division and contain $E(q_{i,c})(\sqrt{c})$, and the two algebras are still distinct.

We build a field F from F_0 inductively. Suppose we have constructed the field F_j for some $j\geq 0$. Let F_{j+1} be the composita of the extensions $F_j(q_{i,c})$ for c as in the previous paragraph with $E=F_j$ and $i=1,2$. Let F be the colimit of the F_j.

By construction, $Q_1\otimes F$ and $Q_2\otimes F$ are both division, are not isomorphic to each other, and have the same quadratic subfields. This shows that some hypothesis on the field F is necessary for the conclusion of the theorem to hold.

One cannot simply omit the hypothesis "division" in the theorem, by Example 3.6.

Furthermore, Theorem 1.2 does not generalize to division algebras of prime degree > 2, even over number fields. One can easily construct examples using the local–global principle for division algebras over a number field, see [PR, Example 6.5] for details.

3 Discrete Valuations: Good Residue Characteristic

Fix a field F with a discrete valuation v. We write $\bar{F}$ for the residue field and $\hat{F}$ for the completion. (Throughout this note, for fields with a discrete valuation and elements of such a field, we use bars and hats to indicate the corresponding residue field/completion and residues/image over the completion.)

For a central simple F-algebra A, we write $\hat{A}$ for $A \otimes \hat{F}$. It is Brauer-equivalent to a central division algebra B over $\hat{F}$. As v is complete on $\hat{F}$, it extends uniquely to a valuation on B by setting $v(b) := \frac{1}{\deg B} v(\mathrm{Nrd}_B(b))$ for $b \in B^\times$, see, e.g., [R, 12.6]. We say that A is *unramified* if $v(B^\times) = v(F^\times)$ – e.g., if $\hat{F}$ splits A – and *ramified* if $v(B^\times)$ is strictly larger. That is, A is ramified or unramified if v is so on B. Note that these meanings for ramified and unramified are quite a bit weaker than the usual definitions (which usually require that the residue division algebra of B be separable over $\bar{F}$).

The valuation ring in $\hat{F}$ is contained in a noncommutative discrete valuation ring S in B, and the residue algebra of S is a (possibly commutative) division algebra $\bar{B}$ whose center contains $\bar{F}$. One has the formula

$$\dim_{\bar{F}} \bar{B} \cdot [v(B^\times) : v(F^\times)] = \dim_{\hat{F}} B$$

(see [W, p. 393] for references). That is, A is unramified if and only if $\dim_{\bar{F}} \bar{B} = \dim_{\hat{F}} B$.

We use a few warm-up lemmas.

Lemma 3.1. *Let A_1, A_2 be central simple algebras over a field F that has a discrete valuation. If there is a separable maximal commutative subalgebra that embeds in one of the $\hat{A}_i$ and not the other, then the same is true for the A_i.*

Proof. Let $\hat{L}$ be a separable maximal commutative subalgebra of $\hat{A}_1$ that is not a maximal subalgebra of $\hat{A}_2$. Choose $\hat{\alpha} \in \hat{L}$ so that $\hat{L} = \hat{F}(\hat{\alpha})$. As A_1 is dense in $\hat{A}_1$, we can choose $\alpha \in A_1$ as close as we want to $\hat{\alpha}$. Thus we can choose the Cayley-Hamilton polynomial of α to be as close as we need to that of $\hat{\alpha}$. In particular, by Krasner's Lemma (applied as in [R, 33.8]), we can assume that $\hat{F}(\alpha) \cong \hat{F}(\hat{\alpha})$. In particular, $\hat{F}(\alpha)$ is not a maximal subalgebra of $\hat{A}_2$, which implies that $F(\alpha)$ is not a maximal subalgebra of A_2 and is by construction a maximal subfield of A_1. Because $\hat{F}(\alpha) \cong \hat{F}(\hat{\alpha})$, the minimal polynomial of α over F has nonzero discriminant and hence is separable. $\square$

Lemma 3.2. *Let A_1, A_2 be central division algebras of prime degree over a field F with a discrete valuation. If*

1. *$\hat{A}_1$ is split and $\hat{A}_2$ is not; or*
2. *Both $\hat{A}_1$ and $\hat{A}_2$ are division, but only one is ramified,*

then there is a separable maximal subfield of A_1 or A_2 that does not embed in the other.

Proof. The statement is obvious from Lemma 3.1. In case (1), we take the diagonal subalgebra in $\hat{A}_1$. In case (2), we take a maximal separable subfield that is ramified. □

For the rest of this section, we fix a prime p and let F be a field with a primitive p-th root of unity ζ; we suppose that F has a discrete valuation v with residue field of characteristic different from p.

A *degree p symbol algebra* is an (associative) F-algebra generated by elements α, β subject to the relations $\alpha^p = a$, $\beta^p = b$, and $\alpha\beta = \zeta\beta\alpha$. It is central simple over F [D, p. 78] and we denote it by $(a,b)_F$ or simply (a,b).

Lemma 3.3. *If A is a degree p symbol algebra over F, then A is isomorphic to $(a,b)_F$ for some $a,b \in F^\times$ with $v(a) = 0$.*

Proof. Write A as (a,b) where $a = x\pi^{n_a}$ and $b = y\pi^{n_b}$ where x, y have value 0 and π is a uniformizer for F. We may assume that p divides neither n_a nor n_b, so $n_a = sn_b$ modulo p. But A is isomorphic to $(a(-b)^{-s}, b)$ because $(-b,b)$ is split [D, p. 82, Cor. 5], and $v(a(-b)^{-s})$ is divisible by p. □

3.4. Let (a,b) be a symbol algebra as in Lemma 3.3 and write $\hat{F}$ for the completion of F at v. If $(a,b) \otimes \hat{F}$ is not division, certainly (a,b) is *unramified*. Otherwise, there are two cases:

- If $v(b)$ is divisible by p, then we can assume $v(b) = 0$, (a,b) is unramified, and $\overline{(a,b)}$ is the symbol algebra $(\bar{a}, \bar{b})_{\bar{F}}$. (The residue algebra – which is division – contains $(\bar{a}, \bar{b})_{\bar{F}}$, hence they must be equal.)
- If $v(b)$ is not divisible by p, then (a,b) is ramified and $\overline{(a,b)}$ is the field extension $\bar{F}(\sqrt[p]{\bar{a}})$. (By hypothesis, a is not a p-th power in $\hat{F}$, so by Hensel's Lemma $\bar{a}$ is not a p-th power in $\bar{F}$.)

Proposition 3.5. *Let A_1 and A_2 be degree p symbol algebras over F that are division algebras. If*

1. *A_1 ramifies and A_2 does not; or*
2. *A_1 and A_2 both ramify but their ramification defines different extensions of the residue field $\bar{F}$,*

then there is a maximal subfield L of one of the A_i that does not split the other.

Proof. Write A_i as (a_i, b_i). We can assume $v(a_1) = v(a_2) = 0$. If both the A_i ramify, then the $v(b_i)$ must be prime to p and the field extensions of the ramification of the A_i must be $\bar{F}(\sqrt[p]{\bar{a}_i})$. If these are different fields, then the field $L_2 := F(\sqrt[p]{a_2})$ cannot split A_1 because it does not split the ramification of A_1.

Thus assume A_2 is unramified and A_1 ramifies. In particular, $A_1 \otimes \hat{F}$ is division, and we are done by Lemma 3.2. □

Example 3.6. In the proposition, the hypothesis that A_1 and A_2 are both division is necessary. Indeed, for $\ell \neq 2$, the field $\mathbb{Q}_\ell$ of ℓ-adic numbers has two quaternion algebras: one split and one division. Only one is ramified, but both are split by every quadratic extension of $\mathbb{Q}_\ell$.

4 Discrete Valuations: Bad Residue Characteristic

In this section, we consider quaternion algebras over a field with a dyadic discrete valuation. The purpose of this section is to prove:

Proposition 4.1. *Let A_1, A_2 be quaternion division algebras over a field F of characteristic* 0 *that has a dyadic discrete valuation. If $A_1 \otimes A_2$ is Brauer-equivalent to a ramified quaternion division algebra with residue algebra a separable quadratic extension of $\bar{F}$, then there is a quadratic extension of F that embeds in A_1 or A_2 but not both.*

What really helps nail down the structure of $A_1 \otimes A_2$ is the hypothesis that the residue algebra is a separable quadratic extension. In particular, the division algebra underlying $A_1 \otimes A_2$ is "inertially split" in the language of [JW] or "tame" in the language of [GP].

Example 4.2. Let B be a quaternion division algebra over a field F of characteristic 0 that is complete with respect to a dyadic discrete valuation, and suppose that the residue algebra $\bar{B}$ contains a separable quadratic extension $\bar{L}$ of F. One can lift $\bar{L}/\bar{F}$ to a *unique* quadratic extension L/F and write $B = (L, b)$ for some $b \in F^\times$ that we may assume has value 0 or 1. One finds two possibilities:

- If $v(b) = 0$, then $\bar{B}$ is a quaternion algebra over $\bar{F}$ generated by elements i, j such that
$$\bar{F}(i) = \bar{L},\ i^2 + i \in \bar{F},\ j^2 = \bar{b}, \quad \text{and} \quad ij = j(i+1).$$
In this case B is unramified.
- If $v(b) = 1$, then $\bar{B} = \bar{L}$ and B is ramified.

For detailed explanation of these claims, see, e.g., [T] or [GP]. (Unlike the situation in the preceding section, there are more than just these two possibilities for general quaternion algebras over F, but in those other cases the residue algebra $\bar{B}$ is a purely inseparable extension of $\bar{F}$ of dimension 2 or 4 with $\bar{B}^2 \subseteq \bar{F}$. Note that if L/F is unramified and $\bar{L}/\bar{F}$ is purely inseparable, then L/F is *not* uniquely determined by $\bar{L}/\bar{F}$.)

Proof (of Proposition 4.1). Put B for the quaternion division F-algebra underlying $A_1 \otimes A_2$. By the hypothesis on its residue algebra, B remains division when we extend scalars to the completion $\hat{F}$. Hence at least one of $\hat{A}_1$, $\hat{A}_2$ is division; by Lemma 3.2 (using that A_1 and A_2 are division) we may assume that both $\hat{A}_1$ and $\hat{A}_2$ are division and that the valuation has the same ramification index on both algebras. By Lemma 3.1, we may assume that F is complete.

For sake of contradiction, suppose that A_1 and A_2 have the same subfields. The residue division algebra $\bar{A}_1$ is distinct from $\bar{F}$ and we can find a quadratic subfield L of A_1 so that the residue field $\bar{L}$ is a quadratic extension of $\bar{F}$. As L is a maximal subfield of A_1, it is also one for A_2 and hence B. Certainly, $\bar{L}$ is a subfield of the residue algebra $\bar{B}$; as both have dimension 2 over $\bar{F}$ they are equal. That is, $\bar{L}/\bar{F}$ is separable. We write $A_i = (L, a_i)$ and $B = (L, b)$ for some $a_i, b \in F^\times$. As the valuation does not ramify on L we may assume that $v(b) = 1$. As $\bar{A}_i$ contains the separable extension $\bar{L}/\bar{F}$, we have $v(a_1) = v(a_2)$ as in Example 4.2. Then $A_1 \otimes A_2 \otimes B$ – which is split – is Brauer-equivalent to (L, a_1a_2b), which is ramified (because $v(a_1a_2b) = 1 + 2v(a_i)$ is odd) and in particular not split. This is a contradiction, which completes the proof of the proposition. □

5 Unramified Cohomology

For a field F of characteristic not 2, we write $H^d(F)$ for the Galois cohomology group $H^d(F, \mathbb{Z}/2\mathbb{Z})$. We remind the reader that for $d = 1$, this group is $F^\times/F^{\times 2}$ and for $d = 2$ it is identified with the 2-torsion in the Brauer group of F.

Definition 5.1. Fix an integer $d \geq 2$. We define $H^d_u(F)$ to be the subgroup of $H^d(F)$ consisting of classes that are unramified at every nondyadic discrete valuation of F (in the usual sense, as in [GMS, p. 19]) and are killed by $H^d(F) \to H^d(R)$ for every real closure R of F.

Example 5.2. 1. A local field F (of characteristic $\neq 2$) has $H^2_u(F) = 0$ if and only if F is nondyadic. Indeed, F has no orderings, so it suffices to consider the unique discrete valuation on F.

2. A global field F (of characteristic $\neq 2$) has $H^2_u(F) = 0$ if and only if F has at most 1 dyadic place. This is Hasse's local–global theorem for central simple algebras [NSW, 8.1.17].
3. A real closed field F has $H^d_u(F) = 0$ for all $d \geq 2$; this is trivial.

A local field F (of characteristic $\neq 2$) has $H^d_u(F) = 0$ for $d \geq 3$. This is trivial because such a field has no orderings and cohomological 2-dimension 2.

Lemma 5.3. *If $F(\sqrt{-1})$ has cohomological 2-dimension $< d$, then $H^d_u(F)$ is zero.*

Proof. If an element $x \in H^d(F)$ is zero at every real closure, then by [A, Satz 3] $x \cdot (-1)^r$ is zero for some $r \geq 0$. On the other hand, there is an exact sequence for every n [KMRT, 30.12(1)]:

$$H^n(F(\sqrt{-1})) \xrightarrow{\text{cor}} H^n(F) \xrightarrow{\cdot(-1)} H^{n+1}(F) \xrightarrow{\text{res}} H^{n+1}(F(\sqrt{-1}))$$

For $n \geq d$, the two end terms are zero, so the cup product with $(-1)^r$ defines an isomorphism $H^d(F) \xrightarrow{\sim} H^{d+r}(F)$ for all $r \geq 0$. □

We immediately obtain:

Corollary 5.4. *A global field F of characteristic $\neq 2$ has $H^d_u(F) = 0$ for all $d \geq 3$.* □

Corollary 5.5. *If F has transcendence degree $\geq t$ over a real-closed field then $H^d_u(F) = 0$ for all $d > t$.*

Proof. $F(\sqrt{-1})$ has transcendence degree t over an algebraically closed field, hence has cohomological dimension $\leq t$ [Se, Sect. II.4.3]. □

We define a discrete valuation of an extension F/F_0 to be a discrete valuation on F that vanishes on F_0.

Proposition 5.6. *For every extension F/F_0, the homomorphism $\mathrm{res}: H^d(F_0) \to H^d(F)$ restricts to a homomorphism $H^d_u(F_0) \to H^d_u(F)$. If, additionally, F/F_0 is unirational and*

every class in $H^d(F)$ that is unramified at every discrete valuation of F/F_0 comes from $H^d(F_0)$ (5.7)

then the homomorphism $H^d_u(F_0) \to H^d_u(F)$ is an isomorphism.

Proof. Fix $y \in H^d_u(F_0)$. Every ordering of F restricts to an ordering on F_0; write R and R_0 for the corresponding real closures. By hypothesis, the image of y in $H^d(R_0)$ is zero, hence it also has zero image under the composition $H^d(F_0) \to H^d(R_0) \to H^d(R)$. It is easy to see that $\mathrm{res}(y)$ is unramified at every nondyadic discrete valuation of F, and the first claim follows.

We now prove the second sentence. The natural map $H^d(F_0) \to H^d(F)$ is injective by [GMS, p. 28]. Fix $x \in H^d_u(F)$. As it is unramified at every discrete valuation of F/F_0, it is the restriction of some element $x_0 \in H^d(F_0)$ by (5.7). We will show that x_0 belongs to $H^d_u(F_0)$.

Fix an extension $E := F_0(x_1, x_2, \ldots, x_n)$ containing F. Every ordering on F_0 extends to an ordering v on E (and hence also on F) by a recipe as in [Lam 80, pp. 9–11]. As the map $H^d((F_0)_v) \to H^d(F_v)$ is an injection by Lemma 5.8 below, we deduce that x_0 is killed by every real-closure of F_0.

One extends a nondyadic discrete valuation v on F_0 to E by setting $v(x_i) = 0$ and $\bar{x}_i$ to be transcendental over $\bar{F}_0$ as in [B, Sect. VI.10.1, Prop. 2]; then the residue field of $\bar{E}$ is $\bar{F}_0(x_1, x_2, \ldots, x_n)$ and the natural map $H^{d-1}(\bar{F}_0) \to H^{d-1}(\bar{E})$ is injective, hence so is $H^{d-1}(\bar{F}_0) \to H^{d-1}(\bar{F})$. It follows that the image of x_0 in $H^{d-1}(\bar{F}_0)$ is zero, which completes the proof. □

Here is the promised lemma:

Lemma 5.8. *If $R_1 \subseteq R_2$ are real-closed fields, then the natural map $H^d(R_1) \to H^d(R_2)$ is an isomorphism for every $d \geq 0$.*

Proof. Trivially, $H^0(R_i) = \mathbb{Z}/2\mathbb{Z}$. Also, $H^1(R_i) = \mathbb{Z}/2\mathbb{Z}$ with nonzero element $(-1) \in R_i^\times/R_i^{\times 2}$. For all d, $H^d(R_i)$ (Galois cohomology) equals $H^d(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ (group cohomology), and two-periodicity for the cohomology of finite cyclic groups shows that $H^d(R_i) = \mathbb{Z}/2\mathbb{Z}$ for all $d \geq 0$, with nonzero element $(-1)^d$. $\square$

Example 5.9. Recall that an extension F of F_0 is *retract rational* if it is the field of fractions of an F_0-algebra domain S and there are F_0-algebra homomorphisms $S \to F_0[x_1,\dots,x_n](1/s) \to S$ whose composition is the identity on S, where $F_0[x_1,\dots,x_n]$ is a polynomial ring and $s \in F_0[x_1,\dots,x_n]$ is a nonzero element. Obviously such an extension is unirational, and (5.7) holds by [Sa, 11.8] or [M, Prop. 2.15], so $H^d_u(F_0) \cong H^d_u(F)$.

6 Transparent Fields

Definition 6.1. Fix a field F of characteristic $\neq 2$. For each dyadic valuation v, fix a completion $\hat{F}$ of F. Write K for the limit of the finite unramified extensions of $\hat{F}$ with separable residue field. This extension is called the *maximal unramified extension of* $\hat{F}$ (which highlights the fact that usually the word "unramified" is quite a bit stronger than how we are using it). There is a well-defined ramification map

$$H^2(K/\hat{F}, \mu_2) \to H^1(\bar{F}, \mathbb{Z}/2\mathbb{Z}) \quad \text{s.t.} \quad (a,b) \mapsto \begin{cases} 0 & \text{if } v(a) = v(b) = 0 \\ (\bar{a}) & \text{if } v(a) = 0 \ \& \ v(b) = 1 \end{cases}$$

We say that F is *transparent* if for every division algebra $D \neq F$ of exponent two such that $[D]$ belongs to $H^2_u(F)$, there is some dyadic place v of F and completion $\hat{F}$ such that

1. $D \otimes \hat{F}$ is split by the maximal unramified extension of $\hat{F}$, and
2. The image of $[D]$ in $H^1(\bar{F}, \mathbb{Z}/2\mathbb{Z})$ is not zero.

In case D is a quaternion algebra over F, these hypotheses may be rephrased as: *$D \otimes \hat{F}$ is division and the residue division algebra $\bar{D}$ is a separable quadratic extension of $\bar{F}$.*

Roughly speaking, transparent fields are those for which nonzero 2-torsion elements of the Brauer group can be detected using ramification.

Example 6.2. 0. If $H^2_u(F) = 0$ – e.g., if F is real closed – then F is (vacuously, trivially) transparent.

1. *If F is local then F is transparent.* If F is nondyadic, this is Example 5.2(1). Otherwise, for each nonzero $x \in H^2_u(F)$, the residue division algebra is necessarily a separable quadratic extension of $\bar{F}$, because $\bar{F}$ is perfect with zero Brauer group.
2. If F is global then F is transparent. Indeed, $H^2_u(F)$ consists of classes ramified only at dyadic places, and every such place has finite residue field.

The *unramified Brauer group* of an extension F/F_0 is the subgroup of the Brauer group of F consisting of elements that are unramified at every discrete valuation of F/F_0.

Proposition 6.3. *If F_0 is transparent, F/F_0 is unirational, and the unramified Brauer group of F/F_0 is zero, then F is transparent.*

Proof. Suppose there is a nonzero $x \in H^2_u(F)$. By Proposition 5.6, x is the image of some nonzero $x_0 \in H^2_u(F_0)$ and there is a dyadic valuation v of F_0 such that conditions (1) and (2) of Definition 6.1 holds for the division algebra D_0 represented by x_0. Extend v to a valuation on F as in the proof of Proposition 5.6. The maximal unramified extension of $\hat{F}$ (with respect to v) contains the maximal unramified extension of $\hat{F}_0$, so it kills x_0 and hence also x; this verifies condition (6.1.1). For condition (6.1.2), it suffices to note that the map $H^1(\bar{F}_0, \mathbb{Z}/2\mathbb{Z}) \to H^1(\bar{F}, \mathbb{Z}/2\mathbb{Z})$ is injective as in the proof of Proposition 5.6. $\square$

Example 6.4. A retract rational extension of a transparent field is transparent, cf. Example 5.9.

7 Proof of the Main Theorem

We now prove Theorem 1.2. We assume that D_1 and D_2 are not isomorphic and that there is some quadratic extension of F that is contained in both of them, hence that $D_1 \otimes D_2$ has index 2. We will produce a quadratic extension of F that is contained in one and not the other.

Suppose that first there is a real closure R of F that does not split $D_1 \otimes D_2$. Then one of the D_i is split by R and the other is not; say D_1 is split. We can write $D_1 = (a_1, b_1)$, where a_1 is positive in R. The field $F(\sqrt{a_1})$ is contained in D_1, but not contained in D_2 because $D_2 \otimes R$ is division.

If there is a nondyadic discrete valuation of F where $D_1 \otimes D_2$ is ramified then $[D_1]$ and $[D_2]$ have different images under the residue map $H^2(F) \to H^1(\bar{F})$ and Proposition 3.5 provides the desired quadratic extension.

Finally, suppose that $D_1 \otimes D_2$ is split by every real closure and is unramified at every nondyadic place, so $D_1 \otimes D_2$ belongs to $H^2_u(F)$. By the original hypotheses on D_1 and D_2, the class $[D_1 \otimes D_2]$ is represented by a quaternion division algebra B. But F is transparent, so Proposition 4.1 provides a quadratic extension of F that embeds in D_1 or D_2 but not the other. $\square$

8 Pfister forms and Nondyadic Valuations

With the theorem from the introduction proved, we now set to proving a version of it for Pfister forms. The goal of this section is the following proposition, which is an analogue of Proposition 3.5.

Proposition 8.1. *Let F be a field with a nondyadic discrete valuation. Let φ_1, φ_2 be d-Pfister forms over F for some $d \geq 2$. If*

1. *φ_1 is ramified and φ_2 is not; or*
2. *φ_1 and φ_2 both ramify, but with different ramification,*

then there is a $(d-1)$-Pfister form γ over F such that γ divides φ_1 or φ_2 but not both.

The proof given later for case (1) of the proposition was suggested to us by Adrian Wadsworth, and is much simpler than our original proof for that case. It makes use of the following lemma:

Lemma 8.2. *Let $\psi = \langle a_1, \ldots, a_n \rangle$ be a nondegenerate quadratic form over a field F with a nondyadic discrete valuation v. If $v(a_i) = 0$ for all i and ψ is isotropic over the completion $\hat{F}$ of F then there is a 2-dimensional nondegenerate subform q of ψ such that $q \otimes \hat{F}$ is isotropic.*

Proof. As $\varphi \otimes \hat{F}$ is isotropic, there exist $x_i \in \hat{F}$ not all zero so that $\sum a_i x_i^2 = 0$. Scaling by a uniformizer, we may assume that $v(x_i) \geq 0$ for all i and that at least one x_i has value 0. Let j be the smallest index such that $v(x_j) = 0$; there must be at least two such indices, so $j < n$.

Fix t_i in the valuation ring of F so that $\bar{t}_i = \bar{x}_i$, and put

$$r := \sum_{i=1}^{j} a_i t_i^2 \quad \text{and} \quad s := \sum_{i=j+1}^{n} a_i t_i^2 \quad \text{in } F.$$

By construction of j, $v(r) = 0$. As $r + s = 0$, also $v(s) = 0$. Now $\langle r, s \rangle$ is a subform of ψ (over F), and

$$\bar{r} + \bar{s} = \overline{r+s} = \overline{\sum a_i t_i^2} = \overline{\sum a_i x_i^2} = 0 \quad \in \bar{F}.$$

So $\langle r, s \rangle$ is isotropic over $\hat{F}$ [Lam 05]. □

Proof (of Proposition 8.1). Obviously, $\langle\langle x\pi, y\pi \rangle\rangle \cong \langle\langle -xy, y\pi \rangle\rangle$, so we may assume that

$$\varphi_i = \langle\langle a_{i2}, a_{i3}, \ldots, a_{id}, b_i \rangle\rangle,$$

where a_{ij} has value 0 and b_i has value 0 or 1.

In case (2), b_1 and b_2 have value 1 and the residue forms

$$r(\varphi_i) = \langle\langle \bar{a}_{i2}, \bar{a}_{i3}, \ldots, \bar{a}_{id} \rangle\rangle$$

are not isomorphic. We take γ to be $\langle\langle a_{12}, a_{13}, \ldots, a_{1d}\rangle\rangle$; it divides φ_1. The projective quadric X defined by $\gamma = 0$ is defined over the discrete valuation ring, and $\bar{F}(X)$ does not split $r(\varphi_2)$ by [Lam 05, X.4.10]. Hence, $F(X)$ does not split φ_2 and γ does not divide φ_2.

Now suppose we are in case (1); obviously $v(b_1) = 1$. If $\varphi_2 \otimes \hat{F}$ is anisotropic, then as φ_2 does not ramify, $v(b_2) = 0$ and the second residue form of φ_2 is zero. Certainly, $\gamma := \langle\langle a_{13}, \ldots, a_{1d}, b_1\rangle\rangle$ divides φ_1. On the other hand, every anisotropic multiple of $\gamma \otimes \hat{F}$ over $\hat{F}$ will have a nonzero second residue form, so φ_2 cannot contain γ.

Otherwise, $\varphi_2 \otimes \hat{F}$ is hyperbolic, and there exists some 2-dimensional subform q of φ_2 that becomes hyperbolic over $\hat{F}$ by Lemma 8.2. It follows that there is a $(d-1)$-Pfister ψ that is contained in φ_2 and that becomes hyperbolic over $\hat{F}$. But $\varphi_1 \otimes \hat{F}$ is ramified, hence anisotropic, so φ_1 cannot contain ψ. $\square$

9 Theorem for Quadratic Forms

Theorem 9.1. *Let F be a field of characteristic $\neq 2$ such that $H^d_u(F) = 0$ for some $d \geq 2$. Let φ_1 and φ_2 be anisotropic d-Pfister forms over F such that, for every $(d-1)$-Pfister form γ, we have: γ divides φ_1 if and only if γ divides φ_2. Then φ_1 is isomorphic to φ_2.*

We remark that for $d = 2$, Theorem 9.1 does not include the case where F is a retract rational extension of a global field with more than one dyadic place, a case included in Theorem 1.2.

Proof (of Theorem 9.1). Suppose that φ_1 and φ_2 are d-Pfister forms over F for some $d \geq 2$, $H^d_u(F)$ is zero, and φ_1 is not isomorphic to φ_2. Then $\varphi_1 + \varphi_2$ is in $H^d(F) \setminus H^d_u(F)$.

If there is a nondyadic discrete valuation where $\varphi_1 + \varphi_2$ ramifies, then Proposition 8.1 gives a $(d-1)$-Pfister form that divides one of the φ_i and not the other. Otherwise, there is an ordering v of F such that φ_1 and φ_2 are not isomorphic over the real closure F_v, i.e., one is locally hyperbolic and the other is not. Write $\varphi_i = \langle\langle a_{i1}, a_{i2}, \ldots, a_{id}\rangle\rangle$ and suppose that φ_1 is locally hyperbolic, so some a_{1j} is positive; renumbering if necessary, we may assume that it is a_{1d}. Then the form $\langle\langle a_{12}, a_{13}, \ldots, a_{1d}\rangle\rangle$ divides φ_1, but it is hyperbolic over F_v and so does not divide φ_2. $\square$

10 Appendix: Tractable Fields

We now use the notion of unramified cohomology from Sect. 5 to prove some new results and give new proofs of some known results regarding tractable fields. Recall from [CTW] that a field F of characteristic $\neq 2$ is called *tractable* if for every a_1,

$a_2, a_3, b_1, b_2, b_3 \in F^\times$ such that the six quaternion algebras (a_i, b_j) are split for all $i \neq j$ and the three quaternion algebras (a_i, b_i) are pairwise isomorphic, the algebras (a_i, b_i) are necessarily split. (This condition was motivated by studying conditions for decomposability of central simple algebras of degree 8 and exponent 2.) We prove:

Proposition 10.1. *If $H^2_u(F) = 0$, then F is tractable.*

Proof. For the sake of contradiction, suppose we are given a_i, b_i as in the definition of tractable where the quaternion algebras (a_i, b_i) are not split. If the (a_i, b_i) do not split at some real closure of F, then the a_i and b_i are all negative there. Hence (a_i, b_j) for $i \neq j$ is also not split, a contradiction.

So the (a_i, b_i) ramify at some nondyadic discrete valuation v of F and in particular are division over the completion of F at v. We replace F with its completion and derive a contradiction. Modifying each a_i or b_i by a square if necessary, we may assume that each one has value 0 or 1. Further, as each (a_i, b_i) is ramified, at most one of the two slots has value 0.

Suppose first that one of the a_i or b_i – say, a_1 – has value 0. Then b_1 has value 1 and a_1 is not a square in F. As (a_1, b_j) is split for $j \neq 1$, we deduce that $v(b_j) = 0$. Hence $v(a_2) = v(a_3) = 1$. As (a_3, b_3) is division, b_3 is not a square in F. Since $v(a_2) = 1$ and $v(b_3) = 0$, it follows that (a_2, b_3) is division, a contradiction.

It remains to consider the case where the a_i's and b_i's all have value 1. We can write $a_i = \pi\alpha_i$ and $b_i = \pi\beta_i$, where π is a prime element – say, a_1 so $\alpha_1 = 1$ – and α_i, β_i have value 0. In the Brauer group of F, we have for $i \neq j$:

$$0 = (\pi\alpha_i, \pi\beta_j) = (\pi\alpha_i, -\alpha_i\beta_j) = (\pi, -\alpha_i\beta_j) + (\alpha_i, \beta_j).$$

It follows that $-\alpha_i\beta_j$ is a square in F for $i \neq j$. In particular, $-\beta_2$, $-\beta_3$, α_2, and α_3 are all squares. Then

$$(a_2, b_2) = (\pi\alpha_2, \pi\beta_2) = (\pi, -\pi) = 0,$$

a contradiction. □

Example 10.2. In [CTW], the authors proved that a local field is tractable if and only if it is nondyadic (ibid., Cor. 2.3) and a global field is tractable if and only if it has at most 1 dyadic place (ibid., Th. 2.10). Combining the preceding proposition and Example 5.2 gives a proof of the "if" direction for both of these statements.

Corollary 10.3 ([CTW, Th. 3.17]). *Every field of transcendence degree 1 over a real-closed is tractable.*

Proof. Combine the proposition and Corollary 5.5. □

Example 10.4. The converse of Proposition 10.1 is false. For every odd prime p, $\mathbb{Q}_p((x))$ is tractable by [CTW, Prop. 2.5]. On the other hand, the usual discrete valuation on the formal power series ring is the unique one [EP, 4.4.1], so $H^2_u(\mathbb{Q}_p((x))) = H^2(\mathbb{Q}_p) = \mathbb{Z}/2\mathbb{Z}$.

Corollary 10.5. *Let F_0 be a field of characteristic $\neq 2$ that*

- *Is tractable and*
- *Is global, local, real-closed, or has no 2-torsion in its Brauer group.*

Then every unirational extension F/F_0 satisfying (5.7) – e.g., every retract rational extension F/F_0 – is also tractable.

Proof. We note that F_0 has $H^2_u(F_0) = 0$. In case F_0 is global or local, then F_0 has one dyadic place or is nondyadic, respectively, by [CTW], and the claim follows, see Example 5.2. Then $H^2_u(F)$ is also zero by Proposition 5.6, hence F is tractable. □

Of course, Corollary 10.5 includes the statement that rational extensions of tractable global fields are tractable, which was a nontrivial result (Example 3.14) in [CTW]. However, a stronger result has already been proved in [Han, Cor. 2.14]: every rational extension of a tractable field is tractable.

We do get a large family of new examples of tractable fields:

Corollary 10.6. *Let F be a global field with at most one dyadic place. If G is an isotropic, simply connected, absolutely almost simple linear algebraic group over F, then the function field $F(G)$ is tractable.*

Proof. $F(G)/F$ is retract rational by Theorems 5.9 and 8.1 in [Gi]. □

Acknowledgements The first author's research was partially supported by National Science Foundation grant no. DMS-0653502. Both authors thank Adrian Wadsworth and Kelly McKinnie for their comments on an earlier version of this paper.

References

[A] J.Kr. Arason, *Primideale im graduierten Wittring und im mod 2 Cohomologiering*, Math. Z. **145** (1975), 139–143.

[B] N. Bourbaki, *Commutative algebra. Chapters 1–7*, Elements of Mathematics, Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation.

[CTW] M. Chacron, J.-P. Tignol, and A.R. Wadsworth, *Tractable fields*, Can. J. Math. **51** (1999), no. 1, 10–25.

[D] P.K. Draxl, *Skew fields*, Lond. Math. Soc. Lecture Note Series, vol. 81, Cambridge University Press, Cambridge-New York, 1983.

[EP] A.J. Engler and A. Prestel, *Valued fields*, Springer, Berlin, 2005.

[Gi] P. Gille, Le problème de Kneser-Tits, Astérisque **326** (2009), 39–82.

[GMS] S. Garibaldi, A. Merkurjev, and J-P. Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, Am. Math. Soc., 2003.

[GP] S. Garibaldi and H.P. Petersson, *Wild Pfister forms over Henselian fields, K-theory, and conic division algebras*, arxiv:1002.3280v1, 2010.

[Han] I. Han, *Tractability of algebraic function fields in one variable of genus zero over global fields*, J. Algebra **244** (2001), no. 1, 217–235.

[JW] B. Jacob and A. Wadsworth, *Division algebras over Henselian fields*, J. Algebra **128** (1990), 126–179.

[KMRT] M.-A. Knus, A.S. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, Colloquium Publications, vol. 44, Am. Math. Soc., 1998.

[Lam 80] T.Y. Lam, *The theory of ordered fields*, Ring theory and algebra, III (Proc. Third Conf., Univ. Oklahoma, Norman, Okla., 1979), Lecture Notes in Pure and Appl. Math., vol. 55, Dekker, New York, 1980, pp. 1–152.

[Lam 05] ———, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, Am. Math. Soc., Providence, RI, 2005.

[M] A. Merkurjev, *Unramified elements in cycle modules*, J. Lond. Math. Soc. **78** (2008), no. 2, 51–64.

[NSW] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der math. Wissenschaften, vol. 323, Springer, Berlin, 2008.

[PR] G. Prasad and A.S. Rapinchuk, *Weakly commensurable arithmetic groups and isospectral locally symmetric spaces*, Pub. Math. IHES **109** (2009), 113–184.

[R] I. Reiner, *Maximal orders*, LMS Monographs, vol. 5, Academic Press, London, 1975.

[Sa] D.J. Saltman, *Lectures on division algebras*, CBMS Regional Conference Series in Mathematics, vol. 94, American Mathematical Society, Providence, RI, 1999.

[Se] J-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 2002, originally published as *Cohomologie galoisienne* (1965).

[T] J.-P. Tignol, *Classification of wild cyclic field extensions and division algebras of prime degree over a Henselian field*, Proceedings of the International Conference on Algebra, Part 2 (Novosibirsk, 1989), Contemp. Math., vol. 131, Am. Math. Soc., 1992, pp. 491–508.

[W] A.R. Wadsworth, *Valuation theory on finite dimensional division algebras*, Valuation theory and its applications, Vol. I (Saskatoon, SK, 1999), Fields Inst. Commun., vol. 32, Am. Math. Soc., Providence, RI, 2002, pp. 385–449.

Lifting of Coefficients for Chow Motives of Quadrics

Olivier Haution

Summary We prove that the natural functor from the category of Chow motives of smooth projective quadrics with integral coefficients to the category with coefficients modulo 2 induces a bijection on the isomorphism classes of objects.

1 Introduction

Alexander Vishik has given a description of the Chow motives of quadrics with integral coefficients in [6]. It uses much subtler methods than the ones used to give a similar description with coefficients in $\mathbb{Z}/2$, found for example in [2], but the description obtained is the same ([2, Theorems 93.1 and 94.1]). The result presented here allows one to recover Vishik's results from the modulo 2 description.

In order to state the main result, we first define the categories involved. Let Λ be a commutative ring. We write $\mathscr{Q}_F$ for the class of smooth projective quadrics over a field F. We consider the additive category $\mathscr{C}(\mathscr{Q}_F,\Lambda)$, where objects are (coproducts of) quadrics in $\mathscr{Q}_F$ and if X,Y are two such quadrics, $\mathrm{Hom}(X,Y)$ is the group of correspondences of degree 0, namely $\mathrm{CH}_{\dim X}(X\times Y,\Lambda)$. We write $\mathscr{C}\mathscr{M}(\mathscr{Q}_F,\Lambda)$ for the idempotent completion of $\mathscr{C}(\mathscr{Q}_F,\Lambda)$. This is the category of graded Chow motives of smooth projective quadrics with coefficients in Λ. If $(X,\rho),(Y,\sigma)$ are two such motives then we have:

$$\mathrm{Hom}((X,\rho),(Y,\sigma)) = \sigma\circ \mathrm{CH}_{\dim X}(X\times Y,\Lambda)\circ\rho.$$

Olivier Haution
Institut de mathématiques de Jussieu, 175 rue du Chevaleret 75013 Paris, France,
e-mail: olivier.haution@gmail.com

2010 Mathematics subject classification. 11E04, 14C25.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_14,

We will prove the following:

Theorem 1. *The functor* $\mathscr{CM}(\mathscr{Q}_F,\mathbb{Z}) \to \mathscr{CM}(\mathscr{Q}_F,\mathbb{Z}/2)$ *induces a bijection on the isomorphism classes of objects.*

The proof mostly relies on the low rank of the homogeneous components of the Chow groups of quadrics when passing to a splitting field. These components are almost always indecomposable if we take into account the Galois action. The only exception is the component of rank 2 when the discriminant is trivial but in this case the Galois action on the Chow group is trivial which allows the proof to go through.

It seems that Theorem 1 may be deduced from [6] (see [3, Theorem E.11.2, p. 254]). Here we try to give a more direct and self-contained proof.

2 Chow Groups of Quadrics

We first recall some facts and fix the notations that we will use.

If L/F is a field extension, and S is a scheme over F, we write S_L for the scheme $S \times_{\mathrm{Spec}(F)} \mathrm{Spec}(L)$. Similarly, for an F-vector space U, we write U_L for $U \otimes_F L$, and for a cycle $x \in \mathrm{CH}(S)$, the element $x_L \in \mathrm{CH}(S_L)$ is the pull-back of x along the flat morphism $S_L \to S$.

We say that a cycle in $\mathrm{CH}(S_L)$ is F*-rational* (or simply *rational* when no confusion seems possible) if it can be written as x_L for some cycle $x \in \mathrm{CH}(S)$, i.e., if it belongs to the image of the pull-back homomorphism $\mathrm{CH}(S) \to \mathrm{CH}(S_L)$.

Let F be a field and φ be a nondegenerate quadratic form on an F-vector space V of dimension $D+2$. The associated projective quadric X is smooth of dimension $D = 2d$ or $2d+1$. Let L/F be a splitting extension for X, i.e., a field extension such that V_L has a totally isotropic subspace of dimension $d+1$. We write h^i, l_i for the usual basis of $\mathrm{CH}(X_L)$, where $0 \leq i \leq d$. The class h is the pull-back of the hyperplane class of the projective space of V_L, the class l_i is the class of the projectivisation of a totally isotropic subspace of V_L of dimension $i+1$.

If D is even, then $\mathrm{CH}_d(X_L)$ is freely generated by h^d and l_d. In this case, there are exactly two classes of maximal totally isotropic spaces, l_d and $l_d{}'$. They correspond to spaces exchanged by a reflection and verify the relation $l_d + l_d{}' = h^d$.

The group $\mathrm{Aut}(L/F)$ acts on $\mathrm{CH}(X_L)$. It acts trivially on the ith homogeneous component of $\mathrm{CH}(X_L)$, as long as $2i \neq D$.

See [2] for proofs of all these facts.

In the next proposition, X is a smooth projective quadric of dimension $D = 2d$ associated with a quadratic space (V,φ) over a field F, L/F is a splitting extension for X, and $\operatorname{disc} X$ is the discriminant algebra of φ.

Proposition 2. *Under the natural* $\mathrm{Aut}(L/F)$*-actions, the pair* $\{l_d, l_d{}'\}$ *can be identified with the connected components of* $\mathrm{Spec}(\operatorname{disc} X \otimes L)$.

Proof. We consider the scheme $G(\varphi)$ of maximal totally isotropic subspaces of V, i.e., the grassmannian variety of isotropic $(d+1)$-dimensional subspaces of V. The scheme $G(\varphi)_L$ has two connected components exchanged by any reflection of the quadratic space (V,φ). There is a faithfully flat morphism $G(\varphi) \to \mathrm{Spec}(\mathrm{disc}\, X)$ (see [2, §85, p. 357]), hence the connected components of $G(\varphi)_L$ are in correspondence with those of $\mathrm{Spec}(\mathrm{disc}\, X \otimes L)$, in a way respecting the natural $\mathrm{Aut}(L/F)$-actions.

Now two maximal totally isotropic subspaces lie in the same connected component of $G(\varphi)_L$ if and only if the corresponding d-dimensional closed subvarieties of the quadric X_L are rationally equivalent (see [2, §86, p. 358]). Therefore, the pair $\{l_d, l_d{}'\}$ is $\mathrm{Aut}(L/F)$-isomorphic to the pair of connected components of $G(\varphi)_L$. The statement follows. □

3 Lifting of Coefficients

We now give a useful characterization of rational cycles (Proposition 7). The proof will rely on the following theorem from [5, Proposition 9]:

Theorem 3 (Rost's nilpotence for quadrics). *Let X be a smooth projective quadric over a field F, and let $\alpha \in \mathrm{End}_{\mathscr{C}\mathscr{M}(\mathscr{Q}_F,\Lambda)}(X)$. If $\alpha_L \in \mathrm{CH}(X_L^2)$ vanishes for some field extension L/F then α is nilpotent.*

We will use the following classical corollaries:

Corollary 4 ([2, Corollary 92.5]). *Let X be a smooth projective quadric over a field F and L/F a field extension. Let π a projector in $\mathrm{End}_{\mathscr{C}\mathscr{M}(\mathscr{Q}_L,\Lambda)}(X_L)$ that is the restriction of some element in $\mathrm{End}_{\mathscr{C}\mathscr{M}(\mathscr{Q}_F,\Lambda)}(X)$. Then there exist a projector φ in $\mathrm{End}_{\mathscr{C}\mathscr{M}(\mathscr{Q}_F,\Lambda)}(X)$ such that $\varphi_L = \pi$.*

Corollary 5 ([2, Corollary 92.7]). *Let $f\colon (X,\rho) \to (Y,\sigma)$ be a morphism in the category $\mathscr{C}\mathscr{M}(\mathscr{Q}_F,\Lambda)$. If f_L is an isomorphism for some field extension L/F then f is an isomorphism.*

Proposition 6. *For any $n \geq 1$, the functor $\mathscr{C}\mathscr{M}(\mathscr{Q}_F,\mathbb{Z}/2^n) \to \mathscr{C}\mathscr{M}(\mathscr{Q}_F,\mathbb{Z}/2)$ is bijective on the isomorphism classes of objects.*

Proof. We are clearly in the situation $(\star)$ of [7, Sect. 2, p. 587] for the obvious functor $\mathscr{C}(\mathscr{Q}_F,\mathbb{Z}/2^n) \to \mathscr{C}(\mathscr{Q}_F,\mathbb{Z}/2)$. The statement then follows from [7, Propositions 2.5 and 2.2] (see also [4, Corollary 2.7]). □

Any smooth projective quadric admits a (noncanonical) finite Galois splitting extension, of degree a power of 2. This will be used together with the following proposition when we will need to prove that a given cycle with integral coefficients (and defined over some extension of the base field) is rational.

Proposition 7. *Let $X,Y \in \mathscr{Q}_F$ and L/F be a splitting Galois extension of degree m for X and Y. A correspondence in $\mathrm{CH}((X\times Y)_L,\mathbb{Z})$ is rational if and only if it is invariant under the group $\mathrm{Gal}(L/F)$ and its image in $\mathrm{CH}((X\times Y)_L,\mathbb{Z}/m)$ is rational.*

Proof. We write Z for $X \times Y$. We first prove that if x is a $\mathrm{Gal}(L/F)$-invariant cycle in $\mathrm{CH}(Z_L)$ then $[L:F]\cdot x$ is rational.

Let $\tau\colon L \to \bar{F}$ be a separable closure so that we have an $\bar{F}$-isomorphism $L\otimes\bar{F} \to \bar{F}\times\cdots\times\bar{F}$ given by $u\otimes 1 \mapsto (\tau\circ\gamma(u))_{\gamma\in\mathrm{Gal}(L/F)}$.

We have a cartesian square:

$$\begin{tikzcd} Z_L & Z_{L\otimes\bar{F}} \arrow[l] \arrow[d] \\ Z \arrow[from=u] & Z_{\bar{F}} \arrow[l] \end{tikzcd}$$

It follows that we have a commutative diagram of pull-backs and push-forward:

$$\begin{tikzcd} \mathrm{CH}(Z_L) \arrow[r] \arrow[d] & \mathrm{CH}(Z_{L\otimes\bar{F}}) \arrow[d] \\ \mathrm{CH}(Z) \arrow[r] & \mathrm{CH}(Z_{\bar{F}}) \end{tikzcd}$$

The top map followed by the map on the right is:

$$x \mapsto \sum_{\gamma\in\mathrm{Gal}(L/F)} t^*({}^{\gamma}x)$$

where $t: Z_{\bar{F}} \to Z_L$ is the map induced by τ. Using the commutativity of the diagram and the injectivity of t^*, we see that the composite $\mathrm{CH}(Z_L) \to \mathrm{CH}(Z) \to \mathrm{CH}(Z_L)$ maps x to $\sum {}^{\gamma}x$, where γ runs in $\mathrm{Gal}(L/F)$. The claim follows.

Now suppose that u is a cycle in $\mathrm{CH}(Z_L,\mathbb{Z})$ invariant under $\mathrm{Gal}(L/F)$, and that its image in $\mathrm{CH}(Z_L,\mathbb{Z}/m)$ is rational. We can find a rational cycle v in $\mathrm{CH}(Z_L,\mathbb{Z})$ and a cycle δ in $\mathrm{CH}(Z_L,\mathbb{Z})$ such that $m\delta = v-u$. As $\mathrm{CH}(Z_L,\mathbb{Z})$ is torsion-free, δ is invariant under $\mathrm{Gal}(L/F)$. The first claim ensures that $v-u$ is rational, hence u is rational, and we have proven the proposition. $\square$

Let us remark that if $X \in \mathscr{Q}_F$, L/F is a splitting extension, and $2i < \dim X$ then $2l_i = h^{\dim X - i} \in \mathrm{CH}(X_L)$ is always rational. It follows that $2\,\mathrm{CH}_i(X_L)$ consists of rational cycles when $2i \neq \dim X$.

4 Surjectivity in the Main Theorem

Proposition 8. *The functor $\mathscr{CM}(\mathscr{Q}_F,\mathbb{Z}) \to \mathscr{CM}(\mathscr{Q}_F,\mathbb{Z}/2)$ is surjective on the isomorphism classes of objects.*

Proof. Let $(X,\pi) \in \mathscr{CM}(\mathscr{Q}_F,\mathbb{Z}/2)$ and L/F a finite splitting Galois extension for X of degree 2^n. By Proposition 6, we can lift the isomorphism class of (X,π) to the isomorphism class of some $(X,\tau) \in \mathscr{CM}(\mathscr{Q}_F,\mathbb{Z}/2^n)$.

Assume that we have found a $\mathrm{Gal}(L/F)$-invariant projector ρ in $\mathrm{CH}_{\dim X}(X \times X)_L$ which gives modulo 2^n the projector τ_L. By Proposition 7, ρ is a rational cycle, and Corollary 4 provides a projector p such that $\rho = p_L$. Write $\tilde{p} \in \mathrm{CH}(X \times X, \mathbb{Z}/2^n)$ for the image of p. Consider the morphism $(X, \tau) \to (X, \tilde{p})$ given by $\tilde{p} \circ \tau$. Since $\tilde{p}_L = \rho \mod 2^n = \tau_L$, this morphism becomes an isomorphism (the identity) after extending scalars to L hence is an isomorphism by Corollary 5. It follows that the isomorphism class of $(X, p) \in \mathscr{CM}(\mathscr{Q}_F, \mathbb{Z})$ is a lifting of the class of $(X, \tau) \in \mathscr{CM}(\mathscr{Q}_F, \mathbb{Z}/2^n)$.

We now build the projector ρ. For any commutative ring Λ, projectors in $\mathrm{CH}((X \times X)_L, \Lambda)$ are in bijective correspondence with ordered pairs of subgroups of $\mathrm{CH}(X_L, \Lambda)$ which form a direct sum decomposition. This bijection is compatible with the natural $\mathrm{Gal}(L/F)$-actions. A projector is of degree 0 if and only if the two summands in the associated decomposition are graded subgroups of $\mathrm{CH}(X_L, \Lambda)$.

When $\dim X$ is odd or when $\mathrm{disc}\, X$ is a field, each homogeneous component of $\mathrm{CH}(X_L, \Lambda)$ is $\mathrm{Gal}(L/F)$-indecomposable, hence $\mathrm{Gal}(L/F)$-invariant projectors of degree 0 of $\mathrm{CH}(X_L, \Lambda)$ are in one-to-one correspondence with the subsets of $\{0, \ldots, \dim X\}$. It follows that we can lift any $\mathrm{Gal}(L/F)$-invariant projector of degree 0 with coefficients in $\mathbb{Z}/2^n$ to an integral $\mathrm{Gal}(L/F)$-invariant projector of degree 0.

When $\dim X$ is even and $\mathrm{disc}\, X$ is trivial, $\mathrm{CH}_i(X_L, \Lambda)$ is indecomposable if $2i \neq 2d_X = \dim X$. The group $\mathrm{Gal}(L/F)$ acts trivially on $\mathrm{CH}_{d_X}(X_L, \Lambda)$. If the rank of the restriction of $(\tau_L)_*$ to $\mathrm{CH}_{d_X}(X_L, \mathbb{Z}/2^n)$ is 0 or 2, the projector τ_L clearly lifts to a $\mathrm{Gal}(L/F)$-invariant projector in $\mathrm{CH}_{\dim X}(X \times X)_L$.

The last case is when the rank is 1. We fix a decomposition of the group $\mathrm{CH}_{d_X}(X_L, \mathbb{Z})$ into the direct sum of rank 1 summands. Any such decomposition of $\mathrm{CH}_{d_X}(X_L, \Lambda)$ is then given by some element of $SL_2(\Lambda)$. The next lemma ensures that we can lift any element of $SL_2(\mathbb{Z}/2^n)$ to $SL_2(\mathbb{Z})$, thus that τ_L lifts to a projector with integral coefficients. It remains to notice that $\mathrm{Gal}(L/F)$ acts trivially on $\mathrm{CH}_{\dim X}(X \times X)_L$ since $\mathrm{disc}\, X$ is trivial, to conclude the proof. □

Lemma 9 ([4, Lemma 2.14]). *For any positive integers k and p, the reduction homomorphism $SL_k(\mathbb{Z}) \to SL_k(\mathbb{Z}/p)$ is surjective.*

Proof. As $\mathbb{Z}/p$ is a semilocal commutative ring, it follows from [1, Corollary 9.3, Chap. V, p. 267], applied with $A = \mathbb{Z}$ and $\underline{q} = p\mathbb{Z}$, that any matrix in $SL_k(\mathbb{Z}/p)$ is the image modulo p of a product of elementary matrices with integral coefficients. Such a product in particular belongs to $SL_k(\mathbb{Z})$, as required. □

5 Injectivity in the Main Theorem

In order to prove injectivity in Theorem 1, we may assume that we are given two motives $(X, \rho), (Y, \sigma)$ in $\mathscr{CM}(\mathscr{Q}_F, \mathbb{Z})$ and an isomorphism between their images in $\mathscr{CM}(\mathscr{Q}_F, \mathbb{Z}/2)$. We will build an isomorphism with integral coefficients between the two motives (which will not, in general, be an integral lifting of the original isomorphism with finite coefficients).

We fix a finite Galois splitting extension L/F for X and Y of degree 2^n. Using Proposition 6 we may assume that there exists an isomorphism α between (X,ρ) and (Y,σ) in $\mathscr{CM}(\mathscr{Q}_F,\mathbb{Z}/2^n)$. By Proposition 7 and Corollary 5, it is enough to build an isomorphism $(X_L,\rho_L) \to (Y_L,\sigma_L)$ which reduces to a rational correspondence modulo 2^n and which is equivariant under $\mathrm{Gal}(L/F)$.

Let d_X be such that $\dim X = 2d_X$ or $2d_X+1$ and d_Y defined similarly for Y. Let $r(X,\rho)$ be the rank of $\mathrm{CH}_{d_X}(X_L) \cap \mathrm{im}\,(\rho_L)_*$ if $\dim X$ is even and $r(X,\rho)=0$ if $\dim X$ is odd. We define $r(Y,\sigma)$ in a similar fashion. We will distinguish cases using these integers.

A basis of $\mathrm{CH}(X_L) \cap \mathrm{im}\,(\rho_L)_*$ gives an isomorphism of (X_L,ρ_L) with twists of Tate motives, thus choosing bases for the groups $\mathrm{CH}(X_L) \cap \mathrm{im}\,(\rho_L)_*$ and $\mathrm{CH}(Y_L) \cap \mathrm{im}\,(\sigma_L)_*$, we can see morphisms between the two motives as matrices.

We fix a basis (e_i) of $\mathrm{CH}(X_L) \cap \mathrm{im}\,(\rho_L)_*$ as follows: we choose $e_i \in \mathrm{CH}_i(X_L)$ among the cycles $h^{\dim X - i}, l_i$ for $2i \neq \dim X$. We are done when $r(X,\rho)=0$.

If $r(X,\rho)=2$ we complete the basis with $e_{d_X} = l_{d_X}, e'_{d_X} = l'_{d_X} \in \mathrm{CH}_{d_X}(X_L)$.

If $r(X,\rho)=1$ we choose a generator e_{d_X} of $\mathrm{CH}_{d_X}(X_L) \cap \mathrm{im}\,(\rho_L)_*$ to complete the basis.

We choose a basis (f_i) for $\mathrm{CH}(Y_L) \cap \mathrm{im}\,(\sigma_L)_*$ in a similar way.

If we write $\tilde{\rho}$ and $\tilde{\sigma}$ for the reduction modulo 2^n of ρ and σ, these bases reduce to bases $(\tilde{e}_i)$ of $\mathrm{CH}(X_L,\mathbb{Z}/2^n) \cap \mathrm{im}(\tilde{\rho}_L)_*$ and $(\tilde{f}_i)$ of $\mathrm{CH}(Y_L,\mathbb{Z}/2^n) \cap \mathrm{im}(\tilde{\sigma}_L)_*$. In these homogeneous bases the matrix of a correspondence of degree 0 is diagonal by blocks. The sizes of the blocks are the ranks of the homogeneous components of $\mathrm{im}\,(\rho_L)_*$.

Lemma 10. *If* $r(X,\rho)=1$ *then* $\mathrm{disc}\,X$ *is trivial.*

Proof. Assume $\mathrm{disc}\,X$ is not trivial. The correspondence ρ induces a projection of $\mathrm{CH}_{d_X}(X_L)$ which is equivariant under the action of $\mathrm{Gal}(L/F)$. But $\mathrm{CH}_{d_X}(X_L)$ is indecomposable as a $\mathrm{Gal}(L/F)$-module. It follows that $(\rho_L)_*$ is either the identity or 0 when restricted to $\mathrm{CH}_{d_X}(X_L)$, hence $r(X,\rho) \neq 1$. □

Corollary 11. *If* $r(X,\rho) \neq 2$ *then* $\mathrm{Gal}(L/F)$ *acts trivially on* $\mathrm{im}\,(\rho_L)_*$.

Lemma 12. *If* $r(X,\rho)=2$ *then* $r(Y,\rho)=2$*,* $\dim Y = \dim X$ *and* $\mathrm{disc}\,Y = \mathrm{disc}\,X$.

Proof. As the isomorphism $(\alpha_L)_*$ is graded, the d_X-th homogeneous component of $\mathrm{im}(\alpha_L)_*$ has rank 2. This image is a subgroup of the Chow group with coefficients in $\mathbb{Z}/2^n$ of a split quadric, thus the only possibility is that $\dim Y$ is even, $d_X = d_Y$ and $r(Y,\sigma)=2$.

The isomorphism $(\alpha_L)_*$ is equivariant under the action of $\mathrm{Gal}(L/F)$. It follows that an element of the group $\mathrm{Gal}(L/F)$ acts trivially on $\mathrm{CH}(X_L,\mathbb{Z}/2^n)$ if and only if it acts trivially on $\mathrm{CH}(Y_L,\mathbb{Z}/2^n)$. But such an element acts trivially on $\mathrm{CH}(X_L,\mathbb{Z}/2^n)$ (respectively, $\mathrm{CH}(Y_L,\mathbb{Z}/2^n)$) if and only if it acts trivially on the pair of integral cycles $\{l_{d_X}, {l_{d_X}}'\} \subset \mathrm{CH}(X_L)$ (respectively, $\{l_{d_Y}, {l_{d_Y}}'\} \subset \mathrm{CH}(Y_L)$). Therefore, the pair of integral cycles $\{l_{d_X}, {l_{d_X}}'\}$ is $\mathrm{Gal}(L/F)$-isomorphic to the pair $\{l_{d_Y}, {l_{d_Y}}'\}$. By proposition 2, we have a $\mathrm{Gal}(L/F)$-isomorphism between the split étale algebras $\mathrm{disc}\,X \otimes L$ and $\mathrm{disc}\,Y \otimes L$. Hence, $\mathrm{disc}\,X$ and $\mathrm{disc}\,Y$ correspond to the same cocycle in $H^1(\mathrm{Gal}(L/F),\mathbb{Z}/2)$, thus are isomorphic. □

We now proceed with the proof of the injectivity.

Let us first assume that $r(X,\rho) \neq 2$. Then $r(Y,\sigma) \neq 2$ by the preceding lemma. By Corollary 11 the group $\mathrm{Gal}(L/F)$ acts trivially on $\mathrm{im}\,(\rho_L)_*$ and on $\mathrm{im}\,(\sigma_L)_*$, therefore any morphism $(X_L,\rho_L) \to (Y_L,\sigma_L)$ is defined by a cycle invariant under $\mathrm{Gal}(L/F)$.

Because the isomorphism α_L is of degree 0, its matrix in our graded bases of the modulo 2^n Chow groups is diagonal. Let $\lambda_i \in (\mathbb{Z}/2^n)^\times$ be the coefficients in the diagonal so that we have $(\alpha_L)_*(\tilde{e}_i) = \lambda_i \tilde{f}_i$ for all i such that $\mathrm{CH}_i(X_L) \cap \mathrm{im}\,(\rho_L)_* \neq \emptyset$.

If $r(X,\rho) = 1$ then λ_{d_X} is defined and we consider the cycle $\beta = (\lambda_{d_X})^{-1}\alpha_L$. If $r(X,\rho) = 0$, we just put $\beta = \alpha_L$.

Now we take $k_i \in \mathbb{Z}/2^n$ such that $\lambda_i^{-1} = 2k_i + 1$. Let $\Delta \in \mathrm{End}(X_L,\tilde{\rho}_L)$ be the identity morphism. We consider the rational cycle

$$\gamma = \Delta + 2\sum k_i \tilde{e}_i \times \tilde{e}_{\dim X - i},$$

where the sum is taken over all i such that $\mathrm{CH}_i(X_L) \subset \mathrm{im}\,(\rho_L)_*$ (which implies in case $r(X,\rho) = 1$ that we do not take $i = d_X$). The composite $\beta \circ \gamma$ is rational, and its matrix in our bases is the identity matrix. This correspondence lifts to an isomorphism with integral coefficients $(X_L,\rho_L) \to (Y_L,\sigma_L)$.

Next assume that $r(X,\rho) = 2$. Then we have $\dim X = \dim Y$, $r(Y,\sigma) = 2$, and $\mathrm{disc}\, X = \mathrm{disc}\, Y$ by Lemma 12. The matrix of $(\alpha_L)_*$ is diagonal by blocks:

$$\begin{pmatrix} \nu_{i_1} & & & & & & \\ & \ddots & & & & & \\ & & \nu_{i_r} & & & & \\ & & & B & & & \\ & & & & \nu_{i_{r+1}} & & \\ & & & & & \ddots & \\ & & & & & & \nu_{i_p} \end{pmatrix},$$

where $\nu_i \in (\mathbb{Z}/2^n)^\times$ and $B \in GL_2(\mathbb{Z}/2^n)$.

Now if $\mathrm{disc}\, X = \mathrm{disc}\, Y$ is a field, there is an element in $\mathrm{Gal}(L/F)$ that simultaneously exchanges the cycles in the bases $\{l_{d_X}, l_{d_X}'\}$ of $\mathrm{CH}_{d_X}(X_L,\mathbb{Z}/2^n)$ and $\{l_{d_Y}, l_{d_Y}'\}$ of $\mathrm{CH}_{d_Y}(Y_L,\mathbb{Z}/2^n)$. It follows that we may write B as:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

for some a and b in $\mathbb{Z}/2^n$. The determinant of B is $(a+b)(a-b) \in (\mathbb{Z}/2^n)^\times$, hence $(a-b) \in (\mathbb{Z}/2^n)^\times$. Thus, we may replace α_L by $(a-b)^{-1}\alpha_L$ and assume that $a = b+1$.

As before we may write $\nu_i^{-1} = 2k_i + 1$ and replace α_L by the rational cycle:

$$\alpha_L \circ \left(\Delta + 2\sum k_i \tilde{e}_i \times \tilde{e}_{\dim X - i}\right)$$

the sum being taken over all i such that $\mathrm{CH}_i(X_L) \cap \mathrm{im}(\rho_L)_* \neq \emptyset$ and $i \neq d_X$. Therefore, we may assume that $\nu_i = 1$ for all i and that we have a matrix of the shape (I_r being the identity block of size r):

$$\begin{pmatrix} I_s & & & 0 \\ & a{+}1 & a & \\ & a & a{+}1 & \\ 0 & & & I_t \end{pmatrix}.$$

The matrix of the rational cycle $h^{d_X} \times h^{d_Y} \in \mathrm{CH}((X \times Y)_L, \mathbb{Z}/2^n)$ is:

$$\begin{pmatrix} 0 & & & 0 \\ & 1 & 1 & \\ & 1 & 1 & \\ 0 & & & 0 \end{pmatrix}$$

Now $\alpha_L - a(h^{d_X} \times h^{d_Y})$ is rational and its matrix is the identity. This cycle is invariant under $\mathrm{Gal}(L/F)$ and lifts to an isomorphism $(X_L, \rho_L) \to (Y_L, \sigma_L)$.

It remains to treat the case when $\operatorname{disc} X$ is trivial. In this case the group $\mathrm{Gal}(L/F)$ acts trivially on $\mathrm{CH}(X_L)$ (and on $\mathrm{CH}(Y_L)$ as $\operatorname{disc} Y$ is also trivial). As before, composing with a rational cycle, we may assume that $\nu_i = 1$ for all i. We write $\det B^{-1} = 2k + 1$.

The cycle $\Delta + k(h^{d_X} \times h^{d_X}) \in \mathrm{End}(X_L, \tilde{\rho}_L)$ is rational and its matrix in our basis is:

$$\begin{pmatrix} I_p & & & 0 \\ & 1{+}k & k & \\ & k & 1{+}k & \\ 0 & & & I_r \end{pmatrix}.$$

We see that the determinant of this matrix is $1 + 2k$. Therefore, the composite $\alpha_L \circ (\Delta + k(h^{d_X} \times h^{d_X}))$ has determinant 1. We use Lemma 9 to conclude, which completes the proof of Theorem 1.

Acknowledgements This work is part of my PhD thesis at the University of Paris 6 under the direction of Nikita Karpenko. I am very grateful to him for his useful suggestions.

References

1. Bass H., *Algebraic K-theory* (1968), W. A. Benjamin, Inc., New York-Amsterdam.
2. Elman R., Karpenko N., Merkurjev A., *Algebraic and Geometric Theory of Quadratic Forms* (2008), American Mathematical Society Colloquium Publications, vol 56.
3. Kahn B., *Formes Quadratiques sur un Corps*, Cours spécialisés **15**, Société mathématique de France, 2008.
4. Petrov V., Semenov N., Zainoulline K., *J-invariant of Linear Algebraic Groups* (2008), Ann. Sci. Éc. Norm. Supér. (4), 41(6):1023–1053.

5. Rost M., *The Motive of a Pfister Form*, preprint (1998), available at http://www.math.uni-bielefeld.de/~rost/motive.html
6. Vishik A., *Motives of Quadrics with Applications to the Theory of Quadratic Forms* (2004) in Geometric methods in the algebraic theory of quadratic forms, Lect. Notes in Math. 1835, Springer, Berlin, 25–101.
7. Vishik A., Yagita N., *Algebraic Cobordisms of a Pfister Quadric* (2007), J. Lond. Math. Soc. (2) 76 (2007) 586–604.

Upper Motives of Outer Algebraic Groups

Nikita A. Karpenko

Summary Let G be a semisimple affine algebraic group over a field F. Assuming that G becomes of inner type over some finite field extension of F of degree a power of a prime p, we investigate the structure of the Chow motives with coefficients in a finite field of characteristic p of the projective G-homogeneous varieties. The complete motivic decomposition of any such variety contains one specific summand, which is the most understandable among the others and which we call the *upper* indecomposable summand of the variety. We show that every indecomposable motivic summand of any projective G-homogeneous variety is isomorphic to a shift of the upper summand of some (other) projective G-homogeneous variety. This result is already known (and has applications) in the case of G of inner type and is new for G of outer type (over F).

1 Introduction

We fix an arbitrary base field F. Besides that, we fix a finite field $\mathbb{F}$ and we consider the Grothendieck Chow motives over F with coefficients in $\mathbb{F}$. These are the objects of the category $\mathrm{CM}(F, \mathbb{F})$, defined as in [4].

Let G be a semisimple affine algebraic group over F. According to [3, Corollary 35(4)] (see also Corollary 2.2 here), the motive of any projective G-homogeneous variety decomposes (in a unique way) into a finite direct sum of indecomposable motives. One would like to describe the indecomposable motives that appear this way. In this paper we do it under certain assumption on G formulated in terms of the (unique up to F-isomorphism) minimal field extension E/F such that the group G_E is of inner type: the degree of E/F is assumed to be a power of p, where $p = \mathrm{char}\,\mathbb{F}$.

Nikita A. Karpenko
UPMC Univ Paris 06, Institut de Mathématiques de Jussieu, Paris, France,
e-mail: karpenko@math.jussieu.fr

2010 Mathematics subject classification. 14L17, 14C25.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_15,

Note that this has already been done in [5] in the case when $E = F$, that is, when G itself is of inner type. Therefore, though the inner case is formally included in the present paper, we concentrate here on the special effects of the outer case. This remark explains the choice of the title.

Note that the extension E/F is galois. Actually, we do not use the minimality condition on the extension E/F in the paper. Therefore, E/F could be any finite p-primary galois field extension with G_E of inner type. However, it is reasonable to keep the minimality condition at least for the sake of the definition of the *set of the upper motives* of G which we give now.

For any intermediate field L of the extension E/F and any projective G_L-homogeneous variety Y, we consider the upper (see [5, Definition 2.10]) indecomposable summand M_Y of the motive $M(Y) \in \mathrm{CM}(F,\mathbb{F})$ of Y (considered as an F-variety at this point). By definition, this is the (unique up to isomorphism) indecomposable summand of $M(Y)$ with nonzero 0-codimensional Chow group. The set of the isomorphism classes of the motives M_Y for all L and Y is called the set of *upper motives* of the algebraic group G.

The summand M_Y is definitely the "easiest" indecomposable summand of $M(Y)$ over which we have the best control. For instance, the motive M_Y is isomorphic to the motive $M_{Y'}$ for another projective homogeneous (not necessarily under an action of the same group G) variety Y' if and only if there exist multiplicity 1 correspondences $Y \rightsquigarrow Y'$ and $Y' \rightsquigarrow Y$, [5, Corollary 2.15]. Here a *correspondence* $Y \rightsquigarrow Y'$ is an element of the $(\dim Y)$-dimensional Chow group of $Y \times_F Y'$ with coefficients in $\mathbb{F}$; its *multiplicity* is its image under the push-forward to the $(\dim Y)$-dimensional Chow group of Y identified with $\mathbb{F}$.

One more nice property of M_Y (which will be used in the proof of Theorem 1.1) is an easy control over the condition that M_Y is a summand of an arbitrary motive M: by [5, Lemma 2.14], this condition holds if and only if there exist morphisms $\alpha : M(Y) \to M$ and $\beta : M \to M(Y)$ such that the correspondence $\beta \circ \alpha$ is of multiplicity 1.

We are going to claim that the complete motivic decomposition of any projective G-homogeneous variety X consists of shifts of upper motives of G. In fact, the information we have is a bit more precise:

Theorem 1.1. *For F, G, E, and X as earlier, the complete motivic decomposition of X consists of shifts of upper motives of the algebraic group G. More precisely, any indecomposable summand of the motive of X is isomorphic a shift of an upper motive M_Y such that the Tits index of G over the function field of the variety Y contains the Tits index of G over the function field of X.*

Remark 1.2. Theorem 1.1 fails if the degree of the extension E/F is divisible by a prime different from p (see Example 3.3).

The proof of Theorem 1.1 is given in Sect. 4. Before this, we get some preparatory results which are also of independent interest. In Sect. 2, we prove the nilpotence principle for the quasi-homogeneous varieties. In Sect. 3, we establish some properties of a motivic corestriction functor.

By a *sum* of motives we always mean the *direct* sum; a *summand* is a *direct* summand; a direct sum decomposition is called *complete* if the summands are indecomposable.

2 Nilpotence Principle for Quasi-homogeneous Varieties

Let us consider the category $\mathrm{CM}(F,\Lambda)$ of Grothendieck Chow motives over a field F with coefficients in an *arbitrary* associative commutative unital ring Λ.

We say that a smooth complete F-variety X satisfies the nilpotence principle if for any Λ and any field extension K/F, the kernel of the change of field homomorphism

$$\mathrm{End}\,(M(X)) \to \mathrm{End}\,(M(X_K))$$

consists of nilpotents, where $M(X)$ stands for the motive of X in $\mathrm{CM}(F,\Lambda)$.

We say that an F-variety X is *quasi-homogeneous* if each connected component X^0 of X has the following property: there exists a finite separable field extension L/F, a semisimple affine algebraic group G over L, and a projective G-homogeneous variety Y such that Y, considered as an F-variety via the composition $Y \to \mathrm{Spec}\,L \to \mathrm{Spec}\,F$, is isomorphic to X^0. (Note that the algebraic group G need not be defined over F in this definition.)

We note that any variety that is *projective quasi-homogeneous* in the sense of [1, Sect. 4] is also quasi-homogeneous in the above sense. The following statement generalizes [2, Theorem 8.2] (see also [1, Theorem 5.1]) and [3, Theorem 25]:

Theorem 2.1. *Every quasi-homogeneous variety satisfies the nilpotence principle.*

Proof. By [4, Theorem 92.4] it suffices to show that the quasi-homogeneous varieties form a *tractable class*. We first recall the definition of a tractable class $\mathscr{C}$ (over F). This is a disjoint union of classes $\mathscr{C}_K$ of smooth complete K-varieties, where K runs over *all* field extensions of F, having the following properties:

(1) If Y_1 and Y_2 are in $\mathscr{C}_K$ for some K, then the disjoint union of Y_1 and Y_2 is also in $\mathscr{C}_K$;
(2) If Y is in $\mathscr{C}_K$ for some K, then each component of Y is also in $\mathscr{C}_K$;
(3) If Y is in $\mathscr{C}_K$ for some K, then for every field extension K'/K the K'-variety $Y_{K'}$ is in $\mathscr{C}_{K'}$;
(4) If Y is in $\mathscr{C}_K$ for some K, Y is irreducible, $\dim Y > 0$, and $Y(K) \neq \emptyset$, then $\mathscr{C}_K$ contains a (not necessarily connected) variety Y_0 such that $\dim Y_0 < \dim Y$ and $M(Y) \simeq M(Y_0)$ in $\mathrm{CM}(K,\Lambda)$ (for any Λ or, equivalently, for $\Lambda = \mathbb{Z}$).

Let us define a class $\mathscr{C}$ as follows. For every field extension K/F, $\mathscr{C}_K$ is the class of all quasi-homogeneous K-varieties.

We claim that the class $\mathscr{C}$ is tractable. Indeed, the properties (1)–(3) are trivial and the property (4) is [2, Theorem 7.2]. $\square$

We turn back to the case where the coefficient ring Λ is a finite field $\mathbb{F}$.

Corollary 2.2. *Let $M \in \mathrm{CM}(F,\mathbb{F})$ be a summand of the motive of a quasi-homogeneous variety. Then M decomposes in a finite direct sum of indecomposable motives; moreover, such a decomposition is unique (up to a permutation of the summands).*

Proof. Any quasi-homogeneous variety is *geometrically cellular*. In particular, it is *geometrically split* in the sense of [5, Sect. 2a]. Finally, by Theorem 2.1, it satisfies the nilpotence principle. The statement to be proved follows now by [5, Corollary 2.6]. □

3 Corestriction of Scalars for Motives

As in the previous section, let Λ be an arbitrary (coefficient) ring. We write Ch for the Chow group with coefficients in Λ. Let $\mathrm{C}(F,\Lambda)$ be the category whose objects are pairs (X,i), where X is a smooth complete equidimensional F-variety and i is an integer. A morphism $(X,i) \to (Y,j)$ in this category is an element of the Chow group $\mathrm{Ch}_{\dim X+i-j}(X \times Y)$ (and the composition is the usual composition of correspondences). The category $\mathrm{C}(F,\Lambda)$ is preadditive. Taking first the additive completion of it, and taking then the idempotent completion of the resulting category, one gets the category of motives $\mathrm{CM}(F,\Lambda)$, cf. [4, Sects. 63 and 64].

Let L/F be a finite separable field extension. We define a functor

$$\mathrm{cor}_{L/F} : \mathrm{C}(L,\Lambda) \to \mathrm{C}(F,\Lambda)$$

as follows: on the objects $\mathrm{cor}_{L/F}(X,i) = (X,i)$, where on the right-hand side X is considered as an F-variety via the composition $X \to \mathrm{Spec}\,L \to \mathrm{Spec}\,F$; on the morphisms, the map

$$\mathrm{Hom}_{\mathrm{C}(L,\Lambda)}\big((X,i),(Y,j)\big) \to \mathrm{Hom}_{\mathrm{C}(F,\Lambda)}\big((X,i),(Y,j)\big)$$

is the push-forward homomorphism $\mathrm{Ch}_{\dim X+i-j}(X \times_L Y) \to \mathrm{Ch}_{\dim X+i-j}(X \times_F Y)$ with respect to the closed imbedding $X \times_L Y \hookrightarrow X \times_F Y$. Passing to the additive completion and then to the idempotent completion, we get an additive and commuting with the Tate shift functor $\mathrm{CM}(L,\Lambda) \to \mathrm{CM}(F,\Lambda)$, which we also denote by $\mathrm{cor}_{L/F}$.

The functor $\mathrm{cor}_{L/F} : \mathrm{C}(L,\Lambda) \to \mathrm{C}(F,\Lambda)$ is left-adjoint and right-adjoint to the change of field functor $\mathrm{res}_{L/F} : \mathrm{C}(F,\Lambda) \to \mathrm{C}(L,\Lambda)$, associating to (X,i) the object (X_L,i). Therefore, the functor $\mathrm{cor}_{L/F} : \mathrm{CM}(L,\Lambda) \to \mathrm{CM}(F,\Lambda)$ is also left-adjoint and right-adjoint to the change of field functor $\mathrm{res}_{L/F} : \mathrm{CM}(F,\Lambda) \to \mathrm{CM}(L,\Lambda)$. (This makes a funny difference with the category of varieties, where the functor $\mathrm{cor}_{L/F}$ is only left-adjoint to $\mathrm{res}_{L/F}$, while the right-adjoint to $\mathrm{res}_{L/F}$ functor is the Weil transfer.) It follows that for any $M \in \mathrm{CM}(L,\Lambda)$ and any $i \in \mathbb{Z}$, the Chow groups

$\mathrm{Ch}^i(M)$ and $\mathrm{Ch}^i(\mathrm{cor}_{L/F} M)$ are canonically isomorphic as well as the Chow groups $\mathrm{Ch}_i(M)$ and $\mathrm{Ch}_i(\mathrm{cor}_{L/F} M)$ are. Indeed, since $\mathrm{res}_{L/F} \Lambda = \Lambda \in \mathrm{CM}(L,\Lambda)$, we have

$$\mathrm{Ch}^i(M) := \mathrm{Hom}(M,\Lambda(i)) = \mathrm{Hom}\big(\mathrm{cor}_{L/F} M,\Lambda(i)\big) =: \mathrm{Ch}^i(\mathrm{cor}_{L/F} M) \qquad \text{and}$$
$$\mathrm{Ch}_i(M) := \mathrm{Hom}(\Lambda(i),M) = \mathrm{Hom}\big(\Lambda(i),\mathrm{cor}_{L/F} M\big) =: \mathrm{Ch}_i(\mathrm{cor}_{L/F} M).$$

In particular, if the ring Λ is connected and $M \in \mathrm{CM}(L,\Lambda)$ is an *upper* (see [5, Definition 2.10] or Sect. 1 here) motivic summand of an irreducible smooth complete L-variety X, then $\mathrm{cor}_{L/F} M$ is an upper motivic summand of the F-variety X.

Now we turn back to the situation where Λ is a finite field $\mathbb{F}$:

Proposition 3.1. *The following three conditions on a finite galois field extension E/F are equivalent:*

(1) *For any intermediate field $F \subset K \subset E$, the K-motive of* $\mathrm{Spec}\, E$ *is indecomposable;*
(2) *For any intermediate fields $F \subset K \subset L \subset E$ and any indecomposable L-motive M, the K-motive* $\mathrm{cor}_{L/K}(M)$ *is indecomposable;*
(3) *The degree of E/F is a power of p (where p is the characteristic of the coefficient field $\mathbb{F}$).*

Proof. We start by showing that $(3) \Rightarrow (2)$. So, we assume that $[E:F]$ is a power of p and we prove (2). The extension L/K decomposes in a finite chain of galois degree p extensions. Therefore, we may assume that L/K itself is a galois degree p extension. Let $R = \mathrm{End}(M)$. This is an associative, unital, but not necessarily commutative $\mathbb{F}$-algebra. Moreover, since M is indecomposable, the ring R has no nontrivial idempotents. We have $\mathrm{End}\big(\mathrm{cor}_{L/K}(M)\big) = R \otimes_{\mathbb{F}} \mathrm{End}(M_K(\mathrm{Spec}\, L))$ where $M_K(\mathrm{Spec}\, L) \in \mathrm{CM}(K,\mathbb{F})$ is the motive of the K-variety $\mathrm{Spec}\, L$. According to [3, Sect. 7], the ring $\mathrm{End}(M_K(\mathrm{Spec}\, L))$ is isomorphic to the group ring $\mathbb{F}\Gamma$, where Γ is the Galois group of L/K. As the group Γ is (cyclic) of order p, we have $\mathbb{F}\Gamma \simeq \mathbb{F}[t]/(t^p-1)$. Because $p = \mathrm{char}\,\mathbb{F}$, $\mathbb{F}[t]/(t^p-1) \simeq \mathbb{F}[t]/(t^p)$. It follows that the ring $\mathrm{End}\big(\mathrm{cor}_{L/K}(M)\big)$ is isomorphic to the ring $R[t]/(t^p)$. We prove (2) by showing that the latter ring does not contain nontrivial idempotents. An arbitrary element of $R[t]/(t^p)$ can be written in the form $a+b$ in a unique way, where $a \in R$ and b is an element of $R[t]/(t^p)$ divisible by the class of t. Note that b is nilpotent. Let us take an idempotent of $R[t]/(t^p)$ and write it in the earlier form $a+b$. Then a is an idempotent of R. Therefore $a = 1$ or $a = 0$. If $a = 1$ then $a+b$ is invertible and therefore $a+b = 1$. If $a = 0$ then $a+b$ is nilpotent and therefore $a+b = 0$.

We have proved the implication $(3) \Rightarrow (2)$. The implication $(2) \Rightarrow (1)$ is trivial. We finish by proving that $(1) \Rightarrow (3)$.

We assume that $[E:F]$ is divisible by a different from p prime q and we show that (1) does not hold. Indeed, the galois group of E/F contains an element σ of order q. Let K be the subfield of E consisting of the elements of E fixed by σ. We have $F \subset K \subset E$ and E/K is galois of degree q. The endomorphisms ring of $M_K(\mathrm{Spec}\, E)$ is isomorphic to $\mathbb{F}[t]/(t^q-1)$. As $q \neq \mathrm{char}\,\mathbb{F}$, the factors of the decomposition $t^q-1 = (t-1)\cdot(t^{q-1}+t^{q-2}+\cdots+1) \in \mathbb{F}[t]$ are coprime. Therefore, the ring $F[t]/(t^q-1)$

is the direct product of the rings $\mathbb{F}[t]/(t-1) = \mathbb{F}$ and $\mathbb{F}[t]/(t^{q-1} + \cdots + 1)$, and it follows that the motive $M_K(\operatorname{Spec} E)$ is not indecomposable. $\square$

Corollary 3.2. *Let E/F be a finite p-primary galois field extension and let L be an intermediate field: $F \subset L \subset E$. Let $M \in \mathrm{CM}(L, \mathbb{F})$ be an upper indecomposable motivic summand of an irreducible smooth complete L-variety X. Then $\mathrm{cor}_{L/F} M$ is an upper indecomposable summand of the F-variety X.* $\square$

Example 3.3. Let X be a projective quadric given by an isotropic nondegenerate 4-dimensional quadratic form of nontrivial discriminant. The variety X is projective homogeneous under the action of the orthogonal group of the quadratic form. This group is outer and the corresponding field extension E/F of this group is the quadratic extension given by the discriminant of the quadratic form. The motive of X contains a shift of the motive $M(\operatorname{Spec} E)$.

Now let us assume that the characteristic p of the coefficient field $\mathbb{F}$ is odd. Then $M(\operatorname{Spec} E)$ decomposes into a sum of two indecomposable summands. The (total) Chow group of one of these two summands is 0. In particular, this summand is not an upper motive of G (because the Chow group of an upper motive is nontrivial by the very definition of upper). Therefore, Theorem 1.1 fails without the hypothesis that the extension E/F is p-primary.

4 Proof of Theorem 1.1

Before starting the proof of Theorem 1.1, let us recall some classical facts and introduce some notation.

We write $\mathscr{D}$ (or $\mathscr{D}_G$) for the set of vertices of the Dynkin diagram of G. The absolute galois group Γ_F of the field F acts on $\mathscr{D}$. The subgroup $\Gamma_E \subset \Gamma_F$ is the kernel of the action.

Let L be a field extension of F. The set $\mathscr{D}_{G_L}$ is identified with $\mathscr{D} = \mathscr{D}_G$. The action of Γ_L on $\mathscr{D}$ is trivial if and only if the group G_L is of inner type. Any Γ_L-stable subset τ in $\mathscr{D}$ determines a projective G_L-homogeneous variety X_{τ,G_L} in the way described in [5, Sect. 3]. This is the variety corresponding to the set $\mathscr{D} \setminus \tau$ in the sense of [6]. For instance, $X_{\mathscr{D},G_L}$ is the variety of the Borel subgroups of G_L, and $X_{\emptyset,G_L} = \operatorname{Spec} L$. Any projective G_L-homogeneous variety is G_L-isomorphic to X_{τ,G_L} for some Γ_L-stable $\tau \subset \mathscr{D}$.

If the extension L/F is finite separable, we write M_{τ,G_L} for the upper indecomposable motivic summand of the F-variety X_{τ,G_L} (where τ is a Γ_L-stable subset in $\mathscr{D}$). If $L \subset E$, the isomorphism class of M_{τ,G_L} is an *upper motive of* G.

For any field extension L/F, the set $\mathscr{D}_{G'}$, attached to the semisimple anisotropic kernel G' of G_L, is identified with a (Γ_L-invariant) subset in $\mathscr{D}$. We write τ_L (or $\tau_{L,G}$) for its complement. The subset $\tau_L \subset \mathscr{D}$ is (the set of circled vertices of) the Tits index of G_L defined in [6]. For any Γ_L-stable subset $\tau \subset \mathscr{D}$, the variety X_{τ,G_L} has a rational point if and only if $\tau \subset \tau_L$.

Proof (of Theorem 1.1). This is a recast of [5, proof of Theorem 3.5].

We prove Theorem 1.1 simultaneously for all F, G, X using an induction on $n = \dim X$. The base of the induction is $n = 0$ where $X = \operatorname{Spec} F$ and the statement is trivial.

From now on we assume that $n \geq 1$ and that Theorem 1.1 is already proven for all varieties of dimension $< n$.

For any field extension L/F, we write $\tilde{L}$ for the function field $L(X)$.

Let M be an indecomposable summand of $M(X)$. We have to show that M is isomorphic to a shift of M_{τ,G_L} for some intermediate field L of E/F and some $\operatorname{Gal}(E/L)$-stable subset $\tau \subset \mathscr{D}_G$ containing $\tau_{\tilde{F}}$.

Let $G'/\tilde{F}$ be the semisimple anisotropic kernel of the group $G_{\tilde{F}}$. The set $\mathscr{D}_{G'}$ is identified with $\mathscr{D}_G \setminus \tau_{\tilde{F},G}$.

We note that the group $G'_{\tilde{E}}$ is of inner type. The field extension $\tilde{E}/\tilde{F}$ is galois with the galois group $\operatorname{Gal}(E/F)$. In particular, its degree is a power of p and every intermediate field is of the form $\tilde{L}$ for some intermediate field L of the extension E/F.

According to [1, Theorem 4.2], the motive of $X_{\tilde{F}}$ decomposes into a sum of shifts of motives of projective $G'_{\tilde{L}}$-homogeneous (where L runs over intermediate fields of the extension E/F) varieties Y, satisfying $\dim Y < \dim X = n$. (We are using the assumption that $n > 0$ here.) It follows by the induction hypothesis and Corollary 3.2 that each summand of the complete motivic decomposition of $X_{\tilde{F}}$ is a shift of $M_{\tau',G'_{\tilde{L}}}$ for some L and some $\tau' \subset \mathscr{D}_{G'}$. By Corollary 2.2, the complete decomposition of $M_{\tilde{F}}$ also consists of shifts of $M_{\tau',G'_{\tilde{L}}}$.

Let us choose a summand $M_{\tau',G'_{\tilde{L}}}(i)$ with minimal i in the complete decomposition of $M_{\tilde{F}}$. We set $\tau = \tau' \cup \tau_{\tilde{F}} \subset \mathscr{D}_G$. We shall show that $M \simeq M_{\tau,G_L}(i)$ for these L, τ, and i.

We write Y for the F-variety X_{τ,G_L} and we write Y' for the $\tilde{F}$-variety $X_{\tau',G'_{\tilde{L}}}$. We write N for the F-motive M_{τ,G_L} and we write N' for the $\tilde{F}$-motive $M_{\tau',G'_{\tilde{L}}}$.

By [5, Lemma 2.14] (also formulated in Sect. 1 here) and since M is indecomposable, it suffices to construct morphisms

$$\alpha : M(Y)(i) \to M \text{ and } \beta : M \to M(Y)(i)$$

satisfying $\operatorname{mult}(\beta \circ \alpha) = 1$, where $\operatorname{mult}(\beta \circ \alpha)$ is the *multiplicity*, defined in Sect. 1, of the correspondence $(\beta \circ \alpha) \in \operatorname{Ch}_{\dim Y}(Y \times_F Y)$.

We construct α first. Since $\tau' \subset \tau$, the $\tilde{F}(Y)$-variety $Y' \times_{\tilde{L}} \operatorname{Spec} \tilde{F}(Y)$ has a rational point. Let $\alpha_1 \in \operatorname{Ch}_0\big(Y' \times_{\tilde{L}} \operatorname{Spec} \tilde{F}(Y)\big)$ be the class of a rational point. Let $\alpha_2 \in \operatorname{Ch}_i(X_{\tilde{F}(Y)})$ be the image of α_1 under the composition

$$\operatorname{Ch}_0\big(Y' \times_{\tilde{L}} \operatorname{Spec} \tilde{F}(Y)\big) \to \operatorname{Ch}_0(Y'_{\tilde{F}(Y)}) \to \operatorname{Ch}_0(N'_{\tilde{F}(Y)}) \hookrightarrow \operatorname{Ch}_i(X_{\tilde{F}(Y)}),$$

where the first map is the push-forward with respect to the closed imbedding

$$Y' \times_{\tilde{L}} \operatorname{Spec} \tilde{F}(Y) \hookrightarrow Y'_{\tilde{F}(Y)} := Y' \times_{\tilde{F}} \operatorname{Spec} \tilde{F}(Y).$$

Since $\tau_{\tilde{F}} \subset \tau$, the variety X has an $F(Y)$-point and, therefore, the field extension $\tilde{F}(Y)/F(Y)$ is purely transcendental. Consequently, the element α_2 is $F(Y)$-rational and lifts to an element $\alpha_3 \in \mathrm{Ch}_{\dim Y+i}(Y \times X)$. We mean here a lifting with respect to the composition

$$\mathrm{Ch}_{\dim Y+i}(Y \times X) \twoheadrightarrow \mathrm{Ch}_i(X_{F(Y)}) \xrightarrow{\mathrm{res}_{\tilde{F}(Y)/F(Y)}} \mathrm{Ch}_i(X_{\tilde{F}(Y)}),$$

where the first map is the epimorphism given by the pull-back with respect to the morphism $X_{F(Y)} \to Y \times X$ induced by the generic point of the variety Y.

We define the morphism α as the composition

$$M(Y)(i) \xrightarrow{\alpha_3} M(X) \longrightarrow M,$$

where the second map is the projection of $M(X)$ onto its summand M.

We proceed by constructing β. Let $\beta_1 \in \mathrm{Ch}_{\dim Y'}(Y' \times_{\tilde{F}} Y_{\tilde{F}})$ be the class of the closure of the graph of a rational map of $\tilde{L}$-varieties $Y' \dashrightarrow Y_{\tilde{F}}$ (which exists because $\tau \subset \tau_{\tilde{F}} \cup \tau'$). Note that this graph is a subset of $Y' \times_{\tilde{L}} Y_{\tilde{F}}$, which we consider as a subset of $Y' \times_{\tilde{F}} Y_{\tilde{F}}$ via the closed imbedding $Y' \times_{\tilde{L}} Y_{\tilde{F}} \hookrightarrow Y' \times_{\tilde{F}} Y_{\tilde{F}}$. Let β_2 be the image of β_1 under the composition

$$\begin{aligned}\mathrm{Ch}^{\dim Y}(Y' \times_{\tilde{F}} Y_{\tilde{F}}) = \mathrm{Ch}^{\dim Y}\big(M(Y') \otimes M(Y_{\tilde{F}})\big) \to \mathrm{Ch}^{\dim Y}\big(N' \otimes M(Y_{\tilde{F}})\big) \to \\ \mathrm{Ch}^{\dim Y+i}(M(X_{\tilde{F}}) \otimes M(Y_{\tilde{F}})) = \mathrm{Ch}^{\dim Y+i}((X \times Y)_{\tilde{F}}),\end{aligned}$$

where the first arrow is induced by the projection $M(Y') \to N'$ and the second arrow is induced by the imbedding $N'(i) \to M(X_{\tilde{F}})$. The element β_2 lifts to an element

$$\beta_3 \in \mathrm{Ch}^{\dim Y+i}(X \times X \times Y).$$

We mean here a lifting with respect to the epimorphism

$$\mathrm{Ch}^{\dim Y+i}(X \times X \times Y) \twoheadrightarrow \mathrm{Ch}^{\dim Y+i}((X \times Y)_{\tilde{F}})$$

given by the pull-back with respect to the morphism $X \times X \times Y \to (X \times Y)_{\tilde{F}}$ induced by the generic point of the second factor in this triple direct product.

Let $\pi \in \mathrm{Ch}_{\dim X}(X \times X)$ be the projector defining the summand M of $M(X)$. Considering β_3 as a correspondence from X to $X \times Y$, we define

$$\beta_4 \in \mathrm{Ch}^{\dim Y+i}(X \times X \times Y)$$

as the composition $\beta_3 \circ \pi$. We get

$$\beta_5 \in \mathrm{Ch}^{\dim Y+i}(X \times Y) = \mathrm{Ch}_{\dim X-i}(X \times Y)$$

as the image of β_4 under the pull-back with respect to the diagonal of X. Finally, we define the morphism β as the composition

$$M \longrightarrow M(X) \xrightarrow{\beta_5} M(Y)(i).$$

The verification of the relation $\mathrm{mult}(\beta \circ \alpha) = 1$, finishing the proof, is similar to that of [5, proof of Theorem 3.5]. As the multiplicity is not changed under extension of scalars, the computation can be done over a splitting field of G. A convenient choice is the field $\bar{F}(X)$, where $\bar{F}$ is an algebraic closure of F. □

Remark 4.1. Theorem 1.1 can be also proven using a weaker result in place of [1, Theorem 4.2], namely, [2, Theorem 7.5].

Acknowledgements The author was supported by the Collaborative Research Centre 701 of the Bielefeld University.

References

1. Brosnan, P.: On motivic decompositions arising from the method of Białynicki-Birula. Invent. Math. **161**(1), 91–111 (2005)
2. Chernousov, V., Gille, S., Merkurjev, A.: Motivic decomposition of isotropic projective homogeneous varieties. Duke Math. J. **126**(1), 137–159 (2005)
3. Chernousov, V., Merkurjev, A.: Motivic decomposition of projective homogeneous varieties and the Krull-Schmidt theorem. Transform. Groups **11**(3), 371–386 (2006)
4. Elman, R., Karpenko, N., Merkurjev, A.: The algebraic and geometric theory of quadratic forms, *American Mathematical Society Colloquium Publications*, vol. 56. American Mathematical Society, Providence, RI (2008)
5. Karpenko, N.A.: Upper motives of algebraic groups and incompressibility of Severi-Brauer varieties. Linear Algebraic Groups and Related Structures (preprint server) 333 (2009, Apr 3, revised: 2009, Apr 24), 18 pages
6. Tits, J.: Classification of algebraic semisimple groups. In: Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), pp. 33–62. American Mathematical Society, Providence, R.I. (1966)

Triality and étale algebras

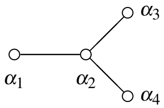
Max-Albert Knus and Jean-Pierre Tignol

Dedicated to R. Parimala at the occasion of her 60^{th} *birthday*

Summary Trialitarian automorphisms are related to automorphisms of order 3 of the Dynkin diagram of type D_4. Octic étale algebras with trivial discriminant containing quartic subalgebras are classified by Galois cohomology with values in the Weyl group of type D_4. This paper discusses triality for such étale extensions.

1 Introduction

All Dynkin diagrams but one admit at most automorphisms of order two, which are related to duality in algebra and geometry. The Dynkin diagram of D_4



is special, in the sense that it admits automorphisms of order 3. Algebraic and geometric objects related to D_4 are of particular interest as they also usually admit exceptional automorphisms of order 3, which are called trialitarian. For example, the special projective orthogonal group PGO_8^+ or the simply connected group Spin_8 admit outer automorphisms of order 3. As already observed by Cartan [5], the Weyl group $W(D_4) = \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4$ of Spin_8 or of PGO_8^+ similarly admits trialitarian

Max-Albert Knus
Departement Mathematik, ETH Zentrum, CH-8092 Zürich, Switzerland,
e-mail: knus@math.ethz.ch

Jean-Pierre Tignol
Institut de Mathématique Pure et Appliquée, Université catholique de Louvain,
B-1348 Louvain-la-Neuve, Belgium, e-mail: jean-pierre.tignol@uclouvain.be

2010 Mathematics subject classification. 13B40, 12F10, 12G0.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_16,

automorphisms. Let F be a field and let F_s be a separable closure of F. The Galois cohomology set $H^1\big(\Gamma, W(D_4)\big)$, where Γ is the absolute Galois group $\mathrm{Gal}(F_s/F)$, classifies isomorphism classes of étale extensions S/S_0 where S has dimension 8, S_0 has dimension 4 and S has trivial discriminant (see Sect. 3). There is an induced trialitarian action on $H^1\big(\Gamma, W(D_4)\big)$, which associates to the isomorphism class of an extension S/S_0 as above, two extensions S'/S'_0 and S''/S''_0, of the same kind, so that the triple $(S/S_0, S'/S'_0, S''/S''_0)$ is cyclically permuted by triality. This paper is devoted to the study of such triples of étale algebras. It grew out of a study, in the spirit of [17], of Severi-Brauer varieties over the "field of one element" [14], which is in preparation (see also [18] and [19]).

In Part 2 we describe some basic constructions on finite Γ-sets and étale algebras. Some results are well-known, others were taken from [14], like the Clifford construction. In Sect. 3 we recall how Γ-sets and étale algebras are related to Galois cohomology. Section 4 is devoted to triality in connection with Γ-sets and in Sect. 5 we discuss trialitarian automorphisms of the Weyl group $W(D_4)$. In Sect. 6 we consider triality at the level of étale algebras. We give in Table 1 a list of isomorphism classes of étale algebras corresponding to the conjugacy classes of subgroups of $W(D_4)$, together with a description of the triality action. We also consider étale algebras associated to subgroups of $W(D_4)$ which are fixed under triality. We then view in Sect. 7 triality as a way to create resolvents and give explicit formulae for polynomials defining étale algebras. Finally, we give in the last section results of Serre on Witt invariants of $W(D_4)$.

2 Étale Algebras and Γ-sets

Throughout most of this work, F is an arbitrary field. We denote by F_s a separable closure of F and by Γ the absolute Galois group $\Gamma = \mathrm{Gal}(F_s/F)$, which is a profinite group.

A finite-dimensional commutative F-algebra S is called *étale* (over F) if $S \otimes_F F_s$ is isomorphic to the F_s-algebra $F_s^n = F_s \times \cdots \times F_s$ (n factors) for some integer $n \geq 1$. Étale F-algebras are the direct products of finite separable field extensions of F. We refer to [12, Sect. 18.A] for various equivalent characterizations. Étale algebras (with F-algebra homomorphisms) form a category $\acute{E}t_F$ in which finite direct products and finite direct sums (= tensor products) are defined.

Finite sets with a continuous left action of Γ (for the discrete topology) are called (finite) Γ-sets. They form a category Set_Γ whose morphisms are the Γ-equivariant maps. Finite direct products and direct sums (= disjoint unions) are defined in this category. We denote by $|X|$ the cardinality of any finite set X.

For any étale F-algebra S of dimension n, the set of F-algebra homomorphisms

$$\mathbf{X}(S) = \mathrm{Hom}_{F\text{-alg}}(S, F_s)$$

is a Γ-set of n elements since Γ acts on F_s. Conversely, if X is a Γ-set of n elements, the F-algebra $\mathbf{M}(X)$ of Γ-equivariant maps $X \to F_s$ is an étale F-algebra of dimension n,

$$\mathbf{M}(X) = \{f\colon X \to F_s \mid \gamma\bigl(f(x)\bigr) = f({}^{\gamma}x) \text{ for } \gamma \in \Gamma, x \in X\}.$$

As first observed by Grothendieck, there are canonical isomorphisms

$$\mathbf{M}\bigl(\mathbf{X}(S)\bigr) \cong S, \qquad \mathbf{X}\bigl(\mathbf{M}(X)\bigr) \cong X,$$

so that the functors $\mathbf{M}$ and $\mathbf{X}$ define an antiequivalence of categories

$$\mathsf{Set}_{\Gamma} \equiv \acute{\mathsf{E}}\mathsf{t}_F \tag{2.1}$$

(see [7, Proposition (4.3), p. 25] or [12, (18.4)]). Under this antiequivalence, the cardinality of Γ-sets corresponds to the dimension of étale F-algebras, the disjoint union $\sqcup$ in Set_{Γ} corresponds to the product $\times$ in $\acute{\mathsf{E}}\mathsf{t}_F$, and the product $\times$ in Set_{Γ} to the tensor product $\otimes$ in $\acute{\mathsf{E}}\mathsf{t}_F$. For any integer $n \geq 1$, we let $\acute{\mathsf{E}}\mathsf{t}_F^n$ denote the groupoid[1] whose objects are n-dimensional étale F-algebras and whose morphisms are F-algebra isomorphisms, and Set_{Γ}^n the groupoid of Γ-sets with n elements. The antiequivalence (2.1) restricts to an antiequivalence $\mathsf{Set}_{\Gamma}^n \equiv \acute{\mathsf{E}}\mathsf{t}_F^n$. The split étale algebra F^n corresponds to the Γ-set $\mathbf{n}$ of n elements with trivial Γ-action. Étale algebras of dimension 2 are also called *quadratic* étale algebras.

A morphism[2] of Γ-sets $Y \xleftarrow{\pi} Z$ is called a Γ*-covering* if the number of elements in each fiber $y^{\pi^{-1}} \subset Z$ does not depend on $y \in Y$. This number is called the *degree* of the covering. For $n, d \geq 1$ we let $\mathsf{Cov}_{\Gamma}^{d/n}$ denote the groupoid whose objects are coverings of degree d of a Γ-set of n elements and whose morphisms are isomorphisms of Γ-coverings.

A homomorphism $S \xrightarrow{\varepsilon} T$ of étale F-algebras is said to be an *extension of degree d of étale algebras* if ε endows T with a structure of a free S-module of rank d. This corresponds under the antiequivalence (2.1) to a *covering of degree d*:

$$\mathbf{X}(S) \xleftarrow{\mathbf{X}(\varepsilon)} \mathbf{X}(T)$$

(see [14]). Let $\acute{\mathsf{E}}\mathsf{tex}_F^{d/n}$ denote the groupoid of étale extensions $S \xrightarrow{\varepsilon} T$ of degree d of F-algebras with $\dim_F S = n$ (hence $\dim_F T = dn$). From (2.1) we obtain an antiequivalence of groupoids

$$\acute{\mathsf{E}}\mathsf{tex}_F^{d/n} \equiv \mathsf{Cov}_{\Gamma}^{d/n}.$$

[1] A groupoid is a category in which all morphisms are isomorphisms.

[2] We let morphisms of Γ-sets act on the right of the arguments (with the exponential notation) and use the usual function notation for morphisms in the antiequivalent category of étale algebras.

The Γ-covering with trivial Γ-action

$$\mathbf{d}/\mathbf{n}: \quad \mathbf{n} \xleftarrow{p_1} \mathbf{n} \times \mathbf{d} \tag{2.2}$$

where p_1 is the first projection corresponds to the extension $F^n \to (F^d)^n$.

Of particular importance in the sequel are coverings of degree 2, which are also called *double coverings*. Each such covering $Y \xleftarrow{\pi} Z$ defines a canonical automorphism $Z \xleftarrow{\sigma} Z$ of order 2, which interchanges the elements in each fiber of π. Clearly, this automorphism has no fixed points. Conversely, if Z is any Γ-set and $Z \xleftarrow{\sigma} Z$ is an automorphism of order 2 without fixed points, the set of orbits

$$Z/\sigma = \big\{\{z, z^\sigma\} \mid z \in Z\big\}$$

is a Γ-set and the canonical map $(Z/\sigma) \leftarrow Z$ is a double covering. An *involution* of a Γ-set with an even number of elements is any automorphism of order 2 without fixed points.

Let $\sigma\colon S \to S$ be an automorphism of order 2 of an étale F-algebra S, and let $S^\sigma \subset S$ denote the F-subalgebra of fixed elements, which is necessarily étale. The following conditions are equivalent (see [14]):

(a) The inclusion $S^\sigma \to S$ is a quadratic étale extension of F-algebras;
(b) The automorphism $\mathbf{X}(\sigma)$ is an involution on $\mathbf{X}(S)$.

We say under these equivalent conditions that the automorphism σ is an *involution* of the étale F-algebra S.

Basic Constructions on Γ-sets

We recall from [12, Sect. 18] and [13, Sect. 2.1] the construction of the discriminant $\Delta(X)$ of a Γ-set X with $|X| = n \geq 2$. Consider the set of n-tuples of elements in X:

$$\Sigma_n(X) = \{(x_1, \dots, x_n) \mid X = \{x_1, \dots, x_n\}\}.$$

This Γ-set carries an obvious transitive (right) action of the symmetric group $\mathfrak{S}_n$. The *discriminant* $\Delta(X)$ is the set of orbits under the alternating group $\mathfrak{A}_n$:

$$\Delta(X) = \Sigma_n(X)/\mathfrak{A}_n.$$

It is a Γ-set of two elements, so Δ is a functor

$$\Delta\colon \mathsf{Set}^n_\Gamma \to \mathsf{Set}^2_\Gamma.$$

For any covering $Z_0 \xleftarrow{\pi} Z$ of degree 2 with $|Z_0| = n$, (hence $|Z| = 2n$), we consider the set of (not necessarily Γ-equivariant) sections of π:

$$C(Z/Z_0) = \big\{\{z_1, \dots, z_n\} \subset Z \mid \{z_1^\pi, \dots, z_n^\pi\} = Z_0\big\}.$$

It is a Γ-set with 2^n elements, so C is a functor

$$C\colon \mathsf{Cov}_\Gamma^{2/n} \to \mathsf{Set}_\Gamma^{2^n},$$

called the *Clifford functor* (see [14]). The Γ-set $C(Z/Z_0)$ is equipped with a canonical surjective morphism

$$\Delta(Z) \xleftarrow{\delta} C(Z/Z_0), \tag{2.3}$$

which is defined in [13, Sect. 2.2] as follows: let $\sigma\colon Z \to Z$ be the involution canonically associated to the double covering $Z_0 \xleftarrow{\pi} Z$, so the fiber of z^π is $\{z, z^\sigma\}$ for each $z \in Z$; then δ maps each section $\{z_1, \dots, z_n\}$ to the $\mathfrak{A}_{2n}$-orbit of the $2n$-tuple $(z_1, \dots, z_n, z_1^\sigma, \dots, z_n^\sigma)$,

$$\{z_1, \dots, z_n\}^\delta = (z_1, \dots, z_n, z_1^\sigma, \dots, z_n^\sigma)^{\mathfrak{A}_{2n}}.$$

Note that the canonical involution σ induces an involution $\underline{\sigma}$ on $C(Z/Z_0)$, which maps each section ω to its complement $Z \setminus \omega$. We may view $C(Z/Z_0)$ as a covering of degree 2 of the set of orbits $C(Z/Z_0)/\underline{\sigma}$, and thus consider the Clifford construction as a functor

$$C\colon \mathsf{Cov}_\Gamma^{2/n} \to \mathsf{Cov}_\Gamma^{2/2^{n-1}}. \tag{2.4}$$

Proposition 2.5. *For sections ω, $\omega' \in C(Z/Z_0)$, we have $\omega^\delta = (\omega')^\delta$ if and only if* $|\omega \cap \omega'| \equiv n \bmod 2$. *Moreover, denoting by ι the nontrivial automorphism of $\Delta(Z)$, we have*

$$\underline{\sigma} \circ \delta = \begin{cases} \delta & \text{if } n \text{ is even,} \\ \delta \circ \iota & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Let $\omega = \{z_1, \dots, z_n\}$ and $\omega' = \{z_1, \dots, z_r, z_{r+1}^\sigma, \dots, z_n^\sigma\}$, so $r = |\omega \cap \omega'|$,

$$\omega^\delta = (z_1, \dots, z_n, z_1^\sigma, \dots, z_n^\sigma)^{\mathfrak{A}_{2n}}$$

and

$$(\omega')^\delta = (z_1, \dots, z_r, z_{r+1}^\sigma, \dots, z_n^\sigma, z_1^\sigma, \dots, z_r^\sigma, z_{r+1}, \dots, z_n)^{\mathfrak{A}_{2n}}.$$

The permutation σ' that interchanges z_i and z_i^σ for $i = r+1, \dots, n$ satisfies

$$(z_1, \dots, z_n, z_1^\sigma, \dots, z_n^\sigma)^{\sigma'} = (z_1, \dots, z_r, z_{r+1}^\sigma, \dots, z_n^\sigma, z_1^\sigma, \dots, z_r^\sigma, z_{r+1}, \dots, z_n);$$

it is in $\mathfrak{A}_{2n}$ if and only if $n - r$ is even, which means $|\omega \cap \omega'| \equiv n \bmod 2$. For $\omega' = \omega^{\underline{\sigma}}$ the complement of ω we have $|\omega \cap \omega^{\underline{\sigma}}| = 0$, hence $\omega^{\underline{\sigma}\delta} = \omega^\delta$ if and only if $n \equiv 0 \bmod 2$. $\square$

Oriented Γ-sets

An *oriented Γ-set* is a pair (Z, ∂_Z) where Z is a Γ-set and ∂_Z is a fixed isomorphism of Γ-sets $\mathbf{2} \xleftarrow{\sim} \Delta(Z)$. In particular the Γ-action on $\Delta(Z)$ is trivial. There are two possible choices for ∂_Z. A choice is an *orientation of Z*. Oriented Γ-sets with n elements form a groupoid $(\mathsf{Set}_\Gamma^n)^+$ whose morphisms are isomorphisms $Z_2 \xleftarrow{f} Z_1$ such that $\Delta(f) \circ \partial_{Z_2} = \partial_{Z_1}$. Similarly, *oriented coverings* are pairs $(Z/Z_0, \partial_Z)$ where $Z_0 \leftarrow Z$ is a Γ-covering and ∂_Z is an orientation of Z. We denote by $(\mathsf{Cov}_\Gamma^{d/n})^+$ the groupoid of oriented coverings of degree d of Γ-sets with n elements. Changing the orientation through the twist $\mathbf{2} \xleftarrow{\iota} \mathbf{2}$ defines an involutive functor

$$\kappa \colon (\mathsf{Cov}_\Gamma^{d/n})^+ \to (\mathsf{Cov}_\Gamma^{d/n})^+.$$

Proposition 2.6. *If n is even the functor $C \colon \mathsf{Cov}_\Gamma^{2/n} \to \mathsf{Cov}_\Gamma^{2/2^{n-1}}$ of (2.4) restricts to a pair of functors*

$$C_1, C_2 \colon (\mathsf{Cov}_\Gamma^{2/n})^+ \to \mathsf{Cov}_\Gamma^{2/2^{n-2}}.$$

Moreover, two sections ω and ω' of the oriented Γ-covering $(Z/Z_0, \partial_Z)$ lie in the same set $C_1(Z/Z_0, \partial_Z)$ or $C_2(Z/Z_0, \partial_Z)$ if and only if $|\omega \cap \omega'| \equiv 0 \mod 2$.

Proof. Let Z/Z_0 be a $2/n$-covering. Proposition 2.5 implies that the covering $\Delta(Z) \xleftarrow{\delta} C(Z/Z_0)$ factors through $C(Z/Z_0)/\underline{\sigma}$, where $\underline{\sigma}$ is the canonical involution of $C(Z/Z_0)$:

$$\Delta(Z) \leftarrow C(Z/Z_0)/\underline{\sigma} \leftarrow C(Z/Z_0).$$

Thus, if Z/Z_0 is oriented, we may use the given isomorphism $\mathbf{2} \xleftarrow{\partial_Z} \Delta(Z)$ to define the Γ-sets

$$C_1(Z/Z_0, \partial_Z) = \{\omega \in C(Z/Z_0) \mid \omega^{\delta\partial_Z} = 1\}$$

and

$$C_2(Z/Z_0, \partial_Z) = \{\omega \in C(Z/Z_0) \mid \omega^{\delta\partial_Z} = 2\}.$$

Obviously, we have $C(Z/Z_0) = C_1(Z/Z_0, \partial_Z) \sqcup C_2(Z/Z_0, \partial_Z)$, and Proposition 2.5 shows that $\underline{\sigma}$ restricts to involutions on $C_1(Z/Z_0, \partial_Z)$ and $C_2(Z/Z_0, \partial_Z)$. The last claim also follows from Proposition 2.5. □

We call the two functors C_1 and C_2 the *spinor functors*. Note that when n is even an orientation ∂_Z on Z/Z_0 can also be defined by specifying whether a given section $\omega \in C(Z/Z_0)$ lies in $C_1(Z/Z_0, \partial_Z)$ or $C_2(Z/Z_0, \partial_Z)$. Indeed, $\omega \in C_1(Z/Z_0, \partial_Z)$ if and only if $\omega^\delta \in \Delta(Z)$ is mapped to 1, which determines ∂_Z uniquely. We shall avail ourselves of this possibility to define orientations on coverings in $\mathsf{Cov}_\Gamma^{2/4}$ in Sect. 4.

Basic Constructions on étale Algebras

We now consider analogues of the functors Δ and C for étale algebras and étale extensions. For S an étale F-algebra of dimension $n \geq 2$, the discriminant $\Delta(S)$ is a quadratic étale F-algebra such that

$$\mathbf{X}\big(\Delta(S)\big) = \Delta\big(\mathbf{X}(S)\big).$$

We thus have a functor

$$\Delta\colon \acute{E}t_F^n \to \acute{E}t_F^2 \qquad \text{for } n \geq 2.$$

If the field F has characteristic different from 2, it is usual to represent $\Delta(S)$ as $F[x]/\big(x^2 - \mathrm{Disc}(S)\big)$, $\mathrm{Disc}(S) \in F^\times$, and the class of $\mathrm{Disc}(S)$ in $F^\times/(F^\times)^2$ is the usual discriminant. We refer to [12, p. 291–293] and [13, Sect. 3.1] for details.

Let $S \xrightarrow{\varepsilon} T$ be an étale extension of degree 2 of (étale) F-algebras, with $\dim_F S = n$, $\dim_F T = 2n$. In [13, Sect. 3.2][3] we define an étale F-algebra $C(T/S)$ such that

$$\mathbf{X}\big(C(T/S)\big) = C\big(\mathbf{X}(T)/\mathbf{X}(S)\big).$$

Example 2.7. If $\dim_F T = 2$ and $S = F$, we have $C(T/S) = T$.

For S_1, S_2 étale algebras of arbitrary dimension, and for arbitrary étale extensions T_1/S_1 and T_2/S_2 of degree 2, there is a canonical isomorphism

$$P\colon C\big((T_1 \times T_2)/(S_1 \times S_2)\big) \xrightarrow{\sim} C(T_1/S_1) \otimes C(T_2/S_2).$$

We call the 2^n-dimensional algebra $C(T/S)$ the *Clifford algebra* of T/S. It admits a canonical involution $\underline{\sigma}$. If $\dim_F S$ is even $\underline{\sigma}$ is the identity on $\Delta(T)$. The canonical morphism δ of (2.3)

$$\Delta\big(\mathbf{X}(T)\big) \xleftarrow{\delta} C\big(\mathbf{X}(T)/\mathbf{X}(S)\big)$$

yields a canonical F-algebra homomorphism which we again denote by δ,

$$\Delta(T) \xrightarrow{\delta} C(T/S),$$

so that $C(T/S)$ is an étale extension of degree 2^{n-1} of a quadratic étale F-algebra.

Oriented étale Algebras

As for oriented Γ-sets we define *oriented étale algebras* as pairs (S, ∂_S) where S is an étale algebra and $\partial_S\colon \Delta(S) \xrightarrow{\sim} F \times F$ is an isomorphism of F-algebras. *Oriented extensions of étale algebras* are pairs $(S/S_0, \partial_S)$ where S/S_0 is an extension of

[3] The notation Ω is used for C in [13].

étale algebras and $\partial_S\colon \Delta(S) \xrightarrow{\sim} F \times F$ is an isomorphism of F-algebras. We have corresponding groupoids $(\acute{E}t_F^n)^+$, $(\acute{E}tex_F^{d/n})^+$ and antiequivalences

$$(Set_\Gamma^n)^+ \equiv (\acute{E}t_F^n)^+ \text{ and } (Cov_\Gamma^{d/n})^+ \equiv (\acute{E}tex_F^{d/n})^+.$$

Switching the orientation induces an involutive functor κ on these groupoids.

The Clifford functor C restricts to a pair of *spinor functors*

$$C_1, C_2\colon (\acute{E}tex_F^{2/n})^+ \to \acute{E}tex_F^{2/2^{n-2}} \tag{2.8}$$

if n is even.

Remark 2.9. The terminology used earlier owes its origin to the fact that the Clifford functor is related to the theory of Clifford algebras in the framework of quadratic forms and central simple algebras with involution. We refer to [14] for details and more properties of the Clifford construction.

3 Cohomology

For any integer $n \geq 1$, we consider the Γ-set $\mathbf{n} = \{1, \dots, n\}$ with the trivial Γ-action and let $\mathfrak{S}_n$ denote the symmetric group on $\mathbf{n}$, i.e., the automorphism group of $\mathbf{n}$,

$$\mathfrak{S}_n = \operatorname{Aut}(\mathbf{n}).$$

Recall from [12, Sect. 28.A] that the cohomology set $H^1(\Gamma, \mathfrak{S}_n)$ (for the trivial action of Γ on $\mathfrak{S}_n$) is the set of continuous group homomorphisms $\Gamma \to \mathfrak{S}_n$ (“cocycles”) up to conjugation.

Letting $\operatorname{Iso}(Set_\Gamma^n)$ denote the set of isomorphism classes in Set_Γ^n, we have a canonical bijection of pointed setsv

$$\operatorname{Iso}(Set_\Gamma^n) \xrightarrow{\sim} H^1(\Gamma, \mathfrak{S}_n). \tag{3.1}$$

Cohomology sets can also be used to describe isomorphism classes of Γ-coverings: for any integers $n, d \geq 1$, the group of automorphisms of the Γ-covering with trivial Γ-action $\mathbf{d}/\mathbf{n}$ is the wreath product (of order $(d!)^n n!$)

$$\operatorname{Aut}(\mathbf{d}/\mathbf{n}) = \mathfrak{S}_d \wr \mathfrak{S}_n \quad (= \mathfrak{S}_d^n \rtimes \mathfrak{S}_n).$$

The same construction as earlier yields a canonical bijection

$$\operatorname{Iso}(Cov_\Gamma^{d/n}) \xrightarrow{\sim} H^1(\Gamma, \mathfrak{S}_d \wr \mathfrak{S}_n), \tag{3.2}$$

where the Γ-action on $\mathfrak{S}_d \wr \mathfrak{S}_n$ is trivial; see [13, Sect. 4.2]. The automorphism group of the oriented Γ-covering $(\mathbf{d}/\mathbf{n}, \partial_{\mathbf{n}\times\mathbf{d}})$ is the group

$$(\mathfrak{S}_d \wr \mathfrak{S}_n)^+ = (\mathfrak{S}_d \wr \mathfrak{S}_n) \cap \mathfrak{A}_{dn}$$

so that

$$\mathrm{Iso}\big((\mathit{Cov}_\Gamma^{d/n})^+\big) \xrightarrow{\sim} H^1\big(\Gamma, (\mathfrak{S}_d \wr \mathfrak{S}_n)^+\big). \tag{3.3}$$

We now assume that Γ is the absolute Galois group $\Gamma = \mathrm{Gal}(F_\mathrm{s}/F)$ of a field F and use the notation $H^1(F, \mathfrak{S}_n)$ for $H^1(\Gamma, \mathfrak{S}_n)$. The antiequivalence $\mathit{Set}_\Gamma^n \equiv \acute{E}t_F^n$ and the bijection (3.1) induce canonical bijections

$$\mathrm{Iso}(\acute{E}t_F^n) \cong \mathrm{Iso}(\mathit{Set}_\Gamma^n) \cong H^1(F, \mathfrak{S}_n)$$

The bijection $\mathrm{Iso}(\acute{E}t_F^n) \cong H^1(F, \mathfrak{S}_n)$ may of course also be defined directly because

$$\mathrm{Aut}_{F\text{-alg}}(F^n) \cong \mathfrak{S}_n,$$

see [12, (29.9)]. Similarly, it follows from (3.2), (3.3), and the antiequivalence of groupoids $\acute{E}tex_F^{d/n} \equiv \mathit{Cov}_\Gamma^{d/n}$, $(\acute{E}tex_F^{d/n})^+ \equiv (\mathit{Cov}_\Gamma^{d/n})^+$, that we have canonical bijections of pointed sets:

$$\mathrm{Iso}(\acute{E}tex_\Gamma^{d/n}) \cong \mathrm{Iso}(\mathit{Cov}_\Gamma^{d/n}) \cong H^1(F, \mathfrak{S}_d \wr \mathfrak{S}_n) \tag{3.4}$$

and

$$\mathrm{Iso}\big((\acute{E}tex_\Gamma^{d/n})^+\big) \cong \mathrm{Iso}\big((\mathit{Cov}_\Gamma^{d/n})^+\big) \cong H^1\big(F, (\mathfrak{S}_d \wr \mathfrak{S}_n)^+\big). \tag{3.5}$$

Remark 3.6. Any group homomorphism $\varphi\colon G \to H$, where G and H are automorphism groups of finite sets or of finite double coverings, induces a map on the level of cocycles $\varphi_*\colon (\gamma\colon \Gamma \to G) \mapsto (\varphi \circ \gamma\colon \Gamma \to H)$. Thus φ associates in a "canonical way" an étale algebra (or an étale algebra with involution) E_φ, whose isomorphism class belongs to $H^1(F, H)$, to an étale algebra E (or an étale algebra E with involution), whose class belongs to $H^1(F, G)$. We say that the algebra E_φ is a *resolvent* of E. For example the discriminant $\Delta(E)$ is the resolvent of E associated to the parity map $\mathfrak{S}_n \to \mathfrak{S}_2$. Other examples of resolvents will be discussed in relation with triality.

4 Triality and Γ-Coverings

Recall the functor C, which associates to any double covering its set of sections. For oriented $2/4$-coverings of Γ-sets, it leads to two functors:

$$C_1, C_2\colon (\mathit{Cov}_\Gamma^{2/4})^+ \to \mathit{Cov}_\Gamma^{2/4},$$

see Proposition 2.6. The functors C_1 and C_2 together with the functor κ, which changes the orientation, give an explicit description of an action of the group $\mathfrak{S}_3$ on the pointed set $\mathrm{Iso}\big((\mathit{Cov}_\Gamma^{2/4})^+\big)$.

Theorem 4.1. *The functors C_1, $C_2\colon (\mathit{Cov}_\Gamma^{2/4})^+ \to \mathit{Cov}_\Gamma^{2/4}$ factor through the forgetful functor $\mathscr{F}\colon (\mathit{Cov}_\Gamma^{2/4})^+ \to \mathit{Cov}_\Gamma^{2/4}$, i.e., there are functors*

$$C_1^+,\, C_2^+\colon (\mathit{Cov}_\Gamma^{2/4})^+ \to (\mathit{Cov}_\Gamma^{2/4})^+$$

such that $\mathscr{F}\circ C_i^+ = C_i$ for $i = 1, 2$. These functors satisfy natural equivalences:

$$(C_1^+)^3 = \mathrm{id}, \qquad (C_1^+)^2 = C_2, \qquad C_1^+\kappa = \kappa C_2^+.$$

Proof. Let $(Z/Z_0,\partial)$ be an object in $(\mathit{Cov}_\Gamma^{2/4})^+$ and let σ denote the involution of Z/Z_0. Consider a real vector space V with basis (e_1,e_2,e_3,e_4). Fixing a bijection φ between a section $\omega\in C_1(Z/Z_0,\partial)$ and $\{e_1,\dots,e_4\}$, we identify Z with a subset of V by:

$$z\mapsto\begin{cases} z^\varphi & \text{if } z\in\omega,\\ -z^{\sigma\varphi} & \text{if } z\notin\omega.\end{cases}$$

Thus, $Z=\{\pm e_1,\pm e_2,\pm e_3,\pm e_4\}$ and σ acts on Z by mapping each element to its opposite. The action of Γ on Z extends to a linear action on V because it commutes with σ. We also identify $C(Z/Z_0)$ with a subset of V by the map

$$\omega'\mapsto \tfrac12\sum_{z\in\omega'} z.$$

The set $C(Z/Z_0)$ then consists of the following vectors and their opposite:

$$\begin{aligned}
f_1 &= \tfrac12(e_1+e_2+e_3+e_4), & g_1 &= \tfrac12(e_1+e_2+e_3-e_4),\\
f_2 &= \tfrac12(e_1+e_2-e_3-e_4), & g_2 &= \tfrac12(e_1+e_2-e_3+e_4),\\
f_3 &= \tfrac12(e_1-e_2+e_3-e_4), & g_3 &= \tfrac12(e_1-e_2+e_3+e_4),\\
f_4 &= \tfrac12(-e_1+e_2+e_3-e_4), & g_4 &= \tfrac12(e_1-e_2-e_3-e_4).
\end{aligned}$$

As $\omega\in C_1(Z/Z_0,\partial)$, we have (see Proposition 2.6)

$$C_1(Z/Z_0,\partial)=\{\pm f_1,\pm f_2,\pm f_3,\pm f_4\}$$

and

$$C_2(Z/Z_0,\partial)=\{\pm g_1,\pm g_2,\pm g_3,\pm g_4\}.$$

The canonical involutions on $C_1(Z/Z_0,\partial)$ and $C_2(Z/Z_0,\partial)$ map each vector to its opposite. Note that these identifications are independent of the choice of the section ω in $C_1(Z/Z_0,\partial)$ and of the bijection φ.

Let ∂_1 be the orientation of $C_1(Z/Z_0,\partial)$ such that $C_1\big(C_1(Z/Z_0,\partial),\partial_1\big)$ contains the section $\{f_1,f_2,f_3,f_4\}$. Thus, by Proposition 2.6, $C_1\big(C_1(Z/Z_0,\partial),\partial_1\big)$ consists of the following sections:

$$\pm\{f_1,f_2,f_3,f_4\},\ \pm\{f_1,f_2,-f_3,-f_4\},\ \pm\{f_1,-f_2,f_3,-f_4\},\ \pm\{-f_1,f_2,f_3,-f_4\}.$$

They are characterized by the property that for each $i = 1, \ldots, 4$ they contain a section $\pm f_j$ containing e_i and a section $\pm f_k$ containing $-e_i$. Identifying these sections to vectors in V as earlier, we obtain

$$C_1\big(C_1(Z/Z_0,\partial),\partial_1\big) = \{\pm\tfrac{1}{2}(f_1+f_2+f_3+f_4), \pm\tfrac{1}{2}(f_1+f_2-f_3-f_4),\\ \pm\tfrac{1}{2}(f_1-f_2+f_3-f_4), \pm\tfrac{1}{2}(-f_1+f_2+f_3-f_4)\}.$$

Likewise, let ∂_2 be the orientation of $C_2(Z/Z_0,\partial)$ such that

$$C_1\big(C_2(Z/Z_0,\partial),\partial_2\big) = \{\pm\tfrac{1}{2}(g_1+g_2+g_3+g_4), \pm\tfrac{1}{2}(g_1+g_2-g_3-g_4),\\ \pm\tfrac{1}{2}(g_1-g_2+g_3-g_4), \pm\tfrac{1}{2}(-g_1+g_2+g_3-g_4)\}.$$

Define the functors $C_1^+, C_2^+ : (\mathsf{Cov}_\Gamma^{2/4})^+ \to (\mathsf{Cov}_\Gamma^{2/4})^+$ by:

$$C_1^+(Z/Z_0,\partial) = \big(C_1(Z/Z_0),\partial_1\big) \qquad \text{and} \qquad C_2^+(Z/Z_0,\partial) = \big(C_2(Z/Z_0),\partial_2\big).$$

By definition, it is clear that $\mathscr{F}\circ C_i^+ = C_i$ for $i = 1, 2$. To establish the natural equivalences, consider the linear map $\mu : V \to V$ defined by $\mu(e_i) = f_i$ for $i = 1, \ldots, 4$. Using this map, we may rephrase the definition of C_1^+ as follows: for $Z = \{\pm e_1, \pm e_2, \pm e_3, \pm e_4\}$ with the orientation ∂ such that $C_1(Z/Z_0,\partial) \ni \mu(e_1)$, we have

$$C_1^+(Z/Z_0,\partial) = \{\pm\mu(e_1), \pm\mu(e_2), \pm\mu(e_3), \pm\mu(e_4)\}$$

with the orientation such that

$$C_1\big(C_1^+(Z/Z_0,\partial)\big) \ni \tfrac{1}{2}\big(\mu(e_1)+\mu(e_2)+\mu(e_3)+\mu(e_4)\big).$$

Note that $\frac{1}{2}\big(\mu(e_1)+\mu(e_2)+\mu(e_3)+\mu(e_4)\big) = \mu(f_1) = \mu^2(e_1)$. Therefore, substituting $\mu(e_i)$ for e_i, for $i = 1, \ldots, 4$, we obtain

$$(C_1^+)^2(Z/Z_0,\partial) = \{\pm\mu^2(e_1), \pm\mu^2(e_2), \pm\mu^2(e_3), \pm\mu^2(e_4)\},$$

endowed with an orientation such that

$$C_1\big((C_1^+)^2(Z/Z_0,\partial)\big) \ni \mu^3(e_1).$$

Computation shows that $\mu^2(e_i) = g_i$ for $i = 1, \ldots, 4$, and $\mu^3 = \mathrm{Id}$. As $\frac{1}{2}(g_1+g_2+g_3+g_4) = e_1$, it follows that $(C_1^+)^2(Z/Z_0,\partial) = C_2^+(Z/Z_0,\partial)$. Similarly, we have

$$(C_1^+)^3(Z/Z_0,\partial) = \{\pm\mu^3(e_1), \pm\mu^3(e_2), \pm\mu^3(e_3), \pm\mu^3(e_4)\} = Z,$$

endowed with an orientation such that

$$C_1\big((C_1^+)^3(Z/Z_0,\partial)\big) \ni \mu^4(e_1) = f_1,$$

hence $(C_1^+)^3(Z/Z_0,\partial) = (Z/Z_0,\partial)$. Finally, we have

$$\kappa(Z/Z_0,\partial) = \{\pm e_1, \pm e_2, \pm e_3, \pm e_4\}$$

with an orientation such that $C_1\kappa(Z/Z_0,\partial) \ni \mu^2(e_1)$, hence

$$C_1^+\kappa(Z/Z_0,\partial) = \{\pm\mu^2(e_1), \pm\mu^2(e_2), \pm\mu^2(e_3), \pm\mu^2(e_4)\}$$

endowed with an orientation such that

$$C_1\big(C_1^+\kappa(Z/Z_0,\partial)\big) \ni \mu^4(e_1) = f_1.$$

Therefore, $C_1^+\kappa(Z/Z_0,\partial) = \kappa C_2^+(Z/Z_0,\partial)$. □

Remark 4.2. The decomposition

$$C(Z/Z_0) = C_1(Z/Z_0,\partial) \sqcup C_2(Z/Z_0,\partial)$$

can also be viewed geometrically on a hypercube: Suppose $V = \mathbb{R}^4$ and write (e_1,e_2,e_3,e_4) for the standard basis. The set

$$C(Z/Z_0) = \{\tfrac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4)\}$$

is the set of vertices of a hypercube $\mathscr{K}$ depicted in Fig. 1, and the set $Z = \{\pm e_1, \pm e_2, \pm e_3, \pm e_4\}$ is in bijection with the set of 3-dimensional cells of $\mathscr{K}$.

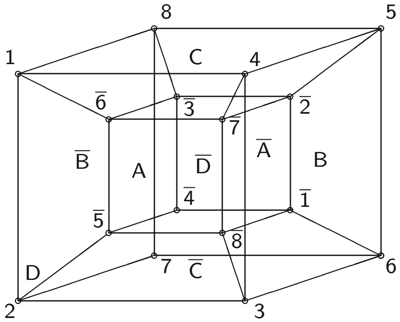


Fig. 1 Hypercube

We identify

$$Z = \{A, \bar{A}, B, \bar{B}, C, \bar{C}, D, \bar{D}\},$$

where $A,\dots,\bar{C}$ are as in Fig. 1, D is the big cell and $\bar{D}$ the small cell inside. The involution permutes a cell with its opposite cell and the set Z_0 is obtained by identifying pairs of opposite cells

$$Z_0 = \{\{A,\bar{A}\},\{B,\bar{B}\},\{C,\bar{C}\},\{D,\bar{D}\}\}.$$

To obtain a corresponding identification of $C(Z/Z_0)$ with the set of vertices of $\mathscr{K}$, observe that a section of Z/Z_0 consists of a set of four cells which are pairwise not opposite. Four such cells intersect in exactly one vertex and conversely each vertex lies in four cells. With the notation in Fig. 1 we have the following identification:

$$\begin{array}{llll}
1=\{A,\bar B,C,D\} & \bar 1=\{\bar A,B,\bar C,\bar D\} & 2=\{A,\bar B,\bar C,D\} & \bar 2=\{\bar A,B,C,\bar D\}\\
3=\{A,B,\bar C,D\} & \bar 3=\{\bar A,\bar B,C,\bar D\} & 4=\{A,B,C,D\} & \bar 4=\{\bar A,\bar B,\bar C,\bar D\}\\
5=\{\bar A,B,C,D\} & \bar 5=\{A,\bar B,\bar C,\bar D\} & 6=\{\bar A,B,\bar C,D\} & \bar 6=\{A,\bar B,C,\bar D\}\\
7=\{\bar A,\bar B,\bar C,D\} & \bar 7=\{A,B,C,\bar D\} & 8=\{\bar A,\bar B,C,D\} & \bar 8=\{A,B,\bar C,\bar D\}
\end{array}$$

This set of vertices decomposes into two classes, two vertices being in the same class if the number of edges in any path connecting them is even. One class is

$$X=\{1,\bar 1,3,\bar 3,5,\bar 5,7,\bar 7\}$$

and the other

$$Y=\{2,\bar 2,4,\bar 4,6,\bar 6,8,\bar 8\}.$$

We get coverings X/X_0 and Y/Y_0 by identifying opposite vertices v and $\bar v$. If $\Delta(Z)\simeq \mathbf{2}$, the decomposition of $C(Z/Z_0)$ as the disjoint union $X/X_0\sqcup Y/Y_0$ is Γ-compatible; the functors C_1 and C_2 are given (up to a possible permutation) by the rule

$$C_1(Z/Z_0,\partial)=X/X_0 \qquad\text{and}\qquad C_2(Z/Z_0,\partial)=Y/Y_0.$$

A section of X/X_0 is a set of four vertices in X which are pairwise not opposite. Four such vertices either lie on a 3-dimensional cell or are adjacent to exactly one vertex in the complementary set Y. A similar claim holds for a section of Y/Y_0. This leads to identifying:

$$\begin{array}{ll}
A=\{1,3,\bar 5,\bar 7\}=\{2,4,\bar 6,\bar 8\} & \bar A=\{\bar 1,\bar 3,5,7\}=\{\bar 2,\bar 4,6,8\}\\
B=\{\bar 1,3,5,\bar 7\}=\{\bar 2,4,6,\bar 8\} & \bar B=\{1,\bar 3,\bar 5,7\}=\{2,\bar 4,\bar 6,8\}\\
C=\{1,\bar 3,5,\bar 7\}=\{\bar 2,4,\bar 6,8\} & \bar C=\{\bar 1,3,\bar 5,7\}=\{2,\bar 4,6,\bar 8\}\\
D=\{1,3,5,7\}=\{2,4,6,8\} & \bar D=\{\bar 1,\bar 3,\bar 5,\bar 7\}=\{\bar 2,\bar 4,\bar 6,\bar 8\}
\end{array}\tag{4.3}$$

and

$$\begin{array}{ll}
1=\{A,\bar B,C,D\}=\{2,4,\bar 6,8\} & \bar 1=\{\bar A,B,\bar C,\bar D\}=\{\bar 2,\bar 4,6,\bar 8\}\\
3=\{A,B,\bar C,D\}=\{2,4,6,\bar 8\} & \bar 3=\{\bar A,\bar B,C,\bar D\}=\{\bar 2,\bar 4,\bar 6,8\}\\
5=\{\bar A,B,C,D\}=\{\bar 2,4,6,8\} & \bar 5=\{A,\bar B,\bar C,\bar D\}=\{2,\bar 4,\bar 6,\bar 8\}\\
7=\{\bar A,\bar B,\bar C,D\}=\{2,\bar 4,6,8\} & \bar 7=\{A,B,C,\bar D\}=\{\bar 2,4,\bar 6,\bar 8\}\\[4pt]
2=\{A,\bar B,\bar C,D\}=\{1,3,\bar 5,7\} & \bar 2=\{\bar A,B,C,\bar D\}=\{\bar 1,\bar 3,5,\bar 7\}\\
4=\{A,B,C,D\}=\{1,3,5,\bar 7\} & \bar 4=\{\bar A,\bar B,\bar C,\bar D\}=\{\bar 1,\bar 3,\bar 5,7\}\\
6=\{\bar A,B,\bar C,D\}=\{\bar 1,3,5,7\} & \bar 6=\{A,\bar B,C,\bar D\}=\{1,\bar 3,\bar 5,\bar 7\}\\
8=\{\bar A,\bar B,C,D\}=\{1,\bar 3,5,7\} & \bar 8=\{A,B,\bar C,\bar D\}=\{\bar 1,3,\bar 5,\bar 7\},
\end{array}\tag{4.4}$$

hence the existence of decompositions $C(X/X_0)=Y/Y_0\sqcup Z/Z_0$ and $C(Y/Y_0)=Z/Z_0\sqcup X/X_0$ which, in fact, are decompositions as Γ-sets.

Remark 4.5. In the proof of Theorem 4.1, μ is not the only linear map that can be used to describe the C_1^+ and the C_2^+ construction. An alternative description uses

Hurwitz' quaternions. Choosing for V the skew field of real quaternions $\mathbb{H}$ and for (e_1, e_2, e_3, e_4) the standard basis $(1, i, j, k)$, we have

$$Z = \{\pm 1, \pm i, \pm j, \pm k\}, \qquad C(Z/Z_0) = \{\tfrac{1}{2}(\pm 1 \pm i \pm j \pm k)\},$$

so the union $Z \cup C(Z/Z_0) \subset \mathbb{H}$ is the group $\mathbb{H}^1$ of Hurwitz integral quaternions of norm 1. The element

$$\rho = -\tfrac{1}{2}(1 + i + j + k)$$

is of order 3 in $\mathbb{H}^1$ and conjugation by ρ permutes i, j, and k cyclically. The set Z is in fact the underlying set of the quaternionic group $\mathfrak{Q}_8$ and

$$\mathbb{H}^1 = \mathfrak{Q}_8 \rtimes \mathfrak{C}_3,$$

where the cyclic group of three elements $\mathfrak{C}_3$ operates on $\mathfrak{Q}_8$ via conjugation with ρ. If ∂ is the orientation of Z/Z_0 such that $\rho \in C_1(Z/Z_0, \partial)$, we have $C_1^+(Z/Z_0, \partial) = \rho \cdot Z$ with the orientation such that $\rho^2 \in C_1\big(C_1^+(Z/Z_0, \partial)\big)$, and $C_2^+(Z/Z_0, \partial) = (C_1^+)^2(Z/Z_0, \partial) = \rho^2 \cdot Z$ with the orientation such that $1 \in C_1\big(C_2^+(Z/Z_0, \partial)\big)$. Note that, with respect to the standard basis, multiplication by ρ is given by the matrix

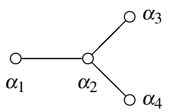
$$\rho = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 \end{pmatrix} \tag{4.6}$$

whereas the matrix of μ is

$$\mu = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{pmatrix}. \tag{4.7}$$

5 The Weyl Group of D_4

The Dynkin diagram D_4



(5.1)

has the permutation group $\mathfrak{S}_3$ as a group of automorphisms. The vertices of the diagram are labeled by the simple roots of the Lie algebra of type D_4. Let (e_1, e_2, e_3, e_4) be the standard orthonormal basis of the Euclidean space $\mathbb{R}^4$. The simple roots are

$$\alpha_1 = e_1 - e_2, \quad \alpha_2 = e_2 - e_3, \quad \alpha_3 = e_3 - e_4, \quad \text{and} \quad \alpha_4 = e_3 + e_4$$

(see [3]). The permutation $\alpha_1 \mapsto \alpha_4,\ \alpha_4 \mapsto \alpha_3,\ \alpha_3 \mapsto \alpha_1,\ \alpha_2 \mapsto \alpha_2$ is an automorphism of order 3 of the Dynkin diagram. Its extension to a linear automorphism of $\mathbb{R}^4$ is given by the orthogonal matrix μ of (4.7). The matrix

$$\nu = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{5.2}$$

extends the automorphism $\alpha_1 \mapsto \alpha_1,\ \alpha_4 \mapsto \alpha_3,\ \alpha_3 \mapsto \alpha_4,\ \alpha_2 \mapsto \alpha_2$. The set $\{\mu, \nu\}$ generates a subgroup of O_4 isomorphic to $\mathfrak{S}_3$, which restricts to the automorphism group of the Dynkin diagram. The group

$$W(D_4) = (\mathfrak{S}_2 \wr \mathfrak{S}_4)^+ = \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4$$

is the Weyl group of the split adjoint algebraic group PGO_8^+, which is of type D_4.

As a subgroup of the orthogonal group O_4, the group $W(D_4)$ is generated by the reflections with respect to the roots of the Lie algebra of PGO_8^+. Elements of $\mathfrak{S}_2 \wr \mathfrak{S}_4$ can be written as matrix products

$$w = D \cdot P(\pi), \tag{5.3}$$

where D is the diagonal matrix $\mathrm{diag}(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$, $\varepsilon_i = \pm 1$, and $P(\pi)$ is the permutation matrix of $\pi \in \mathfrak{S}_4$. The group $\mathfrak{S}_2 \wr \mathfrak{S}_4$ fits into the exact sequence

$$1 \to \mathfrak{S}_2^4 \to \mathfrak{S}_2 \wr \mathfrak{S}_4 \xrightarrow{\beta} \mathfrak{S}_4 \to 1, \tag{5.4}$$

where β maps $w = D \cdot P(\pi)$ to π. Elements of $W(D_4)$ have a similar representation, with the supplementary condition $\prod_i \varepsilon_i = 1$.

In relation with the geometric description of C_1 and C_2 at the end of Sect. 4, note that the group $\mathfrak{S}_2 \wr \mathfrak{S}_4 = \mathfrak{S}_2^4 \rtimes \mathfrak{S}_4$ is the group of automorphisms of the hypercube $\mathscr{K}$. The subgroup $W(D_4) = (\mathfrak{S}_2 \wr \mathfrak{S}_4)^+ = \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4$ consists of the automorphisms of $\mathscr{K}$ respecting the decomposition of the set of vertices as $X \sqcup Y$, i.e., automorphisms of the half-hypercube.

Automorphisms of $W(D_4)$

We view $W(D_4)$ as a subgroup of O_4 as in (5.3). Conjugation $x \mapsto \mu x \mu^{-1}$ with the matrices μ and ν on O_4 induce by restriction outer automorphisms $\tilde{\mu}$ and $\tilde{\nu}$ of $W(D_4)$. The set $\{\tilde{\mu}, \tilde{\nu}\}$ generates a group of automorphisms of $W(D_4)$ isomorphic to $\mathfrak{S}_3$ (see already [5, p. 368]). The center of $W(D_4)$ is isomorphic to $\mathfrak{S}_2$ and is generated by:

$$w_0 = \mathrm{diag}(-1, -1, -1, -1) = -1. \tag{5.5}$$

Thus, $W(D_4)/\langle w_0\rangle$ acts on $W(D_4)$ as the group of inner automorphisms. Let ψ be the automorphism of order 2 of $W(D_4)$ given by:

$$\psi\colon D\cdot P(\pi)\mapsto D\cdot P(\pi)\cdot (w_0)^{\operatorname{sgn}(\pi)},$$

or equivalently by $x\mapsto x\det(x)$, $x\in W(D_4)\subset \mathrm{O}_4$. A proof of the following result can be found in [9, Theorem 31,(5)] or in [8, Prop. 2.8,(e)]:

Proposition 5.6.

$$\operatorname{Aut}\big(W(D_4)\big)\simeq \big((W(D_4)/\langle w_0\rangle)\rtimes \mathfrak{S}_3\big)\times\langle\psi\rangle.$$

For any $w\in W(D_4)$, we let $\operatorname{Int}(w)\colon x\mapsto wxw^{-1}$ be the inner automorphism of $W(D_4)$ defined by conjugation by w, and by $\operatorname{Int}\big(W(D_4)\big)$ the group of inner automorphisms of $W(D_4)$. As an immediate consequence of Proposition 5.6, we have

Corollary 5.7.

$$\operatorname{Aut}\big(W(D_4)\big)/\operatorname{Int}\big(W(D_4)\big)\simeq \mathfrak{S}_3\times\langle\psi\rangle.$$

We call *trialitarian* the outer automorphisms of order 3 of $W(D_4)$. As observed earlier, the automorphisms $\tilde{\mu}$ and $\tilde{\mu}^2$ are trialitarian. Conjugation by the matrix ρ of (4.6) also yields a trialitarian automorphism $\tilde{\rho}$: indeed, we have $\rho^3=1$ and

$$\rho\mu^{-1}=-1\cdot\begin{pmatrix}0&0&0&1\\0&1&0&0\\1&0&0&0\\0&0&1&0\end{pmatrix}\in W(D_4);$$

hence, letting w be the matrix on the right side, we have $\tilde{\rho}=\operatorname{Int}(w)\circ\tilde{\mu}$.

Proposition 5.8. *Any trialitarian automorphism of $W(D_4)$ is conjugate in the group* $\operatorname{Aut}\big(W(D_4)\big)$ *to either $\tilde{\mu}$ or $\tilde{\rho}$.*

Proof. Explicit computation (with the help of the algebra computational system Magma [2]) shows that the conjugation class of $\tilde{\rho}$ contains 16 elements and the conjugation class of $\tilde{\mu}$ contains 32 elements. In view of Proposition 5.6 any trialitarian automorphism of $W(D_4)$ is the restriction to $W(D_4)$ of conjugation by an element $u\in\mathrm{O}_4$ of the form $u=\mu\cdot w$ or $u=\mu^2\cdot w$, with $w\in W(D_4)$ and $u^3=1$. There are 48 elements u of this form, hence the claim. □

Corollary 5.9. *There are up to isomorphism two types of subgroups of fixed points of trialitarian automorphisms of $W(D_4)$, those isomorphic to* $\operatorname{Fix}(\tilde{\mu})$ *and those isomorphic to* $\operatorname{Fix}(\tilde{\rho})$.

Proof. Trialitarian automorphisms which are conjugate in $\operatorname{Aut}\big(W(D_4)\big)$ have isomorphic groups of fixed points. □

Proposition 5.10. *1) The 2-dimensional subspace of $\mathbb{R}^4$ generated by the set of elements $\{e_1+e_3, e_2-e_3\}$ is fixed under μ.*
2) The set $\{e_1+e_3, e_2-e_3\}$ generates a root system of type G_2 and the group $\mathrm{Fix}(\tilde{\mu})$ is the corresponding Weyl group, which is the dihedral group $\mathfrak{D}_6$ of order 12.

Proof. By explicit computation. □

Proposition 5.11. *The group $\mathrm{Fix}(\tilde{\rho})$ is isomorphic to the group of order 24 of Hurwitz quaternions $\mathbb{H}^1 = \mathfrak{Q}_8 \rtimes \mathfrak{C}_3$. This group is isomorphic to the double covering $\tilde{\mathfrak{A}}_4$ of $\mathfrak{A}_4$.*

Proof. Recall that the matrix ρ is obtained by choosing $(1,i,j,k)$ as basis of $\mathbb{R}^4$ and letting $-\frac{1}{2}(1+i+j+k)$ operate by left multiplication in $\mathbb{H}$. The group $\mathbb{H}^1$ has a representation in $W(D_4)$ by right multiplication which obviously commutes with the action of ρ. Hence, $\mathrm{Fix}(\tilde{\rho})$ contains a copy of $\mathbb{H}^1$. The claim then follows from the fact that $\mathrm{Fix}(\tilde{\rho})$ has 24 elements. □

Cohomology with $W(D_4)$ Coefficients

Each automorphism $\alpha \in \mathrm{Aut}\big(W(D_4)\big)$ acts on $H^1\big(\Gamma, W(D_4)\big)$ by:

$$\alpha_*\colon [\varphi] \mapsto [\alpha \circ \varphi],$$

where $\varphi\colon \Gamma \to W(D_4)$ is a cocycle with values in $W(D_4)$. If $\alpha' = \mathrm{Int}(w) \circ \alpha$ for some $w \in W(D_4)$, then for all cocycles $\varphi\colon \Gamma \to W(D_4)$ we have

$$w \cdot \alpha\big(\varphi(\gamma)\big) \cdot w^{-1} = \alpha'\big(\varphi(\gamma)\big) \qquad \text{for all } \gamma \in \Gamma,$$

hence $[\alpha \circ \varphi] = [\alpha' \circ \varphi]$ and therefore $\alpha_* = \alpha'_*$. Thus, the action of $\mathrm{Aut}\big(W(D_4)\big)$ on $H^1\big(\Gamma, W(D_4)\big)$ factors through $\mathrm{Aut}\big(W(D_4)\big)/\mathrm{Int}\big(W(D_4)\big) \simeq \mathfrak{S}_3 \times \langle\psi\rangle$. In particular the symmetric group $\mathfrak{S}_3$ acts on $H^1\big(\Gamma, W(D_4)\big)$. Under the bijections (3.5), the symmetric group $\mathfrak{S}_3$ also acts on $\mathrm{Iso}\big((\mathit{Cov}_\Gamma^{2/4})^+\big)$ and $\mathrm{Iso}\big((\acute{E}\mathit{tex}_\Gamma^{2/4})^+\big)$. The action of the outer automorphism $\tilde{\nu}$ associates to the oriented 2/4-covering $(Z/Z_0, \partial_Z)$ the oriented covering $\kappa(Z/Z_0, \partial) = (Z/Z_0, \partial_Z \circ \iota)$ where $\mathbf{2} \xleftarrow{\iota} \mathbf{2}$ twists the orientation. The proof of Theorem 4.1 shows that the action of $\tilde{\mu}$ maps the class of an oriented covering $(Z/Z_0, \partial_Z)$ to the class of $C_1^+(Z/Z_0, \partial_Z)$.

6 Triality and étale Algebras

We next investigate triality on isomorphism classes of étale algebras using Galois cohomology. Oriented extensions of étale algebras S/S_0 with $\dim_F S = 8$ and $\dim_F S_0 = 4$ correspond to cocycles, i.e., continuous homomorphisms $\Gamma \to W(D_4)$, and isomorphism classes of such algebras correspond to cocycles up to conjugation. If the cocycle factors through a subgroup G of $W(D_4)$, the conjugacy class of G in $W(D_4)$ is determined by the isomorphism class of the algebra. Thus, it makes sense to classify isomorphism classes of algebras according to the conjugacy classes of the subgroups G of $W(D_4)$.

We give in Table 1 a list of all conjugacy classes of subgroups of $W(D_4)$. We still consider $W(D_4)$ as a subgroup of O_4 (see (5.3)) and use the following notation. The group $W(D_4)$ fits into the split exact sequence:

$$1 \to \mathfrak{S}_2^3 \to W(D_4) \xrightarrow{\beta} \mathfrak{S}_4 \to 1, \tag{6.1}$$

where β is as in (5.4). For each subgroup G of $W(D_4)$ we denote by G_1 the restriction $G \cap \mathfrak{S}_2^3$ and by G_0 the projection $\beta(G)$. The center of $W(D_4)$, generated by $w_0 = \mathrm{diag}(-1,-1,-1,-1) = -1$ is denoted by C and we set $w_1 = \mathrm{diag}(1,-1,1,-1)$, $w_2 = \mathrm{diag}(1,-1,-1,1)$, and $w_3 = \mathrm{diag}(-1,-1,1,1)$ for special elements of the subgroup $\mathfrak{S}_2^3 \subset W(D_4)$ given by diagonal matrices. We denote by $\mathfrak{S}_n$ the permutation group of n elements, $\mathfrak{A}_n$ is the alternating subgroup, $\mathfrak{C}_n$ is cyclic of order n, $\mathfrak{D}_n$ is the dihedral group of order $2n$, $\mathfrak{V}_4$ is the Klein 4-group, and $\mathfrak{Q}_8$ is the quaternionic group with eight elements. We refer to [6] for a description of the groups $[2^2]4$ and $\mathfrak{Q}_8 : 2$ in Table 1. In Column S we summarize the various possibilities for étale algebras of dimension 8 associated to the class of a cocycle $\alpha\colon \Gamma \to W$ which factors through G and in Column S_0 étale algebras of dimension 4 associated to the class of the induced cocycle $\beta \circ \alpha\colon \Gamma \to \mathfrak{S}_4$ which factors through G_0. The entry K in one of the columns S or S_0 denotes a quadratic separable field extension. We use symbols E, respectively E_0 for separable field extensions whose Galois closures have Galois groups G, respectively G_0. The symbol $R(E)$ stands for the cubic resolvent of E if E is a quartic separable field extension and $\lambda^2 E$ stands for the second lambda power of E (see [13], where it is denoted $\Lambda_2(E)$ or [10], where it is denoted $E(2)$[4]). If $\dim_F E = 4$, $\lambda^2 E$ admits an involution σ and for any quadratic étale algebra K with involution ι we set $K * \lambda^2 E = (K \otimes_F \lambda^2 E)^{\iota \otimes \sigma}$. We write $\overline{E}_0$ for the Galois closure of E_0. The symbol ℓ gives the number of subgroups in the conjugacy class of G, MS refers to the maximal subgroups of G and in column T we give the two conjugacy classes which are the images of the class of G under the trialitarian automorphisms $\tilde{\mu}$ and $\tilde{\mu}^2$.

Entries N, $|G|$, ℓ, and MS in the table were generated with the help of the Magma algebra software [2]. The computation of the entry T, the explicit representation of the group G as an exact sequence and the decomposition of the étale algebras as products of fields were checked case by case.

Explicit computations of trialitarian triples were made in [1] and [20] using the description of the trialitarian action given in the proof of Theorem 4.1.

[4] The corresponding Γ-set $\lambda^2 X$ is obtained by removing the diagonal from $X \times X$ and dividing by the involution $(x,y) \mapsto (y,x)$.

Trialitarian Triples and Fixed Points

Let α be any trialitarian automorphism of $W(D_4)$. The subset $H^1\big(\Gamma, W(D_4)\big)^{\mathfrak{C}_3}$ of cohomology classes that are fixed under α_* is independent of the particular choice of α. Clearly, the image in $H^1\big(\Gamma, W(D_4)\big)$ of any cohomology class in $H^1\big(\Gamma, \mathrm{Fix}(\alpha)\big)$ is fixed under α_*, hence this image lies in $H^1\big(\Gamma, W(D_4)\big)^{\mathfrak{C}_3}$. Thus, we have a canonical map

$$H^1\big(F, \mathrm{Fix}(\alpha)\big) \to H^1\big(F, W(D_4)\big)^{\mathfrak{C}_3} \tag{6.2}$$

for any trialitarian automorphism α of $W(D_4)$.

Theorem 6.3. *Any class in $H^1\big(F, W(D_4)\big)^{\mathfrak{C}_3}$ lies in the image of the map* (6.2) *for $\alpha = \tilde{\mu}$ or $\alpha = \tilde{\rho}$ as in* (5.8)*.*

Proof. If the class $[\varphi]$ of a cocycle $\varphi\colon \Gamma \to W(D_4)$ belongs to $H^1\big(\Gamma, W(D_4)\big)^{\mathfrak{C}_3}$, the cocycle factors through a subgroup G whose conjugacy class is invariant under $\tilde{\mu}$. We get from Columns N and T of Table 1 a list of all triples of conjugate classes of subgroups $W(D_4)$ which are permuted by a trialitarian automorphism of $W(D_4)$.

A triple consists of three identic labels (for example $(70,70,70)$) if there exists $a \in W(D_4)$ such that

$$\mu G \mu^{-1} = aGa^{-1},$$

where μ is as in (4.7). A cocycle factoring through such a group G does not necessarily correspond to a triple of isomorphism classes of étale algebras fixed under triality. For a triple consisting of isomorphic algebras we must have $a \in W(D_4)$ such that

$$\mu x \mu^{-1} = axa^{-1} \tag{6.4}$$

for all $x \in G$, since isomorphic classes of algebras are given by homomorphisms $\gamma\colon \Gamma \to G$ up to conjugation. Thus, a necessary condition to get a triple of fixed isomorphism classes of algebras is that the conjugacy classes of all subgroups H of G are invariant under triality. The conjugacy classes $N = 24$, 39, 53, 56, 65, 70, 86, 96, 97, and 98 do not correspond to triples of isomorphism classes of algebras invariant under triality. The conjugacy classes left over in Table 1 are $N = 1$, 2, 6, 7, 8, 20, 29, 30, 31, 32, 36, 61, and 85. They give rise to triples of isomorphism classes of étale algebras fixed under triality, because they correspond to subgroups contained in $\mathrm{Fix}(\tilde{\mu})$ $(N = 61)$ or contained in $\mathrm{Fix}(\tilde{\rho})$ $(N = 85)$. □

Observe that fixed étale algebras in class $N = 61$ are of the form $K \times (E_0 \otimes K)$, where K is quadratic and E_0 is cubic. Hence they are not fields over F, in contrast to algebras in class $N = 85$.

Table 1 List of isomorphism classes of étale algebras corresponding to the conjugacy classes of subgroups of $W(D_4)$, together with a description of the triality action

N	S_0	S	$G_1 \to G \to G_0$	$\lvert G\rvert$	ℓ	MS	T
1	F^4	F^8	$1 \to 1 \to 1$	1	1	1	1, 1
2	F^4	K^4	$C \to \mathfrak{S}_2 \to 1$	2	6	1	2, 2
3	K^2	K^4	$1 \to \mathfrak{S}_2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	2	6	1	3, 5
4	K^2	K^4	$1 \to \mathfrak{S}_2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	2	6	1	4, 3
5	F^4	$F^2 \times K^2$	$\langle w_1\rangle \to \mathfrak{S}_2 \to 1$	2	6	1	5, 4
6	$F^2 \times K$	$F^2 \times K^2$	$1 \to \mathfrak{S}_2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	2	12	1	6, 6
7	$F^2 \times K$	$F^2 \times K^2$	$1 \to \mathfrak{S}_2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	2	12	1	7, 7
8	$F \times E_0$	$F^2 \times S_0^2$	$1 \to \mathfrak{C}_3 \to \mathfrak{C}_3$	3	16	1	8, 8
9	F^4	$K_1^2 \times K_2^2$	$\langle C, w_1\rangle \to \mathfrak{S}_2^2 \to 1$	4	3	2 5	11, 10
10	K^2	$K \otimes K_1^2$	$C \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	4	3	2 3	9, 11
11	K^2	$K \otimes K_1^2$	$C \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	4	3	2 4	10, 9
12	$K_1 \otimes K_2$	$K_1 \otimes K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{V}_4$	4	4	4	14, 13
13	F^4	$K_1^2 \times K_2^2$	$\langle w_1, w_2\rangle \to \mathfrak{S}_2^2 \to 1$	4	4	5	12, 14
14	$K_1 \otimes K_2$	$K_1 \otimes K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{V}_4$	4	4	3	13, 12
15	$F^2 \times K$	$F^4 \times K_1 \otimes K$	$\langle w_1\rangle \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	6	5 6	18, 17
16	$K_1 \times K_2$	$K_1 \otimes K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	6	4 7	21, 19
17	$K_1 \times K_2$	$K_1^2 \times K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	6	3 6	15, 18
18	$K_1 \times K_2$	$K_1^2 \times K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	6	4 6	17, 15
19	$F^2 \times K$	$K_1^2 \times K_1 \times K$	$\langle w_1\rangle \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	6	5 7	16, 21
20	K^2	E^2	$C \to \mathfrak{C}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	4	2	2	20, 20
21	$K_1 \times K_2$	$K_1 \otimes K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	6	3 7	19, 16
22	$K_1 \times K_2$	$K_1^2 \times K_1 \otimes K_2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	12	4 6 7	23, 27
23	$K_1 \times K_2$	$K_1^2 \times K_1 \otimes K_2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	12	3 6 7	27, 22
24	K^2	$K^2 \times K \otimes K_1$	$\langle w_1\rangle \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	4	12	3 4 5	24, 24
25	$F^2 \times K$	$F^4 \times E$	$\langle w_1\rangle \to \mathfrak{C}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	12	5	26, 28
26	E_0	E_0^2	$1 \to \mathfrak{C}_4 \to \mathfrak{C}_4$	4	12	4	28, 25
27	$F^2 \times K$	$K_1^2 \times K_1 \otimes K$	$\langle -w_1\rangle \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	12	5 6 7	22, 23
28	E_0	$E_0 \times E_0$	$1 \to \mathfrak{C}_4 \to \mathfrak{C}_4$	4	12	3	25, 26
29	$F^2 \times K$	$K^2 \times K \otimes K_1$	$C \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	12	2 6 7	29, 29
30	$F \times E_0$	$F^2 \times E_0 \otimes \Delta(E_0)$	$1 \to \mathfrak{S}_3 \to \mathfrak{S}_3$	6	16	7 8	30, 30
31	$F \times E_0$	$F^2 \times E$	$C \to \mathfrak{C}_6 \to \mathfrak{C}_3$	6	16	2 8	31, 31
32	$F \times E_0$	$F^2 \times E_0^2$	$1 \to \mathfrak{S}_3 \to \mathfrak{S}_3$	6	16	6 8	32, 32
33	E_0	E	$C \to \mathfrak{S}_2^3 \to \mathfrak{V}_4$	8	1	11 12	34, 35
34	E_0	E	$C \to \mathfrak{S}_2^3 \to \mathfrak{V}_4$	8	1	10 14	35, 33
35	F^4	$K_1 \times K_2 \times K_3 \times K_{123}$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \to 1$	8	1	9 13	33, 34
36	E_0	E	$C \to \mathfrak{Q}_8 \to \mathfrak{V}_4$	8	2	20	36, 36
37	K^2	$E_1 \times E_2$	$\langle C, w_1\rangle \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	8	3	3 20	38, 40
38	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{C}_4$	8	3	11 20	40, 37
39	K^2	$K \otimes K_1 \times K \otimes K_2$	$\langle C, w_1\rangle \to \mathfrak{S}_2^3 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	8	3	9 10 11 24	39, 39
40	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{C}_4$	8	3	10 20	37, 38
41	K^2K	E^2	$\langle C, w_2\rangle \to \mathfrak{D}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	8	6	9 11 20	49, 45
42	$F^2 \times K$	$K_1 \times E$	$\langle C, w_1\rangle \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	8	6	9 25	44, 47
43	$K_1 \times K_2$	$K \otimes K_1 \times K \otimes K_2$	$C \to \mathfrak{S}_2^3 \to \mathfrak{S}_2^2$	8	6	10 17 21 23 29	48, 46
44	E_0	E	$C \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{C}_4$	8	6	11 26	47, 42
45	K^2	E^2	$\langle C, w_2\rangle \to \mathfrak{D}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	8	6	9 10 20	41, 49
46	$K_1 \times K_2$	$K \otimes K_1 \times K \otimes K_2$	$C \to \mathfrak{S}_2^3 \to \mathfrak{S}_2^2$	8	6	11 16 18 22 29	43, 48
47	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{C}_4$	8	6	10 28	42, 44

(continued)

Table 1 (continued)

N	S_0	S	$G_1 \to G \to G_0$	$\lvert G\rvert$	ℓ	MS	T
48	$F^2 \times K$	$K_1^2 \times K \otimes K_2$	$\langle C, w_1\rangle \to \mathfrak{S}_2^3 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	8	6	9 15 19 27 29	$46, 43$
49	E_0	E	$C \to \mathfrak{D}_4 \to \mathfrak{V}_4$	8	6	10 11 20	$45, 41$
50	$F^2 \times K$	$K^2 \times E$	$\langle w_1, w_2\rangle \to \mathfrak{D}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	8	6	13 19 25	$55, 51$
51	E_0	E	$1 \to \mathfrak{D}_4 \to \mathfrak{D}_4$	8	12	14 21 28	$50, 55$
52	E_0	E_0^2	$1 \to \mathfrak{D}_4 \to \mathfrak{D}_4$	8	12	14 17 28	$54, 57$
53	$K_1 \times K_2$	$K \otimes K_1 \times K \otimes K_2$	$\langle w_1\rangle \to \mathfrak{S}_2^3 \to \mathfrak{S}_2^2$	8	12	16 19 21 22 23 24 27	$53, 53$
54	$F^2 \times K$	$F^2 \times K \times E$	$\langle w_1, w_2\rangle \to \mathfrak{D}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	8	12	13 15 25	$57, 52$
55	E_0	$\bar{E}_0$	$1 \to \mathfrak{D}_4 \to \mathfrak{D}_4$	8	12	12 16 26	$51, 50$
56	$K_1 \times K_2$	$K_1^2 \times E$	$\langle w_1\rangle \to \mathfrak{S}_2^3 \to \mathfrak{S}_2^2$	8	12	15 17 18 22 23 24 27	$56, 56$
57	E_0	E_0^2	$1 \to \mathfrak{D}_4 \to \mathfrak{D}_4$	8	12	12 18 26	$52, 54$
58	E_0	E_0^2	$1 \to \mathfrak{A}_4 \to \mathfrak{A}_4$	12	4	8 14	$59, 60$
59	$F \times E_0$	$F^2 \times E_0^2$	$\langle w_1, w_2\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{C}_3 \to \mathfrak{C}_3$	12	4	8 13	$60, 58$
60	E_0	E_0^2	$1 \to \mathfrak{A}_4 \to \mathfrak{A}_4$	12	4	8 12	$58, 59$
61	$F \times E_0$	$K \times K \otimes E_0$	$C \to \mathfrak{S}_2 \times \mathfrak{S}_3 \to \mathfrak{S}_3$	12	4	$29, 30, 31, 32$	$61, 61$
62	$K_1 \times K_2$	E^2	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{S}_2^2$	16	3	39 42	$66, 63$
63	E_0	E	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{C}_4$	16	3	39 47	$62, 66$
64	K^2	$E_1 \times E_2$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	16	3	35 37 39 41 45	$68, 67$
65	$K_1 \times K_2$	$K_1 \otimes K_3 \times K_2 \otimes K_4$	$\langle C, w_1\rangle \to \mathfrak{S}_2^4 \to \mathfrak{S}_2^2$	16	3	39 43 46 48 53 56	$65, 65$
66	E_0	E	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{C}_4$	16	3	39 44	$63, 62$
67	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{V}_4$	16	3	34 39 40 45 49	$64, 68$
68	E_0	E	$\langle C, w_2\rangle \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{V}_4$	16	3	33 38 39 41 49	$67, 64$
69	$K_1 \times K_2$	E^2	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{S}_2^2$	16	6	37 42 48	$73, 72$
70	E_0	E	$\langle C, w_1\rangle \to \mathfrak{Q}_8 : 2 \to \mathfrak{V}_4$	16	6	36 37 38 40 41 45 49	$70, 70$
71	$F^2 \times K$	$K_1^2 \times E$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	16	6	35 42 48 50 54	$75, 74$
72	E_0	E	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{V}_4$	16	6	40 43 47	$69, 73$
73	E_0	E	$C \to [2^2]4 \to \mathfrak{D}_4$	16	6	38 44 46	$72, 69$
74	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{D}_4$	16	6	34 43 47 51 52	$71, 75$
75	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{D}_4$	16	6	33 44 46 55 57	$74, 71$
76	E_0	E_0^2	$1 \to \mathfrak{S}_4 \to \mathfrak{S}_4$	24	4	32 52 58	$79, 81$
77	$F \times R(E)$	$\Delta(E) \times \lambda^2 E$	$\langle w_1, w_3\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{S}_3 \to \mathfrak{S}_3$	24	4	30 50 59	$84, 82$
78	$F \times E_0$	$\Delta(E) \times \lambda^2 E$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{C}_3 \to \mathfrak{C}_3$	24	4	31 35 59	$83, 80$
79	$F \times R(E)$	$F^2 \times \lambda^2 E$	$\langle w_1, w_3\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{S}_3 \to \mathfrak{S}_3$	24	4	32 54 59	$76, 81$
80	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{A}_4 \to \mathfrak{A}_4$	24	4	31 34 58	$78, 83$
81	E_0	E_0^2	$1 \to \mathfrak{S}_4 \to \mathfrak{S}_4$	24	4	32 57 60	$76, 79$
82	E_0	$E_0 \otimes \Delta(E_0)$	$1 \to \mathfrak{S}_4 \to \mathfrak{S}_4$	24	4	30 51 58	$77, 84$
83	E_0	E	$C \to \mathfrak{S}_2 \times \mathfrak{A}_4 \to \mathfrak{A}_4$	24	4	31 33 60	$78, 80$
84	E_0	$E_0 \otimes \Delta(E_0)$	$1 \to \mathfrak{S}_4 \to \mathfrak{S}_4$	24	4	30 55 66	$82, 77$
85	E_0	E	$\mathfrak{S}_2 \to \tilde{\mathfrak{A}}_4 \to \mathfrak{A}_4$	24	4	31 36	$85, 85$
86	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{V}_4 \to \mathfrak{V}_4$	32	1	64 67 68 70	$86, 86$
87	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{D}_4 \to \mathfrak{D}_4$	32	3	63 65 67 72 74	$92, 90$
88	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{C}_4 \to \mathfrak{C}_4$	32	3	63 64 66	$91, 89$
89	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2^3 \rtimes \mathfrak{C}_4 \to \mathfrak{D}_4$	32	3	62 66 67	$88, 91$
90	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{D}_4 \to \mathfrak{D}_4$	32	3	65 66 68 73 75	$92, 87$
91	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2^3 \rtimes \mathfrak{C}_4 \to \mathfrak{D}_4$	32	3	62 63 68	$89, 88$
92	$K_1 \times K_2$	$E_1 \times E_2$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^2 \rtimes \mathfrak{D}_4 \to \mathfrak{S}_2^2$	32	3	62 64 65 69 71	$87, 90$
93	$F \times R(E)$	$\Delta(E) \times K * \lambda^2 E$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2 \times \mathfrak{S}_4 \to \mathfrak{S}_3$	48	4	61 71 77 78 79	$94, 95$
94	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{S}_4 \to \mathfrak{S}_4$	48	4	61 75 81 83 84	$95, 93$
95	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{S}_4 \to \mathfrak{S}_4$	48	4	61 74 76 80 82	$93, 94$
96	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{D}_4 \to \mathfrak{D}_4$	64	3	86 87 88 89 90 91 92	$96, 96$
97	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{A}_4 \to \mathfrak{A}_4$	96	1	78 80 83 85 86	$97, 97$
98	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4 \to \mathfrak{S}_4$	192	1	93 94 95 96 97	$98, 98$

7 Trialitarian Resolvents

Trialitarian triples of étale algebras can be viewed as one étale algebra with two attached resolvents (see Remark 3.6). For example, let E be a quartic separable field with Galois group $\mathfrak{S}_4$. The field $E \otimes \Delta(E)$ is octic with the same Galois group $\mathfrak{S}_4$ and the extension $E \otimes \Delta(E)/E$ corresponds to Class $N = 82$ in Table 1. Class $N = 77$ in the same trialitarian triple corresponds to the extension

$$\big(\Delta(E) \times \lambda^2 E\big)/\big(F \times R(E)\big),$$

where $\Delta(E)$ is the discriminant, $R(E)$ is the cubic resolvent of E and $\lambda^2 E$ is the second lambda power of E, as defined in [13].

In this section we consider the situation where one étale algebra in the triple is given by a separable polynomial and compute polynomials for the two other étale algebras. We assume that the base field F is infinite and has characteristic different from 2.

Proposition 7.1. *Let S/S_0 be an étale algebra with involution of dimension $2n$ over F.*

1) There exists an invertible element $x \in S$ such that x generates S and x^2 generates S_0.
2) There exists a polynomial

$$f_n(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

with coefficients in F such that $S_0 \xrightarrow{\sim} F[x]/\big(f_n(x)\big)$ and $S \xrightarrow{\sim} F[x]/\big(f_{2n}(x)\big)$, where $f_{2n}(x) = f_n(x^2)$.
3) The algebra S has trivial discriminant if and only if $(-1)^n a_0$ is a square in F.

Proof. To prove (1) we are looking for invertible elements x of S such that $\mathrm{Tr}_{S/S_0}(x) = 0$ and such that the discriminant of the characteristic polynomial of x^2 is not zero. Any such element generates S and $x^2 \in S_0$ generates S_0. These elements form a Zariski open subset of the space of trace zero elements. One checks that this open subspace is not empty by going to an algebraic closure of F.
(2) follows from (1) and (3) follows from a discriminant formula (see [4, p. 51]) for the discriminant $D(f_{2n})$ of f_{2n}:

$$D(f_{2n}) = (-1)^n a_0 \cdot \big(2^n D(f_n)\big)^2$$

(recall that $\Delta(S) \xrightarrow{\sim} F[x]/\big(x^2 - D(f_{2n})\big)$). □

Theorem 7.2. *Let S/S_0,* $\dim_F S = 8$*, with trivial discriminant, be given as in Proposition 7.1 by a polynomial*

$$f_4(x) = x^4 + ax^3 + bx^2 + cx + e^2. \tag{7.3}$$

The polynomials

$$\begin{aligned} f_4'(x) &= x^4+ax^3+(\tfrac{3}{8}a^2-\tfrac{1}{2}b+3e)x^2+ \\ &\quad (\tfrac{1}{16}a^3-\tfrac{1}{4}ab+c+\tfrac{1}{2}ae)x+\big(\tfrac{1}{16}a^2-\tfrac{1}{4}b-\tfrac{1}{2}e\big)^2 \quad \textit{and} \\ f_4''(x) &= x^4+ax^3+(\tfrac{3}{8}a^2-\tfrac{1}{2}b-3e)x^2+ \\ &\quad (\tfrac{1}{16}a^3-\tfrac{1}{4}ab+c-\tfrac{1}{2}ae)x+\big(\tfrac{1}{16}a^2-\tfrac{1}{4}b+\tfrac{1}{2}e\big)^2 \end{aligned}$$

define extensions of étale algebras S'/S_0', S''/S_0'' such that the isomorphism classes of S/S_0, S'/S_0', and S''/S_0'' are in triality.

Proof. Let $\{y_1,y_2,y_3,y_4\}$ be the set of zeroes of f_4 in a separable closure F_s of F. The set $\{\pm x_i = \pm\sqrt{y_i},\ i=1,\dots 4\}$ is the set of zeroes of f_8. Let ξ be the column vector $[x_1,x_2,x_3,x_4]^T$. If $\varphi:\Gamma\to W(D_4)\subset \mathrm{O}_4$ is the cocycle corresponding to S/S_0, the group $\varphi(\Gamma)$ permutes the elements $\pm x_i$ through left matrix multiplication on ξ. The cocycle corresponding to S'/S_0' is given by:

$$\varphi' : \gamma \mapsto \mu\varphi(\gamma)\mu^{-1}, \gamma\in\Gamma,$$

where μ is as in (4.7). Thus, $\varphi'(\Gamma)$ permutes the components of $\pm\xi' = \pm\mu\xi = \pm[x_1',x_2',x_3',x_4']^T$ and $\{\pm x_i', i=1,\dots,4\}$ is the set of zeroes of f_8'. It follows that

$$f_8'(x) = f_4'(x^2) = \prod_i (x-x_i')(x+x_i') = \prod_i (x^2-x_i'^2).$$

The x_i' are the components of $\xi'=\mu\xi$. Thus, the coefficients of $f_8'(x)$ can be expressed as functions of the x_i. Using that the symmetric functions in the x_i can be expressed as functions of the coefficients of f_8 one gets (for example with Magma [2]) the expression given in Proposition 7.2 for f_i'. Similar computations with μ^2 instead of μ lead to the formula for f_4''. □

Remark 7.4. Observe that we move from f_8' to f_8'' by replacing e by $-e$, as it should be.

8 Triality and Witt Invariants of étale Algebras

The results of this section were communicated to us by Serre [16]. They are based on results of [15] and [10]. Similar results can be obtained for cohomological invariants of étale algebras instead of Witt invariants. Let k be a fixed base field of characteristic not 2 and F/k be a field extension. Let $WGr(F)$ be the Witt-Grothendieck ring and $W(F)$ the Witt ring of F, viewed as functors of F. We recall that elements of $WGr(F)$ are formal differences $q-q'$ of isomorphism classes of nonsingular quadratic forms over F and that the sum and product are those induced by the orthogonal sum and the tensor product of quadratic forms. The Witt ring $W(F)$ is the quotient of $WGr(F)$ by the ideal consisting of integral multiples of the 2-dimensional diagonal form $\langle 1,-1\rangle$.

Some of the following considerations hold for oriented quadratic extensions S/S_0 of étale algebras of arbitrary dimension. To simplify notation we assume from now on that $\dim_F S = 8$.

Let $(\acute{E}tex^{2/4})^+$ be the functor which associates to F the set $(\acute{E}tex_F^{2/4})^+$ of isomorphism classes of oriented quadratic extensions S/S_0 of étale algebras over F such that $\dim_F S = 8$. A *Witt invariant* on $(\acute{E}tex^{2/4})^+$, more precisely on $W(D_4)$, is a map

$$H^1\big(F, W(D_4)\big) \to W(F)$$

for each F/k, subject to compatibility and specialization conditions (see [10]). The set of Witt invariants

$$\mathrm{Inv}\big(W(D_4), W\big) = \mathrm{Inv}\big((\acute{E}tex^{2/4})^+, W\big)$$

is a module over $W(k)$. The aim of this section is to describe this module and how triality acts on it. A main tool is the following splitting principle, which is a special case of a variant of the splitting principle for étale algebras (see [10, Theorem 24.9]) and which can be proved following the same lines.

Theorem 8.1. *If $a \in \mathrm{Inv}\,\big((\acute{E}tex^{2/4})^+, W\big)$ satisfies $a(S/S_0) = 0$ for every product of two biquadratic algebras*

$$S = F\big(\sqrt{x}, \sqrt{y}\big) \times F\big(\sqrt{z}, \sqrt{t}\big), \quad S_0 = F\big(\sqrt{xy}\big) \times F\big(\sqrt{zt}\big).$$

over every extension F of k, then $a = 0$.

Let G be an elementary abelian subgroup of $W(D_4)$ of type $(2,2,2,2)$. It belongs to the conjugacy class $N = 65$ in Table 1. Theorem 8.1 can be restated in the following form:

Theorem 8.2. *The restriction map*

$$\mathrm{Res}\colon\ \mathrm{Inv}\big(W(D_4), W\big) \to \mathrm{Inv}\big(G, W\big)$$

is injective.

Proof. G-torsors correspond to products of two biquadratic algebras. □

A construction of Witt invariants is through trace forms. Let $S/S_0 \in (\acute{E}tex^{2/4})^+$ and let σ be the involution of S. We may associate two nonsingular quadratic trace forms to the extension S/S_0:

$$\begin{aligned} Q(x) &= Q_S(x) = \tfrac{1}{8}\,\mathrm{Tr}_{S/F}(x^2) \\ Q'(x) &= Q'_S(x) = \tfrac{1}{8}\,\mathrm{Tr}_{S/F}\big(x\sigma(x)\big),\ x \in S. \end{aligned}$$

The decomposition

$$S = \mathrm{Sym}(S,\sigma) \oplus \mathrm{Skew}(S,\sigma)$$

leads to orthogonal decompositions

$$Q = Q^+ \perp Q^-, \quad Q' = Q^+ \perp -Q^-,$$

hence the forms Q^+ and Q^- define two Witt invariants attached to S/S_0. The étale algebras associated to S/S_0 by triality lead to corresponding invariants. We introduce the following notation: $S/S_0 = S_1/S_{0,1}$ and $S_i/S_{0,i}$, $i = 2,3$, for the associated étale algebras. We denote the corresponding Witt invariants by $Q_i^+ = Q_{S_i}^+$ and $Q_i^- = Q_{S_i}^-$, $i = 1$, 2, and 3.

Another construction of Witt invariants is through orthogonal representations. Let O_n be the orthogonal group of the n-dimensional form $\langle 1,\dots,1\rangle$. Quadratic forms over F of dimension n are classified by the cohomology set $H^1(F,\mathrm{O}_n)$. Thus any group homomorphism $W(D_4) \to \mathrm{O}_n$ gives rise to a Witt invariant. In particular we get a Witt invariant q associated with the orthogonal representation $W(D_4) \to \mathrm{O}_4$ described in (5.3). Moreover the group $W(D_4)$ has three normal subgroups H_i of type $(2,2,2)$ (i.e., isomorphic to $\mathfrak{S}_2^3$), corresponding to the classes $N = 33, 34, 35$ of Table 1. As the factor groups are isomorphic to $\mathfrak{S}_4$, the canonical representation $\mathfrak{S}_4 \to \mathrm{O}_4$ through permutation matrices leads to three Witt invariants q_1, q_2, q_3.

Proposition 8.3. *1) The Witt invariant q is invariant under triality and coincides with Q_i^-, $i = 1,2,3$.*
2) We have $q_i = Q_i^+$, $i = 1$, 2, 3, and the three invariants q_1, q_2, q_3 are permuted by triality.

Proof. The fact that q is invariant under triality follows from the fact that triality acts on $W(D_4)$ by an inner automorphism of O_4. Moreover the trialitarian action on $W(D_4)$ permutes the normal subgroups H_i, hence the invariants q_i. For the other claims we may assume by the splitting principle that S_1 is a product of two biquadratic algebras

$$S_1 = F\big(\sqrt{x},\sqrt{y}\big) \times F\big(\sqrt{z},\sqrt{t}\big), \quad S_{0,1} = F\big(\sqrt{xy}\big) \times F\big(\sqrt{zt}\big). \tag{8.4}$$

An explicit computation, using for example the description of triality given in the proof of Theorem 4.1 (see [1] and [20]) shows that one can make the following identifications

$$S_2 = F\big(\sqrt{x},\sqrt{z}\big) \times F\big(\sqrt{y},\sqrt{t}\big), \quad S_{0,2} = F\big(\sqrt{xz}\big) \times F\big(\sqrt{yt}\big)$$

and

$$S_3 = F\big(\sqrt{x},\sqrt{t}\big) \times F\big(\sqrt{y},\sqrt{z}\big), \quad S_{0,3} = F\big(\sqrt{xt}\big) \times F\big(\sqrt{yz}\big).$$

Observe that, with this identification, the three-cycle (y,z,t) permutes cyclically the algebras $S_i/S_{0,i}$. We get

$$Q_i^- = \langle x,y,z,t\rangle$$

for $i = 1$, 2, 3, and

$$Q_1^+ = \langle 1,1,xy,zt\rangle, \quad Q_2^+ = \langle 1,1,xz,yt\rangle, \quad Q_3^+ = \langle 1,1,xt,yz\rangle.$$

The equalities $q = Q_i^-$ and $q_i = Q_i^+$ follow from the fact that the corresponding cocycles are conjugate in O_4. $\square$

Further basic invariants are the constant invariant $\langle 1\rangle$ and the discriminant

$$\langle d\rangle = \mathrm{Disc}(q) = \mathrm{Disc}(q_i),\ i = 1, 2, 3,$$

which corresponds to the 1-dimensional representation $\det\colon W(D_4) \to \mathrm{O}_1 = \pm 1$. Since $Q_i^+(1) = 1$, the quadratic forms $q_i = Q_i^+$ represent 1 and one can replace them by 3-dimensional invariants $\ell_i = (1)^\perp \subset q_i$, $i = 1,2,3$.

In the following result $\lambda^2 q$ denotes the second exterior power of the quadratic form q (see [10]). If $q = \langle \alpha_1, \dots, \alpha_n\rangle$ is diagonal, then $\lambda^2 q$ is the $n(n-1)/2$-dimensional form $\lambda^2 q = \langle \alpha_1\alpha_2, \dots, \alpha_{n-1}\alpha_n\rangle$.

Theorem 8.5. *1) The $W(k)$-module $\mathrm{Inv}\big(W(D_4), W\big) = \mathrm{Inv}\big((\acute{E}tex^{2/4})^+, W\big)$ is free over $W(k)$ with basis*

$$\big(\langle 1\rangle, \langle d\rangle, q, \langle d\rangle \cdot q, \ell_1, \ell_2, \ell_3\big). \tag{8.6}$$

2) The elements $\langle 1\rangle, \langle d\rangle, q, \langle d\rangle\cdot q$ are fixed under triality and the elements ℓ_1, ℓ_2, and ℓ_3 are permuted.

3) The following nonlinear relations hold among elements of (8.6)*:*

$$\begin{aligned} \langle d\rangle &= \mathrm{Disc}(q) = \mathrm{Disc}(q_i), \\ \lambda^2 q &= \ell_1 + \ell_2 + \ell_3 - \langle 1,1,1\rangle \\ \langle 1, d\rangle \cdot q &= q\cdot(\ell_i - \langle 1\rangle),\ i = 1, 2, 3. \end{aligned}$$

Proof. 1) The proof follows the pattern of the proof of [10, Theorem 29.2]. Let G be an elementary subgroup of $W(D_4)$ of type $(2,2,2,2)$, i.e., isomorphic to $\mathfrak{S}_2^4$. An arbitrary element of $H^1(F, G)$ is given by a four-tuple $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \big(F^\times/F^{\times 2}\big)^4$. For I a subset of $\mathbf{4} = \{1,2,3,4\}$, we write α_I for the product of the α_i for $i \in I$. By [10, Theorem 27.15] the set $\mathrm{Inv}(G,W)$ is a free $W(k)$-module with basis $(\alpha_I)_{I\subset\mathbf{4}}$. It then follows from Theorem 8.2 that the family of elements given in (8.6) is linearly independent over $W(k)$. Let a be an element of $\mathrm{Inv}\big((\acute{E}tex^{2/4})^+, W\big)$ and let S_α be the algebra (8.4) for $\alpha_1 = x$, $\alpha_2 = y$, $\alpha_3 = z$, $\alpha_4 = t$. The map $\alpha \mapsto a(S_\alpha)$ is a Witt invariant of G, hence by [10, Theorem 27.15] can be uniquely written as a linear combination

$$\sum c_I \cdot \langle \alpha_I\rangle \text{ with } c_I \in W(k). \tag{8.7}$$

The claim will follow if we show that the invariant α is in fact a linear combination of the elements given in (8.6). By [10, Prop. 13.2], the image of the restriction map $\mathrm{Inv}\big(W(D_4), W\big) \to \mathrm{Inv}(G,W)$ is contained in the $W(k)$-submodule of $\mathrm{Inv}(G,W)$ fixed by the normalizer $H = \mathfrak{S}_2^3 \rtimes \mathfrak{D}_4$ of G in $W(D_4)$ (conjugacy class $N = 96$ in Table 1). The group H acts on the set of isomorphisms classes of algebras S_i by acting in the obvious way on the symbols $\pm\sqrt{x}$, $\pm\sqrt{y}$, $\pm\sqrt{z}$, $\pm\sqrt{t}$. It follows that H acts trivially on this set of isomorphisms classes. This shows that only linear combinations of elements in the family

$$\mathscr{B} = \{\langle 1\rangle, \langle x\rangle + \langle y\rangle + \langle z\rangle + \langle t\rangle, \langle xy\rangle + \langle zt\rangle, \langle xz\rangle + \langle yt\rangle, \langle xt\rangle + \langle yz\rangle, \\ \langle xyz\rangle + \langle xyt\rangle + \langle xzt\rangle + \langle yzt\rangle, \langle xyzt\rangle\}$$

can occur in the sum (8.7). The family $\mathscr{B}$ and the family given in (8.6) are equivalent bases. This implies the first claim of Theorem 8.5. Claim 2) follows from Proposition 8.3 and 3) is easy to check for a product of biquadratic extensions. □

Acknowledgements We are grateful to Parimala for her unshakable interest in triality, in particular for many discussions at earlier stages of this work and we specially thank Serre for communicating to us his results on Witt and cohomological invariants of the group $W(D_4)$. We also thank Emmanuel Kowalski who introduced us to Magma [2] with much patience, Jean Barge for his help with Galois cohomology and Humphreys and Mühlherr for the reference to the paper [9]. The paper [11] on octic fields was a very useful source of inspiration. Finally, we are highly thankful to the referee for many improvements.

References

1. L. Beltrametti Über quadratische Erweiterungen étaler Algebren der Dimension vier. Diplomarbeit, Mathematikdepartement, ETH Zürich (2006). http://www.math.ethz.ch/~knus
2. W. Bosma, J. Cannon, C. Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput. **24** (3–4), 235–265 (1997)
3. N. Bourbaki. Éléments de mathématique. Groupes and algèbres de Lie. Chapitres 4, 5 et 6. (Masson, Paris, 1981)
4. J. Brillhart. On the Euler and Bernoulli polynomials. J. Reine Angew. Math. **234**, 45–64 (1969)
5. E. Cartan. Le principe de dualité et la théorie des groupes simples et semi-simples. Bull. Sci. Math. **49**, 361–374 (1925)
6. J. H. Conway, A. Hulpke, J. McKay. On transitive permutation groups. LMS J. Comput. Math. **1** (1998), 1–8
7. P. Deligne. Séminaire de géométrie algébrique du Bois-Marie, SGA 4 1/2, Cohomologie étale, avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie and J. L. Verdier, Lecture Notes in Mathematics vol. 569. (Springer-Verlag, Berlin, 1977)
8. W. N. Franzsen. Automorphisms of Coxeter Groups. PhD thesis, School of Mathematics and Statistics, University of Sydney (2001). http://www.maths.usyd.edu.au/u/PG/theses.html
9. W. N. Franzsen, R. B. Howlett. Automorphisms of nearly finite Coxeter groups. Adv. Geom. **3** (3), 301–338 (2003)
10. S. Garibaldi, A. A. Merkurjev, J-P. Serre. Cohomological invariants in Galois cohomology. University Lecture Series vol. 28. (American Mathematical Society, Providence, RI, 2003)
11. J. W. Jones, D. P. Roberts. Octic 2-adic fields. J. Number Theory, **128** 1410–1429 (2008)
12. M.-A. Knus, A. A. Merkurjev, M. Rost, J.-P. Tignol. The Book of Involutions. American Mathematical Society Colloquium Publications vol. 44. (American Mathematical Society, Providence, R.I., 1998)
13. M.-A. Knus, J.-P. Tignol. Quartic exercises. Inter. J. Math. Math. Sci. **2003** (68), 4263–4323 (2003)
14. ———. Thin Severi-Brauer varieties. preprint, 2009, arxiv:0912.3359
15. J.-P. Serre. Witt invariants and trace forms. Minicourse, Workshop "From quadratic forms to algebraic groups", Ascona, organized by Paul Balmer, Eva Bayer and Max-Albert Knus, February 18–23 (2007)
16. ———. Les invariants de $W(D_4)$. Emails, June 5, June 6, June 18, 2009

17. J. Tits. Sur les analogues algébriques des groupes semi-simples complexes. In Colloque d'algèbre supérieure, tenu à Bruxelles du 19 au 22 décembre 1956, 261–289. (Centre Belge de Recherches Mathématiques, Établissements Ceuterick, Louvain; Librairie Gauthier-Villars, Paris, 1957)
18. ———. Sur la trialité et certains groupes qui s'en déduisent. Publ. Math. IHES **2**, 14–60 (1959)
19. ———. Buildings of Spherical Type and Finite BN-Pairs. Lecture Notes in Mathematics vol. 386. (Springer-Verlag, Berlin, 1974)
20. S. Zweifel. Etale Algebren und Trialität. Diplomarbeit, Mathematikdepartement, ETH Zürich. (2006). http://www.math.ethz.ch/~knus

Remarks on Unimodular Rows

N. Mohan Kumar and M. Pavaman Murthy

To Parimala Raman

Summary If (a,b,c) is a unimodular row over a commutative ring A and if the polynomial $z^2+bz+ac$ has a root in A, we show that the unimodular row is completable. In particular, if $1/2 \in A$ and b^2-4ac has a square root in A, then (a,b,c) is completable.

1 Introduction

Let A be a commutative ring with identity. A row vector $\underline{a} = (a_1,a_2,\ldots,a_n)$ with $a_i \in A$ is called a *unimodular row* if there exists $b_i \in A$ such that $\sum a_i b_i = 1$. Thus given a unimodular row $\underline{a}$, we get an exact sequence $0 \to A \xrightarrow{\underline{a}} A^n \to P \to 0$, where P is a projective module over A of rank $n-1$ and $P \oplus A \cong A^n$. We call P the projective module associated with the unimodular row $\underline{a}$. So P is stably free. In general, it is important and interesting to find conditions on such a unimodular row so that the associated projective module is free. It is immediate that this is equivalent to the condition that there exists a nonsingular matrix σ of size n with entries in A such that

$$(a_1,a_2,\ldots,a_n)\sigma = (1,0,\ldots,0).$$

Such a unimodular row is called *completable*.

N. Mohan Kumar
Department of Mathematics, Washington University in St. Louis, St. Louis, MO 63130, USA,
e-mail: kumar@wustl.edu

M. Pavaman Murthy
Department of Mathematics, University of Chicago, 5734 University Avenue, Chicago, IL 60637
e-mail: murthy@math.uchicago.edu

2010 Mathematics subject classification. 13C10.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_17,

The first nontrivial condition of this kind was obtained by Swan and Towber [4] and was later generalized by Suslin [3].

Theorem 1 (Suslin). *Let $(a_1, a_2, \ldots, a_n)$ be a unimodular row over a ring A. Assume that $a_i = b_i^{r_i}$ where the r_i's are non-negative integers and $b_i \in A$. If $(n-1)!$ divides $\prod r_i$, then $(a_1, a_2, \ldots, a_n)$ is completable.*

In an attempt to generalize the above theorem, Nori conjectured the following.

Conjecture 2 (Nori). *Let $\varphi : R = k[x_1, x_2, \ldots, x_n] \to A$ be a homomorphism of k-algebras, where k is a field and the x_i's are indeterminates. Assume that the row $(\varphi(x_1), \ldots, \varphi(x_n))$ is unimodular. Let $f_i \in R$ with $1 \le i \le n$ be such that the radical of the ideal generated by the f_i's is $(x_1, \ldots, x_n)$ and the length of $R/(f_1, \ldots, f_n)$ is a multiple of $(n-1)!$. Then the unimodular row $(a_1, a_2, \ldots, a_n)$ where $a_i = \varphi(f_i)$ is completable.*

This conjecture is still open, but the first author proved a partial result in this direction [2].

Theorem 3 (Mohan Kumar). *Assume in the above that k is algebraically closed and the f_i's are homogeneous. Then the conjecture is true.*

In the present article we prove yet another sufficient condition for a unimodular row of length three to be completable, which does not seem to follow from the earlier results.

Theorem 4. *Let $(a,b,c) \in A^3$ be unimodular. Suppose that the polynomial $z^2 + bz + ac$ has a root in A. Then (a,b,c) is completable.*

As an immediate corollary we have

Corollary 5. *Suppose $1/2 \in A$ and $(a,b,c) \in A^3$ unimodular. If $b^2 - 4ac$ is a square in A, then (a,b,c) is completable.*

For larger length unimodular rows we have a somewhat weaker result which can be found in Sect. 3.

2 Proof of Theorem 4

We will give two proofs of Theorem 4. As always, A will be a commutative ring with identity. In all the results, because only finitely many elements of the ring are involved we may assume that A is finitely generated over the prime ring. Thus, we may assume that A is Noetherian.

Lemma 6 (Swan). *Let L be an r-generated line bundle over A. Then for any integer $n \ge 0$, L^n is r-generated. In particular, if $r = 2$, $L^n \oplus L^{-n}$ is free.*

Proof. Let $l_1, l_2, \dots, l_r \in L$ generate L. Then it is immediate that $l_i^n \in L^n$ generate L^n, by a local checking. In particular, if $r = 2$, we have a surjection $A^2 \to L^n$ and by determinant considerations, the kernel of this map is L^{-n}. Thus $L^n \oplus L^{-n} \cong A^2$. $\square$

Let $\pi\colon \mathbb{P}^1_A \to \operatorname{Spec} A$ be the structure morphism and let $\mathscr{O}_{\mathbb{P}^1_A}(1)$ be the tautological line bundle. Then $\pi_* \mathscr{O}_{\mathbb{P}^1_A}(n) = \mathrm{H}^0(\mathbb{P}^1_A, \mathscr{O}_{\mathbb{P}^1_A}(n))$ is a free A-module of rank $n+1$ for all $n \geq 0$. Let x, y be the homogeneous coordinates of $\mathbb{P}^1_A$. Given unimodular $(a,b,c) \in A^3$, we may define a subscheme X of $\mathbb{P}^1_A$ by the vanishing of $s = ax^2 + bxy + cy^2$. Then we have an exact sequence

$$0 \to \mathscr{O}_{\mathbb{P}^1_A}(-2) \xrightarrow{s} \mathscr{O}_{\mathbb{P}^1_A} \to \mathscr{O}_X \to 0. \tag{1}$$

The unimodularity of (a,b,c) implies that the restriction map $\pi\colon X \to \operatorname{Spec} A$ is a projective morphism of degree two. In particular it is quasi-finite. Thus by Chap. III, 11.2 and Chap. II, Exercise 5.17(b) in Hartshorne's book [1], X is affine and so let us write $X = \operatorname{Spec} B$ where $B = \mathrm{H}^0(X, \mathscr{O}_X)$. Taking cohomology of the sequence (1), we get

$$0 \to \mathrm{H}^0(\mathscr{O}_{\mathbb{P}^1_A}) \to \mathrm{H}^0(\mathscr{O}_X) \to \mathrm{H}^1(\mathscr{O}_{\mathbb{P}^1_A}(-2)) \to 0.$$

As $\mathrm{H}^0(\mathscr{O}_{\mathbb{P}^1_A}) \cong A \cong \mathrm{H}^1(\mathscr{O}_{\mathbb{P}^1_A}(-2))$, we see that $B \cong A \oplus A$ as A-modules.

We first identify the ring B. It is generated by one element over A. Since the generator is identified as a generator of $\mathrm{H}^1(\mathbb{P}^1_A, \mathscr{O}_{\mathbb{P}^1_A}(-2))$, we use Čech complex to identify this element. Let U_x (respectively U_y) be the open set $x \neq 0$ (respectively $y \neq 0$) of $\mathbb{P}^1_A$. With respect to this open cover, the Čech complexes for the exact sequence (1) fit into a diagram as follows.

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] \\
\mathrm{H}^0(U_x, \mathscr{O}_{\mathbb{P}^1_A}(-2)) \oplus \mathrm{H}^0(U_y, \mathscr{O}_{\mathbb{P}^1_A}(-2)) \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"'] & \mathrm{H}^0(U_x \cap U_y, \mathscr{O}_{\mathbb{P}^1_A}(-2)) \arrow[d, "\psi_2"] \\
\mathrm{H}^0(U_x, \mathscr{O}_{\mathbb{P}^1_A}) \oplus \mathrm{H}^0(U_y, \mathscr{O}_{\mathbb{P}^1_A}) \arrow[r, "\varphi_2"] \arrow[d] & \mathrm{H}^0(U_x \cap U_y, \mathscr{O}_{\mathbb{P}^1_A}) \arrow[d] \\
\mathrm{H}^0(U_x, \mathscr{O}_X) \oplus \mathrm{H}^0(U_y, \mathscr{O}_X) \arrow[r, "\varphi_3"] & \mathrm{H}^0(U_x \cap U_y, \mathscr{O}_X)
\end{tikzcd}$$

We write these in terms of the corresponding rings. Denote by h the polynomial $at^2 + bt + c \in A[t]$, where $t = y/x$.

$$\begin{array}{ccc}
 & 0 & & 0 \\
 & \downarrow & & \downarrow \\
 & A[t] \oplus A[t^{-1}] & \xrightarrow{\varphi_1} & A[t,t^{-1}] \\
 & \psi_1 \downarrow & & \downarrow \psi_2 \\
 & A[t] \oplus A[t^{-1}] & \xrightarrow{\varphi_2} & A[t,t^{-1}] \\
 & \downarrow & & \downarrow \\
 & A[t]/(h) \oplus A[t^{-1}]/(ht^{-2}) & \xrightarrow{\varphi_3} & A[t,t^{-1}]/(h)
\end{array}$$

Next we explicitly describe the maps which appear earlier.

$$\varphi_1(\alpha,\beta) = \alpha - t^{-2}\beta, \quad \varphi_2(\alpha,\beta) = \alpha - \beta, \quad \varphi_3(\alpha,\beta) = \alpha - \beta,$$
$$\psi_1(\alpha,\beta) = (h\alpha, ht^{-2}\beta), \quad \text{and} \quad \psi_2(\alpha) = h\alpha.$$

The following are easy to check. The kernel of φ_1 is zero (since it equals $\mathrm{H}^0(\mathscr{O}_{\mathbb{P}^1_A}(-2)))$ and similarly, the kernel of φ_2 is A and the kernel of φ_3 is B. The cokernel of φ_1 is naturally identified with At^{-1} and the cokernels of φ_2 and φ_3 are both zero. The element $z = (at, -(b+ct^{-1})) \in A[t]/(h) \oplus A[t^{-1}]/(ht^{-2})$ goes to zero under φ_3 and hence defines an element in B. We claim that this element generates B as an A-algebra. To check this, it suffices to check that this element goes to $t^{-1} \in At^{-1} = \mathrm{H}^1(\mathscr{O}_{\mathbb{P}^1_A}(-2))$. We do this by a simple diagram chase. Clearly z can be lifted to $(at, -(b+ct^{-1})) \in A[t] \oplus A[t^{-1}]$. When we apply φ_2 to this we get $ht^{-1} \in A[t,t^{-1}]$, and thus it is the image of t^{-1} under ψ_2 proving the claim. Next we claim that z satisfies the equation $z^2 + bz + ac = 0$. It suffices to check that $at \in A[t]/(h)$ and $-(b+ct^{-1}) \in A[t^{-1}]/(ht^{-2})$ satisfy this equation:

$$(at)^2 + b(at) + ac = a(at^2 + bt + c) = ah = 0, \quad \text{and}$$
$$(-(b+ct^{-1}))^2 + b(-(b+ct^{-1})) + ac = bct^{-1} + c^2t^{-2} + ac = cht^{-2} = 0.$$

Thus we have identified B to be $A[z]/(z^2 + bz + ac)$.

Since X is affine, for any sheaf $\mathscr{F}$ on X, the natural map $\pi^*\pi_*\mathscr{F} \to \mathscr{F}$ is surjective. Twisting the exact sequence (1) by $\mathscr{O}_{\mathbb{P}^1_A}(2)$ and taking cohomology, we get

$$0 \longrightarrow A \xrightarrow{(a,b,c)} A^3 \longrightarrow P \longrightarrow 0, \tag{2}$$

where $P = \pi_*\mathscr{O}_X(2)$.

We have a surjection $\pi^*(P) \to \mathscr{O}_X(2)$ and thus we see that $\pi^*(P) = \mathscr{O}_X(2) \oplus \mathscr{O}_X(-2)$. But we have seen that $\pi_*\mathscr{O}_X(1) = \pi_*\mathscr{O}_{\mathbb{P}^1_A}(1) = A^2$ and thus $\mathscr{O}_X(1)$ is two generated. So, by Lemma 6, we see that π^*P is free. If $z^2 + bz + ac$ has a root in A, we have a retraction $B \to A$. Since $B \otimes_A P$ is free, we see that P must be free as well, proving Theorem 4. $\square$

Remark 7. Saying that the polynomial $z^2+bz+ac=0$ has a root in A is equivalent to saying that the map $\pi\colon X\to \operatorname{Spec} A$ has a section.

Remark 8 (Nori). Let $(a,b,c)\in A^3$ be unimodular and let P be the associated projective module. *Then for any $n\geq 2$, there exists an A-algebra B, which is A-free of rank n and such that $B\otimes_A P$ is B-free.*

We now justify this claim. Let $s=ax^n+bx^{n-1}y+cy^n$, where as before, x and y are the homogeneous coordinates of $\mathbb{P}^1_A$. The zeros of s define a subscheme X of $\mathbb{P}^1_A$. We have an exact sequence

$$0\to \mathscr{O}_{\mathbb{P}^1_A}(-n)\xrightarrow{s}\mathscr{O}_{\mathbb{P}^1_A}\to \mathscr{O}_X\to 0.$$

Then as before, $\mathrm{H}^0(X,\mathscr{O}_X)=B$ is a free A-module of rank n, since $\mathrm{H}^1(\mathbb{P}^1_A,\mathscr{O}_{\mathbb{P}^1_A}(-n))$ is a free A-module of rank $n-1$ and the map $X\to \operatorname{Spec} A$ is a finite map of degree n since (a,b,c) is unimodular. We have as before a surjection $B^2\to \mathscr{O}_X(n)$ given by sending the basis elements to x^n, y^n. Thus, we get a surjection $B^3\to \mathscr{O}_X(n)$ by sending the basis elements to x^n, $x^{n-1}y$, y^n. As $ax^n+bx^{n-1}y+cy^n=0$ on X, we see that this surjection factors through $B^3/B(a,b,c)=Q$. Thus, the B-projective module Q is isomorphic to $\mathscr{O}_X(n)\oplus\mathscr{O}_X(-n)$ and since $\mathscr{O}_X(n)$ is two generated, we see that Q is free by Lemma 6. But,

$$Q=B^3/B(a,b,c)=A^3/A(a,b,c)\otimes_A B=P\otimes_A B,$$

as desired. □

Next we give another proof of Theorem 4. Consider the ring

$$B=\mathbb{Z}[a,b,c,a',b',c',z]/(aa'+bb'+cc'-1,z^2+bz+ac),$$

where a,b,c,a',b',c',z are indeterminates. Then the ideal $I=(z,a)$ is locally free. This is easily seen as follows. Let $\mathfrak{M}$ be any maximal ideal of B. If either $z\notin\mathfrak{M}$ or $a\notin\mathfrak{M}$, clearly I is locally free at $\mathfrak{M}$. Since $z(z+b)+ac=0$, again, if $z+b\notin\mathfrak{M}$ or $c\notin\mathfrak{M}$, I is locally free. Thus we may assume that $\mathfrak{M}$ contains z, $z+b$, a, c which implies $a,b,c\in\mathfrak{M}$ and there are no such maximal ideals, since (a,b,c) is unimodular. Then as in Lemma 6, we see that $I^2=(z^2,az,a^2)$ is in fact generated by (z^2,a^2). We have a surjective map $\varphi\colon B^3\to I^2$ given by:

$$\varphi(e_1)=z^2,\quad \varphi(e_2)=az,\quad \text{and}\quad \varphi(e_3)=a^2$$

where the e_i's form a basis for B^3. But

$$\varphi(ae_1+be_2+ce_3)=az^2+abz+a^2c=a(z^2+bz+ac)=0.$$

Thus φ factors through $P=B^3/(ae_1+be_2+ce_3)$. So, we see that $P\cong I^2\oplus I^{-2}$ and since I^2 is two generated, P is free by lemma 6. Now, if A is a ring with a unimodular row which also we call by abuse of notation a,b,c and such that the polynomial $z^2+bz+ac$ has a root in A, then writing $aa'+bb'+cc'=1$ for suitable $a',b',c'\in A$, we get a homomorphism $\psi\colon B\to A$ in the obvious fashion, sending z

to a root of the polynomial $z^2 + bz + ac$, which we have assumed exists in A. Then the associated projective module over A is just $P \otimes_B A$ and since we have seen that P is free, we are done.

3 Unimodular Rows of Length more than Three

In this section we consider unimodular rows $(a_1, a_2, \ldots, a_n)$ with n at least three. Notation will be as before. We will also assume that A satisfies the following condition on A which was not necessary for the $n = 3$ case.

Any two-generated line bundle on A is free. $\quad (*)$

For example, $(*)$ holds if A is a unique factorization domain.

As before, given $(a_1, a_2, \ldots, a_n) \in A^n$ a unimodular row, we consider the polynomial $s(x,y) = a_1 x^{n-1} + a_2 x^{n-2} y + \cdots + a_n y^{n-1}$ and define $X \subset \mathbb{P}^1_A$ to be the subscheme defined by the vanishing of s. Then, as before, the map $\pi : X \to \operatorname{Spec} A$ is a finite map of degree $n-1$ and in particular X is affine, since we may assume that A is Noetherian.

Theorem 9. *In the notation of the previous paragraph, if $\pi : X \to \operatorname{Spec} A$ has a section then the unimodular row is completable.*

Proof. Let $\varepsilon : \operatorname{Spec} A \to X$ be a section. Then we can consider it as a section $\varepsilon : \operatorname{Spec} A \to \mathbb{P}^1_A$ whose image is contained in X. But any such section is given by a surjection from $V = A^2 = \mathrm{H}^0(\mathbb{P}^1_A, \mathscr{O}_{\mathbb{P}^1_A}(1))$ to a line bundle (which is just $\varepsilon^*(\mathscr{O}_{\mathbb{P}^1_A}(1))$) on A. By our hypothesis, this line bundle is trivial. So, this is just choosing a basis for V. In other words, giving such a section is the same as a change of variables $(x,y) \mapsto (u,v)$ and then the section is contained in X implies that the equation s after a change of variables is divisible by say u. On the other hand, the change of variables – which is just an A-automorphism of V – induces an automorphism $S^{n-1}V \to S^{n-1}V$ and s maps to an s' divisible by u. Thus in the new variables, we get $s' = a'_1 u^n + \cdots + a'_{n-1} u v^{n-1}$ and since the quotient of $S^{n-1}V$ by s or s' gives the same projective module, we see that $(a_1, a_2, \ldots, a_n) \sim (a'_1, \ldots, a'_{n-1}, 0)$ and thus completable. $\square$

Remark 10. From the proof earlier, we see that with the condition $(*)$ on A, having a section of $\pi : X \to \operatorname{Spec} A$ implies that s has a linear factor. Conversely, if s has a linear factor, say $bx - ay$, then the coefficients of s are contained in the ideal (a,b) and thus (a,b) is unimodular, since the coefficients of s generate the unit ideal. Then it is clear that the map $\pi : X \to \operatorname{Spec} A$ has a section. Thus, Theorem 9 can be restated as follows: *The unimodular row $(a_1, a_2, \ldots, a_n)$ is completable if the associated polynomial s has a linear factor.*

Acknowledgements The first author was partially supported by a grant from the NSA.

References

1. R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, Berlin, 1977.
2. N. Mohan Kumar, *A note on unimodular rows*, J. Algebra **191** (1997), no. 1, 228–234.
3. A.A. Suslin, *Stably free modules*, Mat. Sbornik. **102** (1977), no. 4, 537–550.
4. R.G. Swan and J. Towber, *A class of projective modules which are nearly free*, J. Algebra **36** (1975), no. 3, 427–434.

Vector Bundles Generated by Sections and Morphisms to Grassmannians

F. Laytimi and D.S. Nagaraj

Summary In this short note we study vector bundles generated by sections and the associated morphism to the Grassmannian.

1 Introduction

In this paper we consider vector bundles generated by sections on a projective variety X over the field $\mathbb{C}$ of complex numbers. We study the properties of morphisms they induce from X to the Grassmannian variety $Gr(r,\mathbb{C}^n)$ of r-dimensional quotient spaces of $\mathbb{C}^n$. We give a criterion for a morphism to the Grassmannian to be finite (see Theorem 2.5). We also obtained the following result (see Theorem 3.7):

Theorem 1.1. *Let $n \geq 1$ and $m \geq n+2$ be two integers. If*

$$f : \mathbb{P}^m \to Gr(2,\mathbb{C}^{n+2})$$

is a morphism then f is a constant morphism.

The proof of this theorem is a consequence of a curious result in number theory (see Lemma 3.8).

After this paper was written, we learned that Tango [5] has proved much more general results about morphisms from projective spaces to Grassmannians.

F. Laytimi
Mathématiques - bât. M2, Université Lille 1, F-59655 Villeneuve d'Ascq Cedex, France,
e-mail: laytimi@math.univ-lille1.fr

D.S. Nagaraj
Institute of Mathematical Sciences C.I.T. campus, Taramani, Chennai 600113, India,
e-mail: dsn@imsc.res.in

2010 Mathematics subject classification. 14F05.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_18,

However, our paper contains some further new observations regarding morphisms to Grassmannians and our proof of the above theorem is straightforward.

2 Vector Bundles Generated by Sections

Definition 2.1. Let X be a variety over the field $\mathbb{C}$ and s be a positive integer. A vector bundle E on X is said to be *generated by s sections* if there is a surjection of vector bundles

$$\mathbb{C}^s \otimes \mathcal{O}_X \to E.$$

Note that in this definition we do not assume that the induced map $\mathbb{C}^s \to H^0(X,E)$ is injective.

Definition 2.2. Let E_1, E_2 be vector bundles of rank r on X. Two bundle surjections

$$\varphi_1 : \mathbb{C}^{r+k} \otimes \mathcal{O}_X \to E_1 \quad \text{and} \quad \varphi_2 : \mathbb{C}^{r+k} \otimes \mathcal{O}_X \to E_2$$

are said to be *equivalent* if there is an isomorphism of vector bundles $\psi : E_1 \to E_2$ such that the following diagram

$$\begin{array}{ccc} \mathbb{C}^{r+k} \otimes \mathcal{O}_X & \xrightarrow{\varphi_1} & E_1 \\ \| & & \downarrow \psi \\ \mathbb{C}^{r+k} \otimes \mathcal{O}_X & \xrightarrow{\varphi_2} & E_2 \end{array}$$

commutes.

We recall the following well-known result. For the sake of completeness we will sketch its proof.

Lemma 2.3. *Let X be a projective variety, r and k be two positive integers. Consider the following two sets:*

1) The set of morphisms $f : X \to Gr(r, \mathbb{C}^{r+k})$.
2) The set of equivalence classes of vector bundle surjections

$$\varphi : \mathbb{C}^{r+k} \otimes \mathcal{O}_X \to E,$$

where E is a vector bundle of rank r on X.

Pulling back by f the universal quotient

$$\varphi_0 : \mathbb{C}^{r+k} \otimes \mathcal{O}_{Gr(r,\mathbb{C}^{r+k})} \to Q,$$

on $Gr(r, \mathbb{C}^{r+k})$ gives a natural map from the set in (1) to the set in (2). This map is a bijection between the two sets.

Proof. The data of a surjection $\varphi : \mathbb{C}^{r+k} \otimes \mathscr{O}_X \to E$ defines a morphism

$$f : X \longrightarrow Gr(r, \mathbb{C}^{r+k}) \quad \text{by} \quad x \mapsto \{\mathbb{C}^{r+k} \to E_x\}.$$

This itself defines a map from the set in (2) to the set in (1). Moreover, it is easy to see that

$$f^*(\varphi_0) : f^*(\mathbb{C}^{r+k} \otimes \mathscr{O}_{Gr(r,\mathbb{C}^{r+k})}) \to f^*(Q)$$

is equivalent to $\varphi : \mathbb{C}^{r+k} \otimes \mathscr{O}_X \to E$.

These two maps are clearly inverse to each other, hence the natural map from set in (1) to set in (2) is a bijection. □

Remark 2.4. Lemma 2.3, in the case $r = 1$, gives a correspondence between finite morphisms

$$f : X \longrightarrow Gr(1, \mathbb{C}^{1+k}) \simeq \mathbb{P}^k$$

and ample line bundles generated by $k+1$ sections.

This leads to the following:

Question. For $r \geq 2$, what is the characterisation of the vector bundle in Lemma 2.3 that corresponds to a finite morphism?

The answer is the following

Theorem 2.5. *Let X be a projective variety. The bijective map of Lemma 2.3 induces a natural bijection between the following two sets:*

1) The set of morphisms $f : X \longrightarrow Gr(r, \mathbb{C}^{r+k})$ with f finite (onto its image).
2) The set of equivalence classes of vector bundle surjections

$$\mathbb{C}^{r+k} \otimes \mathscr{O}_X \longrightarrow E$$

with $\det(E)$ *ample, where E is a vector bundle of rank r and* $\det(E)$ *is the determinant line bundle of E.*

Proof. Given an element of the set in (2), i.e., a surjection, $\mathbb{C}^{r+k} \otimes \mathscr{O}_X \longrightarrow E$ with $\mathrm{rk}(E) = r$ and $\det(E)$ ample, then as in Lemma 2.3 it determines a morphism $f : X \longrightarrow Gr(r, \mathbb{C}^{r+k})$ and $f^*(Q) \simeq E$, where Q is the universal quotient bundle of rank r on $Gr(r, \mathbb{C}^{r+k})$. Hence $f^*(\det(Q)) \simeq \det(E)$. Since $\det(E)|_{f^{-1}(f(x))} \simeq f^*(\det(Q))|_{f^{-1}(f(x))}$ is trivial, the ampleness assumption on $\det(E)$ implies that $\dim(f^{-1}(f(x))) \leq 0$. Thus, if $\det(E)$ is ample, then f is finite onto its image.

In the other direction, if $f : X \longrightarrow Gr(r, \mathbb{C}^{r+k})$ is a finite morphism onto its image, then

$$\det(f^*(Q)) \simeq f^*(\det(Q))$$

is ample, since the pull-back of an ample bundle under a finite morphism is ample. □

Corollary 2.6. *Let X be a projective variety of dimension $n > r.k$, where r and k are positive integers. Then there is no vector bundle E on X of rank r generated by $r+k$ sections and with* $\det(E)$ *ample.*

Proof. The assumption on the dimension of X implies that any morphism $f : X \longrightarrow Gr(r, \mathbb{C}^{r+k})$ has positive-dimensional fibers. Hence $f^*(\det(Q))$ cannot be ample. □

Remark 2.7. Let $\mathscr{L}$ be an ample line bundle on a projective variety X of dimension n. Then it is easy to see that if

$$\mathbb{C}^{1+k} \otimes \mathscr{O}_X \to \mathscr{L}$$

is a surjection then we must have $k \geq n$.

Corollary 2.6 and Remark 2.7 lead to the following:

Question. Let d, r, and k be integers such that $r \geq 2$, $k \geq 2$, and $1 \leq d \leq r.k$. Let X be a projective variety of dimension d. Do there exist a rank r vector bundle E with $\det(E)$ ample and a surjection

$$\mathbb{C}^{r+k} \otimes \mathscr{O}_X \longrightarrow E\ ?$$

Or, equivalently, does there exist a finite morphism (onto its image)

$$f : X \longrightarrow Gr(r, \mathbb{C}^{r+k})\ ?$$

The answer to this question is in general negative. To see this, we recall the following:

Theorem 2.8. (Lazarsfeld [3, p. 55, Theorem 4.1]) *Let X be a smooth projective variety of positive dimension and let $f : \mathbb{P}^n \longrightarrow X$ be a surjective map. Then $X \simeq \mathbb{P}^n$.*

Corollary 2.9. *There is no rank two vector bundle E on $\mathbb{P}^4$ with* $\det(E)$ *ample and generated by four sections.*

Proof. As $\dim(\mathrm{Gr}(2, \mathbb{C}^4)) = 4$, any finite morphism $f : \mathbb{P}^4 \longrightarrow Gr(2, \mathbb{C}^4)$ has to be surjective. Hence, by Theorem 2.8, we see that there is no such map. This proves the required result in view of Theorem 2.5. □

Remark 2.10. If $\dim X \leq 2$, then it is easy to see that there is always a finite (onto its image) morphism $f : X \longrightarrow Gr(2, \mathbb{C}^4)$. Hence, if $\dim(\mathrm{X}) \leq 2$ there always exists a rank 2 vector bundle E on X and a surjection

$$\mathbb{C}^4 \otimes \mathscr{O}_X \longrightarrow E.$$

In the next section we consider among other things the question of existence of nonconstant morphisms from $\mathbb{P}^3 \to Gr(2, \mathbb{C}^4)$.

3 Morphisms from Projective Space to $Gr(2, \mathbb{C}^k)$

The simplest projective variety of dimension three is $\mathbb{P}^3$. With Remark 2.10 in mind we consider the following:

Question. Does there exist a rank 2 vector bundle E on $\mathbb{P}^3$ with $\det(E)$ ample and with a surjection

$$\mathbb{C}^4 \otimes \mathscr{O}_{\mathbb{P}^3} \longrightarrow E?$$

Remark 3.1. A result of Fulton and Lazarsfeld [2] implies the following: if E is an ample vector bundle on $\mathbb{P}^3$ then there is no surjective morphism of vector bundles $\mathbb{C}^4 \otimes \mathscr{O}_{\mathbb{P}^3} \longrightarrow E$. Thus, if there is a rank 2 vector bundle E on $\mathbb{P}^3$ generated by four sections and with $\det(E)$ ample, then E has to be nontrivial and nonample. It is also easy to see that the bundles of the form:

$$\mathscr{O}_{\mathbb{P}^3}(a) \oplus \mathscr{O}_{\mathbb{P}^3} \quad (a > 0)$$

are not generated by four sections. Hence, if E is a rank 2 vector bundle on $\mathbb{P}^3$ generated by four sections and $\det(E)$ is ample, then E has to be indecomposable.

The following examples give an affirmative answer to the above question. These examples were pointed out to us by Gruson.

Example 3.2. Let $C = \ell_1 \cup \ell_2$ be a union of two disjoint lines in $\mathbb{P}^3$. Note that $\omega_C \simeq \mathscr{O}_{\mathbb{P}^3}(-2)|_C$, where ω_C is the dualizing sheaf. Hence, by a result of Serre [4, p. 93, Theorem 5.1.1], there exists a rank two vector bundle E on $\mathbb{P}^3$ and an exact sequence

$$0 \to \mathscr{O}_{\mathbb{P}^3} \to E \to I_C(c_1(E)) \to 0,$$

where I_C denotes the ideal sheaf of C in $\mathbb{P}^3$ and $c_1(E)$ denotes the first Chern class of E. It is easy to see that $c_1(E) = 2$ and $h^0(I_C(2)) = 4$, where h^0 stands for the dimension of the vector space of global sections. Thus we conclude that $h^0(E) = 5$. Note that C can be expressed as the intersection of three independent quadrics vanishing on C. (For example, if

$$C = \{X = 0 = Y\} \cup \{Z = 0 = W\},$$

then C is scheme theoretically defined by the three quadrics XZ, $XW - YZ$, $XZ - YW$.) This shows that there is a vector bundle surjection

$$\mathbb{C}^4 \otimes \mathscr{O}_{\mathbb{P}^3} \to E.$$

This defines by Theorem 2.5 a finite morphism $f : \mathbb{P}^3 \to Gr(2, \mathbb{C}^4)$. It can be seen that the image of $\mathbb{P}^3$ is a hypersurface in $Gr(2, \mathbb{C}^4)$ linearly equivalent to $2H$, where H is the ample generator of $\mathrm{Pic}(Gr(2, \mathbb{C}^4))$, and f is a morphism of degree two onto its image.

Example 3.3. Let C be a nonsingular elliptic curve of degree 8 in $\mathbb{P}^3$. Assume C has no 5-secant. Note that the dualizing sheaf ω_C is isomorphic to $\mathscr{O}_{\mathbb{P}^3}|_C$. Hence by a result of Serre [4, p. 93, Theorem 5.1.1] there is a rank two vector bundle E on $\mathbb{P}^3$ together with an exact sequence

$$0 \to \mathscr{O}_{\mathbb{P}^3} \to E \to I_C(c_1(E)) \to 0.$$

It is easy to see that $c_1(E) = 4$ and $h^0(I_C(2)) = 3$. Thus we conclude that $h^0(E) = 4$. Since C has no 5-secant, C is scheme theoretically defined by the three linearly independent quartics containing it [1, p. 579]. This shows that there is a vector bundle surjection

$$\mathbb{C}^4 \otimes \mathscr{O}_{\mathbb{P}^3} \to E.$$

By Theorem 2.5, this surjection defines a finite morphism $f : \mathbb{P}^3 \to Gr(2, \mathbb{C}^4)$.

Remark 3.4. In Example 3.3, we do not know what the image variety is nor whether the morphism is generically one–one. It would be interesting to investigate these questions.

Lemma 3.5. *Let E be a nontrivial rank two vector bundle on $\mathbb{P}^3$ together with a surjection*

$$\mathbb{C}^4 \otimes \mathscr{O}_{\mathbb{P}^3} \to E.$$

Then $c_1(E) = 2m$ and $c_2(E) = 2m^2$ for some integer $m \geq 1$.

Proof. The surjection

$$\mathbb{C}^4 \otimes \mathscr{O}_{\mathbb{P}^3} \to E$$

gives rise to an exact sequence of vector bundles

$$0 \to S \to \mathbb{C}^4 \otimes \mathscr{O}_{\mathbb{P}^3} \to E \to 0.$$

Let $c_1(E) = a$ and $c_2(E) = b$. Since E is generated by sections and nontrivial we see by Lemma 3.9 that $a > 0$. Now, since the rank of S is two, we obtain $0 = c_3(S) = 2b.a - a^3$. But $a \neq 0$ implies $a^2 - 2b = 0$. This gives the required result. $\square$

Remark 3.6. Examples 3.2 and 3.3 give some bundles corresponding to the cases $m = 1$ and $m = 2$ of Lemma 3.5. It will be an interesting problem to study the bundles for the other values of m and to see whether they are generated by 4-sections and if they are generated by 4-section, what are the properties of the induced finite morphisms from $\mathbb{P}^3$ to $Gr(2, \mathbb{C}^4)$. For example, for each $n \geq 1$, consider the morphism

$$f_n : \mathbb{P}^3 \to \mathbb{P}^3$$

defined by $(x_0, x_1, x_2, x_3) \mapsto (x_0^n, x_1^n, x_2^n, x_3^n)$. Since $f_n^*(\mathscr{O}_{\mathbb{P}^3}(1)) = \mathscr{O}_{\mathbb{P}^3}(n)$, we see that the rank two vector bundle $E_n = f_n^*(E)$ is generated by 4 sections with $c_1(E_n) = 2n$ and $c_2(E_n) = 2n^2$, where E is the bundle in Example 3.2 above. But in this case we do not get any new morphism from $\mathbb{P}^3$ to $Gr(2, \mathbb{C}^4)$.

The following result is a generalization of Corollary 2.9 to higher-dimensional projective spaces.

Theorem 3.7. *Let $n \geq 1$ and $m \geq n+2$ be two integers. Then there is no nonconstant morphism $f : \mathbb{P}^m \to Gr(2, \mathbb{C}^{n+2})$.*

Proof. First note that every nontrivial line bundle on $\mathbb{P}^m$ which is generated by sections is necessarily ample. Hence, if X is a projective variety and $f : \mathbb{P}^m \to X$ is a nonconstant morphism then the pull back by f of an ample bundle on X is ample on $\mathbb{P}^m$. This shows that any nonconstant morphism from $\mathbb{P}^m$ is necessarily finite onto its image.

The earlier observation shows that, if $m \geq n+2$ and $f : \mathbb{P}^m \to Gr(2, \mathbb{C}^{n+2})$ is a nonconstant morphism, then $f|_L$ is also a nonconstant morphism, where L is a linear subspace of $\mathbb{P}^m$ of dimension $n+2$. Thus, if we show that there is no nonconstant morphism from $\mathbb{P}^{n+2} \to Gr(2, \mathbb{C}^{n+2})$, then it follows that for any $m \geq n+2$ there are no nonconstant morphism from $\mathbb{P}^m \to Gr(2, \mathbb{C}^{n+2})$. From these remarks, to prove the theorem, it is enough to show that there is no nonconstant morphism $f : \mathbb{P}^{n+2} \to Gr(2, \mathbb{C}^{n+2})$.

Let $f : \mathbb{P}^{n+2} \to Gr(2, \mathbb{C}^{n+2})$ be a morphism. Then by pulling back the universal exact sequence

$$0 \to S \to \mathbb{C}^{n+2} \otimes \mathscr{O}_{Gr(2,\mathbb{C}^{n+2})} \to Q \to 0$$

on $Gr(2, \mathbb{C}^{n+2})$ by f we get an exact sequence

$$0 \to f^*(S) \to \mathbb{C}^{n+2} \otimes \mathscr{O}_{\mathbb{P}^{n+2}} \to f^*(Q) \to 0$$

on $\mathbb{P}^{n+2}$, where Q is the universal rank 2 quotient bundle and S is the kernel of the natural surjection $\mathbb{C}^{n+2} \otimes \mathscr{O}_{Gr(2,\mathbb{C}^{n+2})} \to Q$. Let $c_1(f^*(Q)) = a.H$ and $c_2(f^*(Q)) = b.H^2$ be the Chern class of $f^*(Q)$, where $H \in \mathrm{H}^2(\mathbb{P}^{n+2}, \mathbb{Z})$ is the generator, corresponding to the ample line bundle $\mathscr{O}_{\mathbb{P}^{n+2}}(1)$, of the cohomology algebra of $\mathbb{P}^{n+2}$. Then the total Chern class of $f^*(S)$ is

$$(1 + c_1(f^*(Q)) + c_2(f^*(Q)))^{-1} = (1 + a.H + b.H^2)^{-1} \tag{1}$$

Since the rank of $f^*(S)$ is n, the Chern classes $c_{n+1}(f^*(S))$ and $c_{n+2}(f^*(S))$ are zero. Hence we see from (1) that

$$\begin{aligned} c_{n+1}(f^*(S)) &= \sum_{i=0}^{[\frac{n+1}{2}]} (-1)^i \binom{n+1-i}{i} c_1(f^*(Q))^{n+1-2i} c_2(f^*(Q))^i \\ &= \left(\sum_{i=0}^{[\frac{n+1}{2}]} (-1)^i \binom{n+1-i}{i} a^{n+1-2i} b^i \right) H^{n+1} = 0, \end{aligned}$$

and hence the integers a and b satisfy the equation

$$\sum_{i=0}^{[\frac{n+1}{2}]} (-1)^i \binom{n+1-i}{i} a^{n+1-2i} b^i = 0. \tag{2}$$

Similarly, the vanishing of $c_{n+2}(f^*(S))$ implies that the integers a,b satisfy the equation

$$\sum_{i=0}^{[\frac{n+2}{2}]} (-1)^i \binom{n+2-i}{i} a^{n+2-2i} b^i = 0. \tag{3}$$

By Lemma 3.8 below we see that the only simultaneous integral solution of equations (2) and (3) is $(a,b) = (0,0)$. Hence $c_1(f^*(Q)) = 0$. Since E is generated by sections, Lemma 3.9 below implies $f^*(Q) \simeq \mathscr{O}_{\mathbb{P}^{n+2}} \oplus \mathscr{O}_{\mathbb{P}^{n+2}}$ and hence f is a constant map. This completes the proof of the theorem. $\square$

Lemma 3.8. *Let $n \geq 1$ be a fixed integer. Then the only simultaneous integral solution of the two equations*

$$\sum_{i=0}^{[\frac{n+1}{2}]} (-1)^i \binom{n+1-i}{i} X^{n+1-2i} Y^i = 0 \tag{4}$$

$$\sum_{i=0}^{[\frac{n+2}{2}]} (-1)^i \binom{n+2-i}{i} X^{n+2-2i} Y^i = 0 \tag{5}$$

is $(0,0)$.

Proof. Proof by induction on n. For $n = 1$ the equations (4) and (5) are

$$X^2 - Y = 0 \quad \text{and} \quad X^3 - 2XY = 0.$$

In this case the result is obvious. Assume $n > 1$ and that the result holds for $n-1$. Note that if (a,b) is a simultaneous solution of (4) and (5) and if one of a or b is zero then clearly the other is also zero. Assume both a and b are nonzero and (a,b) is a simultaneous solution of (4) and (5). Then multiplying (4) by X and subtracting by (5) we see that (a,b) is a solution of

$$\sum_{i=1}^{[\frac{n+2}{2}]} (-1)^i \binom{n+1-i}{i-1} X^{n+2-2i} Y^i = 0. \tag{6}$$

Since $b \neq 0$ we see that (a,b) satisfies the equation

$$\sum_{i=0}^{[n/2]} (-1)^i \binom{n-i}{i} X^{n-2i} Y^i = 0. \tag{7}$$

This implies that $(a,b) \neq (0,0)$ is a simultaneous solution of the equations (7) and (4), which leads to a contradiction to the induction assumption. This completes the proof of the lemma. $\square$

Lemma 3.9. *Let X be a projective variety. Let E be a vector bundle generated by sections. If $c_1(E) = 0$ then E is trivial.*

Proof. Choose n linearly independent sections which generate the stalk at one point, where n is the rank of E. Such sections exist because of our assumption that E is generated by sections. Then the set S of points where these sections fail to generate is the zero set of a nonzero section of $\det(E)$. But $\det(E)$ is generated by sections and $c_1(E) = 0$, hence $\det(E) = \mathscr{O}_X$. Since X is projective any nonzero section of $\mathscr{O}_X$ is a nonzero constant. Hence we see that E is trivial. □

Acknowledgements We thank L. Gruson for his encouragement and P. Sankaran for going through an earlier version and suggesting some improvements. The second author would like to thank the University of Lille, France, for its hospitality and IFIM for the financial grants.

References

1. J. D'Almeida: *Une involution sur un espace de modules de fibrés instantons* Bull. Soc. Math. Fr. **128** (2000), 577–584.
2. W. Fulton and R. Lazarsfeld: *On the connectedness of degeneracy loci and special divisors* Acta Math. 146 (1981), no. 3–4, 271–283.
3. R. Lazarsfeld: *Some applications of the theory of Positive vector bundles* In: Complete Intersections, C.I.M.E., Acireale 1983. Lect. Notes. Math. vol. 1092, Springer, Berlin, Heidelberg, New York, 1984.
4. C. Okonek, M. Schneider and H. Spindler: Vector bundles on complex projective spaces. Progress in Mathematics, No. 3, Birkhäuser, Boston, Mass., 1980.
5. H. Tango: *On (n-1)-dimensional projective spaces contained in the Grassmann variety* $Gr(n,1)$. J. Math. Kyoto Univ. 14-3 (1974) 415–460.

Adams Operations and the Brown-Gersten-Quillen Spectral Sequence

Alexander Merkurjev

Summary By means of Adams operations in algebraic K-theory we study the order of differentials in the Brown-Gersten-Quillen spectral sequence for a scheme.

1 Introduction

Let X be a separated scheme of finite type over a field F. We write $X_{(p)}$ for the set of points in X of dimension p. There is the *niveau spectral sequence*

$$E^1_{p,q} = \coprod_{x \in X_{(p)}} K_{p+q}F(x) \Rightarrow G_{p+q}(X)$$

converging to the G-groups of X (the K-groups of the category $M(X)$ of coherent sheaves on X) with the topological filtration [10, Sect. 7, Th. 5.4]. The term $E^1_{p,-p}$ coincides with the group of algebraic cycles of dimension p on X and $E^2_{p,-p}$ with the Chow group $\mathrm{CH}_p(X)$ of classes of cycles of dimension p [10, Sect. 7, Prop. 5.14].

The topological filtration on $G_n(X)$ is defined as follows. Write $M_p(X)$ for the category of coherent sheaves on X supported on a closed subset of dimension at most p. The image the homomorphism $K_n\big(M_p(X)\big) \to G_n(X)$ induced by the inclusion functor $M_p(X) \to M(X)$ is the p-th term $G_n(X)_{(p)}$ of the topological filtration on $G_n(X)$. The subsequent factors of the filtration are denoted by $G_n(X)_{(p/p-1)}$.

The spectral sequence yields surjective homomorphisms

$$\varphi_p : \mathrm{CH}_p(X) = E^2_{p,-p} \to G_0(X)_{(p/p-1)}.$$

Alexander Merkurjev
Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA,
e-mail: merkurev@math.ucla.edu

2010 Mathematics subject classification. 14C35, 19E08, 19L20.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_19,

The kernel of φ_p is detected by the differentials of the spectral sequence arriving at $E^*_{p,-p}$.

In this paper we find some constraints on the order of the differentials in the spectral sequence arriving at the G_0- and G_1-diagonals. We show that for any prime integer l, the Adams operations in algebraic K-theory developed in [4–6, 11], split the spectral sequence localized at l into a direct sum of $l-1$ summands. (For an analogue in topology see [1, p. 91].)

In the paper the word "scheme" means a quasi-projective scheme over a field and a "variety" is an integral scheme.

2 The Category A_l

For a prime integer l, let $\mathbb{Z}_{(l)}$ denote the localization of $\mathbb{Z}$ with respect to the prime ideal $l\mathbb{Z}$.

Lemma 2.1. *Let $f,g \in \mathbb{Z}_{(l)}[t]$ be polynomials such that f and g are coprime over $\mathbb{Q}$ and the residues $\bar{f}$ and $\bar{g}$ are coprime over $\mathbb{Z}/l\mathbb{Z}$. Then f and g are coprime over $\mathbb{Z}_{(l)}$, i.e., f and g generate the unit ideal in $\mathbb{Z}_{(l)}[t]$.*

Proof. Let I be the ideal in $\mathbb{Z}_{(l)}[t]$ generated by f and g. By assumption, I contains l^k and a polynomial $1-lh$ for some $k>0$ and $h \in \mathbb{Z}_{(l)}[t]$. Then $1-l^kh^k \in I$ and hence $1 \in I$. $\square$

2.1 Definition of A_l

Let l be a prime integer. We define the category A_l as follows. An object of A_l is a $\mathbb{Z}_{(l)}$-module M equipped with a filtration

$$\cdots \subset M^{(2)} \subset M^{(1)} \subset M^{(0)} \subset M^{(-1)} \subset \cdots$$

by submodules such that $M^{(n)} = 0$ for $n \gg 0$ and $M^{(n)} = M$ for $n \ll 0$, and endomorphisms $\psi^k_M \in \mathrm{End}_{\mathbb{Z}_{(l)}}(M)$ for all integers k prime to l, satisfying:

(i) $\psi^k_M \circ \psi^{k'}_M = \psi^{kk'}_M$ for all k and k' (in particular, ψ^k_M and $\psi^{k'}_M$ commute).
(ii) For any k, we have $\psi^k_M(M^{(i)}) \subset M^{(i)}$ and ψ^k_M acts on $M^{(i)}/M^{(i+1)}$ by multiplication by k^i for all i.

A morphism between two objects M and N in A_l is a $\mathbb{Z}_{(l)}$-module homomorphism $s : M \to N$ such that $s \circ \psi^k_M = \psi^k_N \circ s$ for all k. (We do not assume that s is compatible with the filtrations.)

Let M be an object of A_l and $r \in \mathbb{Z}$. Define the *shift* $M[r]$ of M as the module M together with the shifted filtration $M[r]^{(i)} = M^{(i+r)}$ and endomorphisms defined by $\psi^k_{M[r]} = k^{-r} \cdot \psi^k_M$. Clearly, the assignment $M \mapsto M[r]$ is an auto-functor of A_l.

2.2 A Decomposition

Let $M \in \mathcal{A}_l$ and let $a \le b$ be two integers such that $M^{(a)} = M$ and $M^{(b)} = 0$. The set J of all integers j such that $a \le j < b$ is called an *interval of* M.

Let $k > 1$ be an integer such that the congruence class $[k]_l$ of k modulo l is a generator of $(\mathbb{Z}/l\mathbb{Z})^\times$. Write $\Lambda = \mathbb{Z}/(l-1)\mathbb{Z}$. For any congruence class $\rho \in \Lambda$, consider the polynomial

$$f_\rho = \prod_{j \in \rho \cap J} (t - k^j) \tag{2.2}$$

over $\mathbb{Z}_{(l)}$, where J is an interval of M, and set

$$f = \prod_{\rho \in \Lambda} f_\rho = \prod_{j \in J} (t - k^j).$$

It follows from (ii) that $(\psi_M^k - k^j)\big(M^{(j)}\big) \subset M^{(j+1)}$ for any j, hence

$$f(\psi_M^k) = 0. \tag{2.3}$$

By construction, every pair of distinct polynomials f_ρ and $f_{\rho'}$ are coprime over $\mathbb{Q}$ and the residues $\bar{f}_\rho$ and $\bar{f}_{\rho'}$ are coprime over $\mathbb{Z}/l\mathbb{Z}$. By Lemma 2.1, f_ρ and $f_{\rho'}$ are coprime over $\mathbb{Z}_{(l)}$. By the Chinese Remainder Theorem, the factor ring $\mathbb{Z}_{(l)}[t]/(f)$ is canonically isomorphic to the product of the rings $\mathbb{Z}_{(l)}[t]/(f_\rho)$ over all $\rho \in \Lambda$. Note that the image of f_ρ in $\mathbb{Z}_{(l)}[t]/(f_{\rho'})$ is zero if $\rho' = \rho$ and invertible otherwise.

It follows then from (2.3) that M has a natural structure of a module over $\mathbb{Z}_{(l)}[t]/(f)$, where t acts by ψ_M^k. Therefore,

$$M = \coprod_{\rho \in \Lambda} M_\rho \tag{2.4}$$

with $M_\rho = \operatorname{Ker} f_\rho(\psi_M^k)$.

We claim that the submodules M_ρ do not depend on the choice of the interval J of M. Indeed, let J' be another interval of M containing J, f'_ρ the polynomials constructed for J' and $M'_\rho = \operatorname{Ker} f'_\rho(\psi_M^k)$. Then f_ρ divides f'_ρ, and hence

$$M_\rho = \operatorname{Ker} f_\rho(\psi_M^k) \subset \operatorname{Ker} f'_\rho(\psi_M^k) = M'_\rho.$$

Therefore, in view of (2.4), both for M_ρ and M'_ρ, we deduce that $M_\rho = M'_\rho$.

For any $\rho \in \Lambda$ set $\widehat{f_\rho} = f/f_\rho \in \mathbb{Z}_{(l)}[t]$. Then the polynomials $\{\widehat{f_\rho}\}_{\rho \in \Lambda}$ are coprime.

Lemma 2.5. $\operatorname{Ker} f_\rho(\psi_M^k) = \operatorname{Im} \widehat{f_\rho}(\psi_M^k)$ *for all* $\rho \in \Lambda$.

Proof. Let $\psi = \psi_M^k$. Because $f_\rho(\psi)\widehat{f_\rho}(\psi) = f(\psi) = 0$, the image of $\widehat{f_\rho}(\psi)$ is contained in the kernel of $f_\rho(\psi)$. As f_ρ and $\widehat{f_\rho}$ are coprime, there are polynomials g and h in $\mathbb{Z}_{(l)}[t]$ such that $f_\rho g + \widehat{f_\rho} h = 1$. Then for any $m \in \operatorname{Ker} f_\rho(\psi)$, we have $m = \widehat{f_\rho}(\psi)h(\psi)(m) \in \operatorname{Im} \widehat{f_\rho}(\psi)$, i.e., $\operatorname{Ker} f_\rho(\psi) \subset \operatorname{Im} \widehat{f_\rho}(\psi)$. $\square$

We also prove that the decomposition (2.4) does not depend on the choice of the integer k. Let $k' > 1$ be an integer such that the congruence class $[k']_l$ is a generator of $(\mathbb{Z}/l\mathbb{Z})^{\times}$. Define the polynomials f, f'_ρ, and $\widehat{f'}$ in $\mathbb{Z}_{(l)}[t]$ as earlier with k replaced by k'. Then M is a direct sum of the submodules $M'_\rho = \operatorname{Ker} f'_\rho(\psi_M^{k'})$ over all $\rho \in \Lambda$.

Lemma 2.6. *$M_\rho = M'_\rho$ for all $\rho \in \Lambda$.*

Proof. Take any $\rho \in \Lambda$ and $j \in J$. If $j \in \rho$, then $t - (k')^j$ divides f'_ρ. If $j \notin \rho$, then $t - (k)^j$ divides $\widehat{f}_\rho$. It follows that $f'_\rho(\psi_M^{k'})\widehat{f}_\rho(\psi_M^k) = 0$ and hence by Lemma 2.5,

$$M_\rho = \operatorname{Ker} f_\rho(\psi_M^k) = \operatorname{Im} \widehat{f}_\rho(\psi_M^k) \subset \operatorname{Ker} f'_\rho(\psi_M^{k'}) = M'_\rho.$$

By symmetry, $M'_\rho \subset M_\rho$. □

Thus, the submodules M_ρ in the decomposition (2.4) depend only on the object M in the category A_l.

Let $s : M \to N$ be a morphism in A_l. Choose a common interval J for both M and N and let f_ρ be the polynomials defined by (2.2). Then $s \circ f_\rho(\psi_M^k) = f_\rho(\psi_N^k) \circ s$, hence

$$s\big(M_\rho\big) = s\big(\operatorname{Ker} f_\rho(\psi_M^k)\big) \subset \operatorname{Ker} f_\rho(\psi_N^k) = N_\rho,$$

i.e., s induces a $\mathbb{Z}_{(l)}$-module homomorphism $M_\rho \to N_\rho$. Thus for every $\rho \in \Lambda$, we have a functor from A_l to the category of $\mathbb{Z}_{(l)}$-modules taking an object M to M_ρ.

Proposition 2.7. *For an object M in A_l and an integer r, we have $M[r]_\rho = M_{\rho+r}$ for all $\rho \in \Lambda$.*

Proof. Let J be an interval of M. Then $J' = J - r$ is an interval of $M[r]$. Let $\{f_\rho\}_{\rho\in\Lambda}$ and $\{f'_\rho\}_{\rho\in\Lambda}$ be the polynomials constructed in (2.2) for J and J', respectively. Then

$$f_{\rho+r}\big(\psi_M^k\big) = \prod_{j\in(\rho+r)\cap J} \big(\psi_M^k - k^j\big) = \prod_{i\in\rho\cap J'} \big(k^r \psi_{M[r]}^k - k^{i+r}\big) = k^{rd} \cdot f'_\rho\big(\psi_{M[r]}^k\big),$$

where $d = \deg(f_\rho)$. It follows that

$$M[r]_\rho = \operatorname{Ker} f'_\rho\big(\psi_{M[r]}^k\big) = \operatorname{Ker} f_{\rho+r}\big(\psi_M^k\big) = M_{\rho+r}.$$

□

3 Spectral Sequences in K-Theory

3.1 Adams Operations

Let M be a scheme and $Z \subset M$ a closed subscheme. We write $K_m^Z(M)$ for the K-groups of M with support in Z and $F_\gamma^i K_m^Z(M)$ for the i-th term of the (finite) gamma-filtration on $K_m^Z(M)$ (see [11, Sect. 4]). If M is a regular scheme, there exists a canonical isomorphism

$$G_m(Z) \simeq K_m^Z(M),$$

where $G_m(Z)$ is the K-group of the category of coherent sheaves on Z [3, Th.2.14].

For any integer k, there is the Adams operation ψ^k on $K_m^Z(M)$ satisfying the following properties [11], [7, Sect. 9]:

- ψ^k is a group endomorphism of $K_m^Z(M)$.
- ψ^k respects the gamma-filtration $F_\gamma^i K_m^Z(M)$.
- ψ^k acts as multiplication by k^i on the subsequent factor $F_\gamma^{(i/i+1)} K_m^Z(M)$.
- $\psi^k \psi^{k'} = \psi^{kk'}$, in particular, φ^k and $\varphi^{k'}$ commute.

Let l be a prime integer. Then the $\mathbb{Z}_{(l)}$-module $K_m^Z(X)\mathbb{Z}_{(l)}$ together with the gamma-filtration and the Adams operations ψ^k on it yield an object of the category $\mathcal{A}_l$. Therefore, $K_m^Z(X)\mathbb{Z}_{(l)}$ decomposes as in (2.4) into a direct sum of submodules $\left(K_m^Z(X)\mathbb{Z}_{(l)}\right)_\rho$ over all $\rho \in \Lambda = \mathbb{Z}/(l-1)\mathbb{Z}$.

Let Z be a scheme. For any integer $k > 0$, there is a well-defined map (see [11, Sect. 4]):

$$\theta^k : K_0(Z) \to K_0(Z),$$

natural in Z, satisfying:

- For every exact sequence of vector bundles $0 \to E' \to E \to E'' \to 0$ over Z, we have $\theta^k[E] = \theta^k[E'] \cdot \theta^k[E'']$.
- For every line bundle L over Z,

$$\theta^k[L] = 1 + [L^{-1}] + [L^{-2}] + \cdots + [L^{-k+1}].$$

In particular, rank $\theta^k(\alpha) = k^{\mathrm{rank}(\alpha)}$ for every $\alpha \in K_0(Z)$.

The following variant of the Riemann-Roch formula was proven in [11, Th. 3] (see also [9, 2.6.2]):

Proposition 3.1. *Let M be a regular variety of dimension d and let $Z \subset M$ be a regular closed subvariety of dimension p. Let N be the normal bundle (of rank $d-p$) for the closed embedding $f : Z \to M$. Then there is an isomorphism*

$$f_* : K_*(Z) = K_*^Z(Z) \xrightarrow{\sim} K_*^Z(M)$$

such that

$$f_*\left(\psi^k(\theta^k(N) \cdot \alpha)\right) = \psi^k\left(f_*(\alpha)\right)$$

for any $\alpha \in K_*(Z)$ and any k.

Corollary 3.2. *Suppose that, in addition, N is a trivial bundle. Then $\theta(N) = k^{d-p}$ and hence*

$$f_*\left(k^{d-p} \cdot \psi^k(\alpha)\right) = \psi^k\left(f_*(\alpha)\right).$$

Thus, for a prime integer l, f_* induces an isomorphism

$$\big(K_*(Z)\mathbb{Z}_{(l)}\big)[p-d] \xrightarrow{\sim} K_*^Z(M)\mathbb{Z}_{(l)}$$

in the category $\mathcal{A}_l$.

3.2 Localization Exact Sequence and the Niveau Spectral Sequence

Let M be a regular scheme. If $Z' \subset Z$ are closed subscheme of M, then there is an exact localization sequence [7, 9.3]:

$$\cdots \to K_m^{Z'}(M) \to K_m^{Z}(M) \to K_m^{Z\setminus Z'}(M\setminus Z') \to K_{m-1}^{Z'}(M) \to \cdots \tag{3.3}$$

that is isomorphic to the localization exact sequence [10, Sect. 7, Prop. 3.2]:

$$\cdots \to G_m(Z') \to G_m(Z) \to G_m(Z\setminus Z') \to G_{m-1}(Z') \to \cdots \tag{3.4}$$

The homomorphisms in (3.3) commute with the Adams operations by [7, Remark 9.6(1)]. Then, localizing at a prime integer l, we can view (3.3) and (3.4) as sequences of morphisms in the category $\mathcal{A}_l$.

Let X be a scheme. We embed X into a regular variety M of dimension d as a closed subscheme. For a pair of integers p and q set

$$E^1_{p,q} = \operatorname{colim} K_{p+q}^{Z\setminus Z'}(M\setminus Z') = \operatorname{colim} G_{p+q}(Z\setminus Z'),$$

where the colimit is taken over all pairs (Z', Z) with Z a closed subscheme of X of dimension p and Z' a closed subscheme of Z of dimension $p-1$. Note that for any such Z one can find a Z' such that $Z\setminus Z'$ is regular and the normal bundle of $Z\setminus Z'$ in $M\setminus Z'$ is trivial. It follows that

$$E^1_{p,q} = \coprod_{x\in X_{(p)}} K_{p+q}F(x)$$

and for any prime integer l,

$$E^1_{p,q}\mathbb{Z}_{(l)} \simeq \coprod_{x\in X_{(p)}} \big(K_{p+q}F(x)\mathbb{Z}_{(l)}\big)[p-d]$$

in $\mathcal{A}_l$ by Corollary 3.2. It follows from Proposition 2.7 that for any $\rho\in\Lambda$,

$$\big(E^1_{p,q}\mathbb{Z}_{(l)}\big)_\rho = \coprod_{x\in X_{(p)}} \big(K_{p+q}F(x)\mathbb{Z}_{(l)}\big)_{\rho+p-d}. \tag{3.5}$$

Set

$$D^1_{p,q} = \operatorname{colim} K^Z_{p+q}(M) = \operatorname{colim} G_{p+q}(Z),$$

where the colimit is taken over all closed subschemes Z of X of dimension p. Taking colimits of the exact sequences (3.3) and (3.4) we get the exact sequences:

$$\cdots \to E^1_{p,q} \to D^1_{p-1,q} \to D^1_{p,q-1} \to E^1_{p,q-1} \to \cdots$$

The latter yields an exact couple and therefore, a (homological) *Brown-Gersten-Quillen (BGQ) spectral sequence*:

$$E^1_{p,q} = \coprod_{x \in X_{(p)}} K_{p+q}F(x) \Rightarrow G_{p+q}(X). \tag{3.6}$$

It is supported in the area $0 \le p \le \dim(X)$ and $p+q \ge 0$. In particular, all the differentials arriving at $E^s_{p,q}$ with $p+q<0$ are trivial. We shall get some information on the differentials arriving at $E^s_{p,q}$ with $p+q=0$ or 1.

Lemma 3.7. *For any prime integer l and any $\rho \in \Lambda$, we have*

$$\left(E^s_{p,q}\mathbb{Z}_{(l)}\right)_\rho = \begin{cases} E^s_{p,q}\mathbb{Z}_{(l)}, & \textit{if } \rho = [d+q]_{l-1}; \\ 0, & \textit{otherwise} \end{cases}$$

for any $s \ge 1$ if $p+q \le 2$.

Proof. By [11, Sect. 2], for a field L and $m \le 2$, we have $F^m_\gamma K_m(L) = K_m(L)$ and $F^{m+1}_\gamma K_m(L) = 0$, hence ψ^k acts on $K_m(L)$ by multiplication by k^m. Therefore,

$$\left(K_m(L)\mathbb{Z}_{(l)}\right)_\rho = \begin{cases} K_m(L)\mathbb{Z}_{(l)}, & \text{if } \rho = [m]_{l-1}; \\ 0, & \text{otherwise.} \end{cases}$$

The statement now follows from (3.5). □

Theorem 3.8. *Let X be a scheme. Let*

$$\partial : E^s_{p,q} \to E^s_{p-s,q+s-1}$$

be the differential in the spectral sequence (3.6) *with $p+q \le 2$. Then the order* $\operatorname{ord}(\partial)$ *is finite and if l is a prime divisor of* $\operatorname{ord}(\partial)$*, then $l \le p$ and $l-1$ divides $s-1$.*

Proof. If $s > p$, then $\partial = 0$ since $E^s_{p-s,q+s-1} = 0$, so we may assume that $s \le p$.

We claim that if l is a prime integer such that $\partial\mathbb{Z}_{(l)} \ne 0$, then $l-1$ divides $s-1$. Set $\rho = [q+d]_{l-1} \in \Lambda$. By Lemma 3.7, the (nonzero) image of $\partial\mathbb{Z}_{(l)}$ is contained in $(E^s_{p-s,q+s-1}\mathbb{Z}_{(l)})_\rho$ and therefore, $\rho + d = [q+d+s-1]_{l-1}$, i.e., $l-1$ divides $s-1$. The claim is proved.

Taking $l > s$, we get $\partial\mathbb{Z}_{(l)} = 0$ from the claim, i.e., ∂ has finite order.

Let l be a prime divisor of $\operatorname{ord}(\partial)$. Then $\partial\mathbb{Z}_{(l)} \ne 0$ and hence by the claim, $l-1$ divides $s-1$. In particular, $l \le s \le p$. □

Example 3.9. Let X be the Severi-Brauer variety of right ideals of dimension l of a central simple algebra of a prime degree l over F. As over a splitting field extension of degree l the variety X is isomorphic to the projective space $\mathbb{P}^{l-1}$, and the BGQ spectral sequence for a projective space degenerates at E_2, all the differentials of the BGQ spectral sequence for X are l-torsion. As $\dim(X) = l-1$, it follows from Theorem 3.8 that all the differentials arriving at the G_0- and G_1-diagonals are trivial. This result was proved in [8] with the help of higher Chern classes.

3.3 Motivic Spectral Sequence

Let X be a smooth scheme. We write $H^i(X,\mathbb{Z}(j))$ for the motivic cohomology groups [12].

The following (cohomological) motivic spectral sequence was constructed in [2]:

$$E_2^{p,q} = H^{p-q}(X,\mathbb{Z}(-q)) \Rightarrow K_{-p-q}(X) \tag{3.10}$$

The spectral sequence is compatible with the Adams operations ψ^k, and ψ^k acts by multiplication by k^q on $E_2^{p,q}$ [7, Th. 9.7].

Theorem 3.11. *Let X be a smooth scheme. Let*

$$\partial : E_s^{p,q} \to E_s^{p+s,q-s+1}$$

be the differential in the spectral sequence (3.10)*. Then* $\operatorname{ord}(\partial)$ *is finite and if l is a prime divisor of* $\operatorname{ord}(\partial)$ *then $l \le \dim(X) - p$ and $l-1$ divides $s-1$.*

Proof. The proof is parallel to the one of Theorem 3.8. One remarks that $\partial = 0$ if $s > \dim(X) - p$. □

Acknowledgements I would like to thank Marc Levine for useful discussions. The work has been supported by the NSF grant DMS #0652316.

References

1. J. F. Adams, *Lectures on generalised cohomology*, Category Theory, Homology Theory and their Applications, III (Battelle Institute Conference, Seattle, Wash., 1968, Vol. Three), Springer, Berlin, 1969, pp. 1–138.
2. E. Friedlander and A. Suslin, *The spectral sequence relating algebraic K-theory to motivic cohomology*, Ann. Sci. École Norm. Sup. (4) **35** (2002), no. 6, 773–875.
3. H. Gillet, *Riemann-Roch theorems for higher algebraic K-theory*, Adv. in Math. **40** (1981), no. 3, 203–289.
4. H. L. Hiller, *λ-rings and algebraic K-theory*, J. Pure Appl. Algebra **20** (1981), no. 3, 241–266.
5. Ch. Kratzer, *λ-structure en K-théorie algébrique*, Comment. Math. Helv. **55** (1980), no. 2, 233–254.

6. ______, *Opérations d'Adams et représentations de groupes*, Enseign. Math. (2) **26** (1980), no. 1–2, 141–154.
7. M. Levine, *K-theory and motivic cohomology of schemes*, http://www.math.uiuc.edu/K-theory/0336/ (1999).
8. A. S. Merkurjev and A. A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 5, 1011–1046, 1135–1136.
9. I. Panin, *Riemann-Roch theorems for oriented cohomology*, Axiomatic, enriched and motivic homotopy theory, NATO Sci. Ser. II Math. Phys. Chem., vol. 131, Kluwer Acadamic Publisher, Dordrecht, 2004, pp. 261–333.
10. D. Quillen, *Higher algebraic K-theory. I*, (1973), 85–147. Lecture Notes in Math., Vol. 341.
11. C. Soulé, *Opérations en K-théorie algébrique*, Can. J. Math. **37** (1985), no. 3, 488–550.
12. V. Voevodsky, A. Suslin, and E. Friedlander, *Cycles, transfers, and motivic homology theories*, Princeton University Press, Princeton, NJ, 2000.

Non-self-dual Stably Free Modules

Madhav V. Nori, Ravi A. Rao, and Richard G. Swan

With best wishes to Parimala on the 21st of November

Summary We give several proofs that a stably free module of even rank need not be self-dual.

1 Introduction

In this note we prove that the projective module corresponding to the universal unimodular vector of odd size > 3 is not isomorphic to its dual. We give three proofs which depend on topological facts, and also two algebraic arguments, one using Suslin matrices and one using Riemann–Roch algebra.

For any commutative ring R, we set

$$A_n(R) = \frac{R[X_1,\ldots,X_n,Y_1,\ldots,Y_n]}{(\sum_{i=1}^n X_iY_i - 1)}.$$

Theorem 1.1. *Let $A = A_{2n-1}(\mathbb{Z})$. Let x_i denote the class of X_i, and y_i denote the class of Y_i in A, for all i. Let $v = (x_1,\ldots,x_{2n-1})$, $v^* = (y_1,\ldots,y_{2n-1})$. Then for*

Madhav V. Nori
Department of Mathematics, The University of Chicago, Chicago, IL 60637, USA,
e-mail: nori@math.uchicago.edu

Ravi A. Rao
School of Mathematics, Tata Institute of Fundamental Research, Mumbai 400 005, India,
e-mail: ravi@math.tifr.res.in

Richard G. Swan
Department of Mathematics, The University of Chicago, Chicago, IL 60637, USA,
e-mail: swan@math.uchicago.edu

2010 Mathematics subject classification. Primary: 13C10, 19A13. Secondary: 14C25, 19B14, 19L10, 55Q05, 55R25.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_20,

$n > 2$, v, v^* are not in the same $\mathrm{GL}_{2n-1}(A)$ *orbit, i.e., the projective module P (of rank $2n-2$) defined by v is not isomorphic to the projective module P^* defined by v^*.*

Thus, one gives examples of non-self-dual stably free modules of rank $2m$ for every even $2m \geq 4$. We now explain why these examples do not work when the rank r is odd or when $r = 2$.

Let P be the projective $A_n(R)$-module of rank $n-1$ corresponding to the unimodular row $v = (x_1, \ldots, x_n)$. Then $P^* = \mathrm{Hom}_R(P, R)$ is isomorphic to the projective R-module corresponding to the unimodular row $w = (y_1, \ldots, y_n)$.

It can be seen easily that P and P^* are isomorphic when rank P is odd; in fact, the rows v, w are in the same elementary orbit by a lemma of Roitman, see [9, Lemma 1].

In [1, Prop. 4.4, Cor. 4.5], Bass showed that any projective R-module P of rank two admits a symplectic structure if and only if the invertible module $\wedge^2 P$ is free. In particular, if $P \oplus R$ is free then P is isomorphic to its dual.

2 Proof via Clutching Functions

Let $\mathrm{Vect}_n(R)$ denote the set of isomorphism classes of projective R-modules of rank n, where R is a commutative ring. The free module R^n serves as the base point $c(n)$ of the set $\mathrm{Vect}_n(R)$. The map $P \mapsto R \oplus P$ defines $f : \mathrm{Vect}_{n-1}(R) \to \mathrm{Vect}_n(R)$. The kernel of f, i.e., $f^{-1}c(n)$, consists of the isomorphism classes of projective modules P such that there is an isomorphism $T : R \oplus P \cong R^n$. In such a situation, with $(1,0) \in R \oplus P$, we obtain $x = (x_1, x_2, ..., x_n) = T(1,0) \in R^n$. With $p : R \oplus P \to R$ denoting the projection to the first factor, we also obtain $y = p \circ T^{-1} : R^n \to R$. Identifying $\mathrm{Hom}_R(R^n, R)$ with R^n in the standard manner, we get $y \in R^n$ so that $\sum_{i=1}^n x_i y_i = 1$. The set of $(x,y) \in R^n \times R^n$ satisfying this identity is $D_n(R)$, the set of ring homomorphisms $A_n(\mathbb{Z}) \to R$.

Note also that every $(x,y) \in D_n(R)$ gives rise to the projective module $\ker(y) : R^n \to R$, which is naturally isomorphic to R^n/Rx. This gives rise to $g : B_n(R) \to \mathrm{Vect}_{n-1}(R)$ and we obtain an exact sequence of pointed sets

$$D_n(R) \to \mathrm{Vect}_{n-1}(R) \to \mathrm{Vect}_n(R). \tag{1}$$

Now let Z be a compact Hausdorff space and let $C(Z)$ be the ring of continuous $\mathbb{C}$-valued functions on Z. By [14] we can identify $\mathrm{Vect}_k(C(Z))$ with the set of isomorphism classes of complex rank k bundles on Z. To simplify notation, we denote $\mathrm{Vect}_k(C(Z))$ by $\mathrm{Vect}_k(Z)$ in this situation. The case of immediate interest is $Z = SY$ the suspension of a compact Hausdorff space Y. Here, by employing clutching functions (cf. [7, 10]), we see that $\mathrm{Vect}_k(SY)$ is identified with $[Y; \mathrm{GL}_k(\mathbb{C})]$, the set of homotopy classes of continuous maps $Y \to \mathrm{GL}_k(\mathbb{C})$. In addition, ring homomorphisms $A_n(\mathbb{Z}) \to C(Z)$ are readily identified with continuous maps $Z \to S^{2n-1}(\mathbb{C})$

where $S^{2n-1}(\mathbb{C}) = \{(x,y) \in \mathbb{C}^n \times \mathbb{C}^n : \sum x_i y_i = 1\}$. The exact sequence of pointed sets (1) reads now as an exact sequence of groups

$$[SY; S^{2n-1}(\mathbb{C})] \to [Y; \mathrm{GL}_{n-1}(\mathbb{C})] \to [Y; \mathrm{GL}_n(\mathbb{C})].$$

When Y is a sphere, the above is contained in the long exact sequence of homotopy groups associated to the fiber bundle $\mathrm{GL}_n(\mathbb{C}) \to S^{2n-1}(\mathbb{C})$ with fiber $\mathrm{GL}_{n-1}(\mathbb{C})$ given by $g \in \mathrm{GL}_n(\mathbb{C}) \mapsto (x,y)$, where x is the first column of g and y is the first row of g^{-1}. When Y is the real sphere S^{2n-2}, the preceding arrow in the long exact sequence is $\pi_{2n-1}(\mathrm{GL}_n(\mathbb{C})) \to [SY; S^{2n-1}(\mathbb{C})]$. Regarding the real $(2n-1)$-sphere S^{2n-1} as the unit sphere in $\mathbb{C}^n$, the embedding $S^{2n-1} \to S^{2n-1}(\mathbb{C})$ given by $i(x) = (x, \bar{x})$ is readily checked to be a homotopy equivalence. Thus, $[SY; S^{2n-1}(\mathbb{C})]$ is naturally identified with $\mathbb{Z}$. Thanks to Bott periodicity, the group $\pi_{2n-1}(\mathrm{GL}_n(\mathbb{C})) = \mathrm{Vect}_n(S^{2n})$ is also identified canonically with $\mathbb{Z}$. The image of the arrow $\pi_{2n-1}(\mathrm{GL}_n(\mathbb{C})) \to [SY; S^{2n-1}(\mathbb{C})]$ is $(n-1)!\mathbb{Z}$, since $\pi_{2n-2}(\mathrm{GL}_{n-1}(\mathbb{C})) = \mathbb{Z}/(n-1)!\mathbb{Z}$ and $\pi_{2n-2}(\mathrm{GL}_n(\mathbb{C})) = 0$ by [3,4]. Thus with $Z = SY = S^{2n-1}$, we see that $a, b : S^{2n-1} \to S^{2n-1}(\mathbb{C})$ give rise to isomorphic rank $(n-1)$ complex vector bundles on S^{2n-1} if and only if $\deg(a) \equiv \deg(b) \mod (n-1)!$.

With $i, j : S^{2n-1} \to S^{2n-1}(\mathbb{C})$ given by $i(x) = (x, \bar{x})$ and $j(x) = (\bar{x}, x)$, we see that $\deg(j) = (-1)^n \deg(i) = (-1)^n$, so the corresponding rank $(n-1)$ projective modules over $C(S^{2n-1})$ are isomorphic to each other if and only if $1-(-1)^n$ is divisible by $(n-1)!$, in other words, if n is even or $n \leq 3$. In particular, when n does not satisfy these restrictions, the projective modules given by the unimodular rows x and y are not isomorphic in the universal situation.

3 Proof via Classifying Spaces

Regard S^{2n-1} as the unit sphere in $\mathbb{C}^n$ with coordinates $z_1, \ldots, z_n$. If E is the vector bundle on S^{2n-1} defined by the unimodular row $(z_1, \ldots, z_n)$ then the associated principal bundle is $U(n-1) \longrightarrow U(n) \longrightarrow S^{2n-1}$ cf. [7, Ch. 8, Theorem 7.1]. It is classified by a map $f : S^{2n-1} \longrightarrow BU(n-1)$, or, equivalently, an element $\gamma \in \pi_{2n-1} BU(n-1)$. If $\iota = [1_{S^{2n-1}}] \in \pi_{2n-1} S^{2n-1}$ then $\gamma = f_*(\iota)$. Map $U(n) \longrightarrow S^{2n-1}$ to the universal bundle getting

$$\begin{array}{ccccc}
U(n-1) & \longrightarrow & U(n) & \longrightarrow & S^{2n-1} \\
\Big\| & & \Big\downarrow & & \Big\downarrow f \\
U(n-1) & \longrightarrow & P & \longrightarrow & BU(n-1).
\end{array}$$

As P is contractible, the map of homotopy sequences gives:

$$\begin{array}{ccccc} \pi_{2n-1}S^{2n-1} & \xrightarrow{\partial} & \pi_{2n-2}U(n-1) & \longrightarrow & \pi_{2n-2}U(n)=0 \\ {\scriptstyle f_*}\downarrow & & \| & & \\ \pi_{2n-1}BU(n-1) & \xrightarrow{\approx} & \pi_{2n-2}U(n-1) & & \end{array}$$

Note that $\pi_{2n-2}U(n)=0$ by [4], and so ∂, and therefore f_*, is onto and γ generates $\pi_{2n-1}BU(n-1)=\mathbb{Z}/(n-1)!$ by [3].

Now E^* is defined by $\bar{z}_1,\ldots,\bar{z}_n$, and so is $c^*(E)$ where $c: S^{2n-1}\longrightarrow S^{2n-1}$ is given by $(z_1,\ldots,z_n)\longrightarrow(\bar{z}_1,\ldots,\bar{z}_n)$. Therefore, E^* is classified by:

$$S^{2n-1}\xrightarrow{c}S^{2n-1}\xrightarrow{f}BU(n-1)$$

or, equivalently, by $\gamma'=f_*c_*(\iota)$. Now c has degree $(-1)^n$ so $c_*(\iota)=(-1)^n\iota$ and $\gamma'=(-1)^n f_*(\iota)=(-1)^n\gamma$. So if n is odd, $n>2$, then $\gamma'\neq\gamma$ showing that $E^*\not\approx E$. $\square$

4 Proof via Homotopy Theory

We now give an alternative proof of Theorem 1.1 using only elementary homotopy theory in addition to Bott's calculations.

Regard $A=A_n(\mathbb{C})$ as the ring of complex polynomial functions on the $(2n-1)$-sphere S^{2n-1} in $\mathbb{C}^n$ by sending x_i to z_i and y_i to $\bar{z}_i$.

Let $f=(f_1,\ldots,f_n)$ be a unimodular row over A. It defines a map $S^{2n-1}\to S^{2n-1}$ sending z to $f(z)/\|f(z)\|$. We write $\deg f$ for the degree of this map and write $[f]$ for its homotopy class in $\pi_{2n-1}(S^{2n-1})=\mathbb{Z}$. So $[f]=\deg f\,\iota$ where ι is the class of the identity map, which generates $\pi_{2n-1}(S^{2n-1})$.

Let $P(f)$ be the projective module defined by f so that $Af\oplus P(f)=A^n$.

Theorem 4.1. *If v and w are unimodular rows of length n over $A_n(\mathbb{C})$ and $P(v)\approx P(w)$ then* $\deg v\equiv\deg w \mod (n-1)!$.

Proof. By taking the direct sum of $P(v)\approx P(w)$ with $Av\approx Aw$ (by $v\mapsto w$) we get an element g of $\mathrm{GL}_n(A)$ such that $gv=w$ cf. [8, Prop. I.4.8]. Regarding elements of A as functions on S^{2n-1} we have $g: S^{2n-1}\to\mathrm{GL}_n(\mathbb{C})$ and, passing to homotopy classes we get $[g]\in\pi_{2n-1}(\mathrm{GL}_n(\mathbb{C}))=\pi_{2n-1}(U(n))$ and $([g],[v])$ maps to $[w]$ under the map

$$\pi_{2n-1}(U(n))\times\pi_{2n-1}(S^{2n-1})=\pi_{2n-1}(U(n)\times S^{2n-1})\to\pi_{2n-1}(S^{2n-1})$$

As this map is linear we have $p_*[g]+[v]=[w]$ where $p: U(n)\to S^{2n-1}$ by $g\mapsto gs$ where s is a base point. Now p is a fibration with fiber $U(n-1)$ [10]. Using Bott's calculations from [3, 4], its homotopy sequence

$$\pi_{2n-1}(U(n))\xrightarrow{p_*}\pi_{2n-1}(S^{2n-1})\to\pi_{2n-2}(U(n-1))\to\pi_{2n-2}(U(n))$$

takes the form

$$\pi_{2n-1}(U(n)) \xrightarrow{p_*} \mathbb{Z} \to \mathbb{Z}/(n-1)! \to 0$$

showing that $\operatorname{im} p_* = (n-1)!\mathbb{Z}$. Therefore, $[v] \equiv [w] \mod (n-1)!$ and the theorem follows. ☐

Corollary 4.2. *If v is a unimodular row of length n over $A_n(\mathbb{C})$ and $P(v)$ is free then* $\deg v \equiv 0 \mod (n-1)!$

As $\deg(x_1{}^{e_1}, \dots, x_n{}^{e_n}) = e_1 \cdots e_n$, this reproves the following result of [18, Theorem 3.1].

Corollary 4.3. *If $P(x_1{}^{e_1}, \dots, x_n{}^{e_n})$ is free then $e_1 \cdots e_n \equiv 0 \mod (n-1)!$*

Corollary 4.4. *If v and w are unimodular rows of length n over $A_n(\mathbb{C})$ and $P(v)^* \approx P(w)$ then* $\deg w \equiv (-1)^n \deg v \mod (n-1)!$.

Proof. Suppose $v \cdot u = 1$. Then $P(v)^* \approx P(u)$ [8, Prop. I.4.10]. The map $u/\|u\|$ is homotopic to the map $\bar{v}/\|\bar{v}\|$ by $(tu + (1-t)\bar{v})/\|(tu + (1-t)\bar{v})\|$. Note that $tu + (1-t)\bar{v}$ is never 0 because its inner product with $\bar{u}$ is $t\|u\|^2 + 1 - t > 0$. Now the map $\bar{v}$ is the composition of v with the map of S^{2n-1} to itself sending $(z_1, \dots, z_n)$ to its conjugate. This map reverses the sign of the n imaginary components and so has degree $(-1)^n$. Therefore, $\deg u = (-1)^n \deg v$ and the theorem applies. ☐

In particular, $P(v) \approx P(v)^*$ implies that $\deg v \equiv (-1)^n \deg v \mod (n-1)!$ so if n is odd, $\deg v \equiv 0 \mod (n-1)!/2$. If $v = (x_1, \dots, x_n)$ then $\deg v = 1$ so, for odd n, $P(v) \approx P(v)^*$ implies that $n \leq 3$.

Corollary 4.5. *If $v = (x_1{}^{e_1}, \dots, x_n{}^{e_n})$ and n is odd then $P(v) \approx P(v)^*$ implies that* $2e_1 \cdots e_n \equiv 0 \mod (n-1)!$

More details and other applications may be found in [16].

5 Proof via Suslin Matrices

We now give an alternative algebraic proof of Theorem 1.1 via Suslin matrices, when $\operatorname{rank} P > 2$ and even. Before proving the theorem we recall the Suslin matrices and some of their properties.

The Suslin Matrices $S_r(v,w)$. The construction of the Suslin matrices $S_r(v,w)$ is possible once we have two rows v, w of length $(r+1)$. It becomes more interesting if their dot product $\langle v, w \rangle = v \cdot w^t = 1$. (The rows are then automatically *unimodular* rows, i.e., the coordinates of each row generate the unit ideal.)

Andrei Suslin's inductive definition: Let $v = (a_0, a_1, \dots, a_r) = (a_0, v_1)$ with $v_1 = (a_1, \dots, a_r)$ and $w = (b_0, b_1, \dots, b_r) = (b_0, w_1)$ with $w_1 = (b_1, \dots, b_r)$. Set $S_0(v,w) = a_0$, and set

$$S_r(v,w) = \begin{pmatrix} a_0 I_{2^{r-1}} & S_{r-1}(v_1, w_1) \\ -S_{r-1}(w_1, v_1)^t & b_0 I_{2^{r-1}} \end{pmatrix}.$$

Suslin noted that

$$S_r(v,w)S_r(w,v)^t = (v\cdot w^t)I_{2^r} = S_r(w,v)^t S_r(v,w) \quad \text{and} \quad \det S_r(v,w) = (v\cdot w^t)^{2^{r-1}}$$

for $r \geq 1$. The Suslin matrices were introduced by Suslin in [11, Sect. 5] to show that a unimodular row of the form $(a_0, a_1, a_2^2, \ldots, a_r^r)$ can be completed to an invertible matrix of determinant one.

Nature of the Suslin Matrices. Suslin defines a sequence of forms $J_r \in M_{2^r}(R)$ by the recurrence formulae:

$$J_r = \begin{cases} 1 & \text{for } r = 0, \\ J_{r-1} \perp -J_{r-1}, & \text{for } r \text{ even, and} \\ J_{r-1} \top - J_{r-1}, & \text{for } r \text{ odd.} \end{cases}$$

(The English translation incorrectly says that $J_r = J_{r-1} \top J_{r-1}$ when r is odd.) Here $\alpha \perp \beta = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$, while $\alpha \top \beta = \left(\begin{smallmatrix} 0 & \alpha \\ \beta & 0 \end{smallmatrix}\right)$.

It is easy to see that $\det J_r = 1$ for all r, and that $J_r^t = J_r^{-1} = (-1)^{\frac{r(r+1)}{2}} J_r$. Moreover, J_r is antisymmetric if $r = 4k+1$ and $r = 4k+2$, whereas J_r is symmetric for $r = 4k$ and $r = 4k+3$. Suslin noted that the following formulae are valid:

$$\begin{array}{rrcl}
\text{for } r = 4k: & (S_r(v,w)J_r)^t &=& S_r(v,w)J_r \\
\text{for } r = 4k+1: & S_r(v,w)J_rS_r(v,w)^t &=& (v\cdot w^t)J_r \\
\text{for } r = 4k+2: & (S_r(v,w)J_r)^t &=& -S_r(v,w)J_r \\
\text{for } r = 4k+3: & S_r(v,w)J_rS_r(v,w)^t &=& (v\cdot w^t)J_r.
\end{array}$$

We next recall the theory of acyclic based complexes. A *based R-module* is a pair (R^n, e) where $e = (e_1, \ldots, e_n)$ is an ordered basis of R^n. A *based complex* is a bounded complex of based modules. The direct sum of two based modules (E,e) and (F,f) is defined as the based module $(E \oplus F, (e,f))$.

Given an acyclic based complex X, and a contraction s for X, the map $d+s\colon X_{\text{odd}} \to X_{\text{even}}$ is an isomorphism as $(d+s)^2 = 1 + s^2$ and s is nilpotent. We denote by $\text{wt}(X)$ the image of the matrix of $(d+s)$ in $\mathrm{K}_1(R)$. (This element is independent of the choice of s.)

Fossum, Foxby, and Iversen [5] applied the earlier theory of attaching an element of $\mathrm{K}_1(R)$ with an acyclic based complex to the Koszul complex with respect to a unimodular row as follows: Let $v = (a_1, \ldots, a_n)$ be a unimodular row. Consider the Koszul complex

$$X(v) : (\cdots\cdots \longrightarrow \wedge^k R^n \xrightarrow{d_v} \wedge^{k-1} R^n \longrightarrow \cdots\cdots)$$

If we order the basis $e_{i_1} \wedge \cdots \wedge e_{i_k}$ of $\wedge^k R^n$ lexicographically, then $X(v)$ is an acyclic based complex. (Note that if $\langle v, w \rangle = 1$ then external multiplication by w defines a contraction for $X(v)$.) Define

$$\text{wt}(v) = (-1)^{\binom{2n-2}{n}} \text{wt}(X(v)).$$

Then they showed that the map $v \mapsto \mathrm{wt}(v)$ is a Mennicke symbol. Moreover, they showed that $\mathrm{wt}(v\alpha) = \mathrm{wt}(v) + \sum_{i=0}^{n}(-1)^i[\wedge^i\alpha]$.

Suslin interprets this map and shows that $\mathrm{wt}(v) = [S_{n-1}(v,w)] \in \mathrm{SK}_1(R)$.

We next recall an important result of Suslin, Theorem 1.2 in [13]. Suslin showed that, $\mathrm{SK}_1(A_n(\mathbb{Z})) \simeq \mathbb{Z}$, with generator $[S_{n-1}((x_1,\dots,x_n),(y_1,\dots,y_n))]$.

We now reprove Theorem 1.1 using Suslin matrices and their properties outlined earlier. Let $R = A_{2n-1}(\mathbb{Z})$ and let $v = (x_1,\dots,x_{2n-1})$ be as earlier so $\mathrm{wt}(v)$ generates $\mathrm{SK}_1(R) = \mathbb{Z}$. Suppose that $v\sigma = w$, for some $\sigma \in \mathrm{GL}_{2n-1}(R)$, with $n > 2$. Then

$$\mathrm{wt}(w) = \mathrm{wt}(v\sigma) = wt(v) + \sum_{i=0}^{2n-1}(-1)^i[\wedge^i\sigma].$$

As $\mathrm{SK}_1(R) = \mathbb{Z}$, $[\sigma] = [S_{2n-2}(v,w)]^r$ for some r. Hence $[\wedge^i\sigma] = r[\wedge^i S_{2n-2}(v,w)]$. Therefore,

$$\begin{aligned}\sum_{i=0}^{2n-1}(-1)^i[\wedge^i\sigma] = r\sum_{i=0}^{2n-1}(-1)^i[\wedge^i S_{2n-2}(v,w)] &= r\,\mathrm{wt}(x_1,x_2,x_3^2,\dots,x_{2n-1}^{2n-2})\\ &= r(2n-2)!\,\mathrm{wt}(v).\end{aligned}$$

Thus,

$$\mathrm{wt}(w) = [S_{2n-2}(w,v)] = (1+r(2n-2)!)wt(v) = (1+r(2n-2)!)[S_{2n-2}(v,w)].$$

As v is of odd length, $[S_{2n-2}(w,v)] = [S_{2n-2}(w,v)^t]$, by the relations of Suslin. But $S_{2n-2}(v,w)S_{2n-2}(w,v)^t = I$, and so $[S_{2n-2}(v,w)] = [S_{2n-2}(w,v)]^{-1}$.

Thus, one gets $(2+r(2n-2)!)\,\mathrm{wt}(v) = 0$, a contradiction except when $n = 2$ and $r = -1$. $\square$

6 Proof via Riemann–Roch

The result of Corollary 4.3 was extended to all characteristics by Suslin and, independently, by Mohan Kumar and Nori. Suslin's proof from [12, 13] used the methods of Sect. 5. It is clear that it suffices to consider rings $A_n(k)$ defined over a field k for these results. We give here another proof of Theorem 1.1 valid in all characteristics using the method of Mohan Kumar and Nori. An expository account of this method is presented in [15, Sect. 17]. It is based on a result coming from Grothendieck's Riemann–Roch theorem. Let R be a smooth affine domain over a field k. Let $A^i(R)$ be the Chow group of algebraic cycles of codimension i on $\mathrm{Spec}\,R$ modulo rational equivalence. We write $[R/I]$ for the class of the cycle $\mathrm{Spec}\,R/I$. Filter $K_0(R)$ by letting $F^iK_0(R)$ be the subgroup generated by all $[R/I]$ with $\mathrm{ht}\,I \geq i$. Then $F^0K_0(R) = K_0(R)$, $F^1K_0(R) = \widetilde{K}_0(R)$, and $F^NK_0(R) = 0$ for $N \gg 0$. Define $\mathrm{gr}^i K_0(R) = F^iK_0(R)/F^{i+1}K_0(R)$. The map $\varphi : A^i(R) \to \mathrm{gr}^i K_0(R)$ sending $[R/I]$ to $[R/I]$ is well defined and is clearly onto. Grothendieck defines algebraic Chern classes and a map $\psi : \mathrm{gr}^i K_0(R) \to A^i(R)$ sending $[P]-[R^i]$ in $\mathrm{gr}^i K_0(R)$ to $c_i(P)$ in $A^i(R)$. The result we will need is the following.

Theorem 6.1. $\psi\varphi = (-1)^{i-1}(i-1)!$ *and* $\varphi\psi = (-1)^{i-1}(i-1)!$

Unfortunately, the sign was omitted in stating this theorem in [15]. The theorem was proved by Grothendieck [6, pp. 150–151] up to torsion (which is all we will need here) and by Jouanolou [2, footnote p. 675] in general.

Lemma 6.2. *Let R be a smooth affine domain over a field k. Suppose $A^i(R) = 0$ for all $i \neq 0,n$. Let J be an ideal of R of height n. If there is a finitely generated projective R-module P of rank n which maps onto J then $[R/J] \equiv 0 \mod (n-1)!$ in $K_0(R)$.*

Proof. As φ is onto, $\mathrm{gr}^i K_0(R) = 0$ for $i \neq 0,n$ so $F^i K_0(R) = \widetilde{K}_0(R)$ for $1 \leq i \leq n$ while $F^i K_0(R) = 0$ for $i > n$ and $\mathrm{gr}^n K_0(R) = \widetilde{K}_0(R)$. Let $\xi = [P] - [R^n]$ in $\widetilde{K}_0(R)$. Then $\psi(\xi) = c_n(P)$. By [6, page 153, Corollary], $c_n(P) = [R/J]$ so, in $\widetilde{K}_0(R)$, $[R/J] = \varphi([R/J]) = \varphi\psi(\xi)$ and the result follows from Theorem 6.1. □

In order to produce a module P as in Lemma 6.2, Mohan Kumar and Nori use the following patching argument. For $r \in R$ we denote by R_r the localisation ring $R[r^{-1}]$.

Lemma 6.3. *Let R be a commutative ring and let M be a finitely generated R-module. Let $R = Ra + Rb$ and let P and Q be finitely generated projectives of rank n over R_a and R_b, respectively. Suppose we have resolutions $0 \to L \to P \to M_a \to 0$ and $0 \to N \to Q \to M_b \to 0$ over R_a and R_b. If these sequences split after tensoring with R_{ab} and if $L_b \approx N_a$ over R_{ab} then there is a finitely generated projective R-module S of rank n with an epimorphism $S \twoheadrightarrow M$.*

Proof. We have $P_b \approx L_b \oplus M_{ab}$ and $Q_a \approx N_a \oplus M_{ab}$ so we get an isomorphism $P_b \approx Q_a$ compatible with the maps $P_b \longrightarrow M_{ab} \longleftarrow Q_a$. Let S be the pullback of $P \longrightarrow P_b \approx Q_a \longleftarrow Q$. This maps to the pullback M of $M_a \longrightarrow M_{ab} = M_{ab} \longleftarrow M_b$. As $S \to M$ is locally isomorphic to $P \to M_a$ and $Q \to M_b$ it is clear that it has the required properties. □

Still following Mohan Kumar and Nori we consider the ring

$$B = B_n = \frac{k[x_1,\dots,x_n,y_1,\dots,y_n,z]}{(\sum x_i y_i - z(1-z))}.$$

This is a smooth domain for $n \geq 1$. Let $I = (x_1,\dots,x_n,z)$.

Lemma 6.4. $\widetilde{K}_0(B_n) = \mathbb{Z}$, *generated by* $[B/I]$. *If $n > 0$ then $A^0(B_n) = \mathbb{Z}$ generated by $[B]$, $A^n(B_n) = \mathbb{Z}$ generated by $[B/I]$, and $A^i(B_n) = 0$ for all $i \neq 0,n$. For $n = 0$, $A^0(B_0) = \mathbb{Z} \oplus \mathbb{Z}$ and $A^i(B_0) = 0$ for all $i \neq 0$.*

Proof. Note that $B_{x_n} = k[x_1,\dots,x_n,y_1,\dots,y_{n-1},z][x_n^{-1}]$ and $B/(x_n) = B_{n-1}[y_n]$. Using the localization sequence and invariance under polynomial extensions, we get all the results easily except that $A^n(B_n)$ is only shown to be cyclic. As Theorem 6.1 implies that $\mathrm{rk}\, K_0 = \mathrm{rk}\, A^*$ it follows that $A^n(B_n) = \mathbb{Z}$. See [15] for details and references. □

Lemma 6.5. *Let $I' = (y_1,\dots,y_n,1-z)$. Then $[B/I'] = (-1)^{n+1}[B/I]$ in $K_0(B)$.*

Proof. Let α_i be the automorphism of B which switches x_i and y_i and let β be the automorphism of B which switches z and $1-z$, all generators not mentioned being fixed. Then $I' = \alpha_1\cdots\alpha_n\beta I$ so it will suffice to show that all α_i and β induce -1 on $\widetilde{K}_0(B)$. It is enough to do the case of α_1 and β. Let $C = B/(x_2,\dots,x_n) = B_1[y_2,\dots,y_n]$. The sequence $0 \to C \xrightarrow{x_1} C \to C/(x_1) \to 0$ shows that $[C/(x_1)] = 0$ but $C/(x_1) = B/I \oplus B/(\beta I)$ so β induces -1 on $\widetilde{K}_0(B)$. Similarly, $[C/(z)] = 0$ and we have $0 \to C/(z) \to B/I \oplus B/(\alpha_1 I) \to C/(x_1,y_1,z) \to 0$. Since $0 \to C/(x_1,z) \xrightarrow{y_1} C/(x_1,z) \to C/(x_1,y_1,z) \to 0$, we have $[C/(x_1,y_1,z)] = 0$ showing that $[B/(\alpha_1 I)] = -[B/I]$. ☐

We recall the result to be proved.

Theorem 6.6. *Let $A = A_n(k)$, where k is a nonzero commutative ring with unit, n is odd and $n > 3$. Then $P(x_1,\dots,x_n) \not\approx P(x_1,\dots,x_n)^*$.*

Proof. For the proof we can assume that k is a field. Recall that $P(x_1,\dots,x_n)^* \approx P(y_1,\dots,y_n)$ by [8, Prop. I.4.10]. Let $J = ((1-z)x_1,\dots,(1-z)x_n, zy_1,\dots,zy_n)$ in B. Then $J_z = (y_1,\dots,y_n)B_z$ and $J_{1-z} = (x_1,\dots,x_n)B_{1-z}$. We have exact sequences $0 \to L \to B^n_{1-z} \to J_{1-z} \to 0$ and $0 \to N \to B^n_z \to J_z \to 0$. These split over $B_{z(1-z)}$ as $J_{z(1-z)} = B_{z(1-z)}$ is projective. Now $L_z = P(x_1,\dots,x_n)$ over $B_{z(1-z)}$ and $N_{1-z} = P(y_1,\dots,y_n)$ over $B_{z(1-z)}$ so L_z and N_{1-z} are induced from $P(x_1,\dots,x_n)$ and $P(y_1,\dots,y_n)$ over A by the map $A \to B_{z(1-z)}$ sending x_i to x_i/z and y_i to $y_i/(1-z)$. If $P(x_1,\dots,x_n)$ is self dual it follows that $L_z \approx N_{1-z}$ so by Lemma 6.3, there is a finitely generated projective B-module Q which maps onto J. Therefore, Lemma 6.2 shows that $[B/J] \equiv 0 \mod (n-1)!$ in $K_0(B)$. Now $z(1-z) \in (x_1,\dots,x_n) \cap (y_1,\dots,y_n)$ so $z(1-z) = z^2(1-z) + z(1-z)^2$ lies in J. Therefore, $B/J = B/(J,z) \oplus B/(J,1-z) = B/I \oplus B/I'$. By Lemma 6.5, $[B/J] = (1+(-1)^{n+1})[B/I] \equiv 0 \mod (n-1)!$. As $[B/I]$ generates $\widetilde{K}_0(B) = \mathbb{Z}$, we get $2 \equiv 0 \mod (n-1)!$ for n odd which implies $n \le 3$. ☐

With a bit more effort a similar proof can be given for Corollary 4.5 over any nonzero commutative ring with unit, see [17]. This also contains an alternative approach which avoids the use of the Riemann–Roch theorem.

References

1. H. Bass, Modules which support nonsingular forms. J. Algebra **13** (1969), 246–252.
2. P. Berthelot, A. Grothendieck, L. Illusie, et al., Théorie des Intersections et Théorème de Riemann–Roch, SGA6, 1966/1967, Lecture notes in Math. **225**, Springer-Verlag, Berlin, 1971.
3. R. Bott, The space of loops on a Lie group, Mich. Math. J. **5** (1958), 35–61.
4. ———, The stable homotopy of the classical groups, Ann. Math. **70** (1959), 313–337.
5. R. Fossum, H. B. Foxby, and B. Iversen, A characteristic class in algebraic K-theory, Aarhus University Preprint No. **29**, 1978/79.

6. A. Grothendieck, La théorie des classes de Chern, Bull. Soc. Math. France **86** (1958), 137–154.
7. D. Husemoller, Fibre bundles, Third edition, Graduate Texts in Mathematics 20, Springer-Verlag, New York, 1994. ISBN: 0-387-94087-1.
8. T. Y. Lam, Serre's Problem on Projective Modules, Monographs in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, 2006.
9. M. Roitman, On stably extended projective modules over polynomial rings, Proc. Amer. Math. Soc. **97** (1986), 585–589.
10. N. Steenrod, The Topology of Fibre Bundles. Princeton Mathematical Series, vol. **14**. Princeton University Press, Princeton, N.J., 1951.
11. A. A. Suslin, Stably free modules. (Russian) Math. Sbornik (N.S.) **102** (144), No. 4, 537–550, 632, 1977; English translation in Math. USSR Sbornik Vol **31**, 479–491, 1977.
12. ———, Mennicke symbols and their applications in the K-theory of fields. Algebraic K-theory, Part I (Oberwolfach, 1980), pp. 334–356, Lecture Notes in Math. **966**, Springer, Berlin-New York, 1982.
13. ———, K-theory and K-cohomology of certain group varieties. Algebraic K-theory, 53–74, Adv. Soviet Math. **4**, American Mathematical Socity, Providence, RI, 1991.
14. R. G. Swan, Vector bundles and projective modules, Trans. Amer. Math. Soc. 105(1962), 264–277.
15. ———, Vector Bundles, Projective Modules and the K-theory of Spheres, 432–522, Ch. XVIII, Algebraic Topology and Algebraic K-theory, ed. W. Browder, Annals of Mathematics Studies **113**, Princeton University Press, Princeton, NJ, 1987.
16. ———, Some stably free modules which are not self dual. http://www.math.uchicago.edu/~swan/stablyfree.pdf
17. ———, On a theorem of Mohan Kumar and Nori, http://www.math.uchicago.edu/~swan/MKN.pdf
18. R. G. Swan, J. Towber, A class of projective modules which are nearly free, J. Algebra **36** (1975), 427–434.

Homotopy Invariance of the Sheaf W_{Nis} and of Its Cohomology

I. Panin

Summary A conjecture of F. Morel states that the motivic group $\pi_{0,0}(k)$ of a field k coincides with the Grothendieck-Witt group $GW(k)$ of quadratic forms over k provided that $char(k) \neq 2$. Morel's proof of the conjecture is based among others on the the following result: the Nisnevich sheaf W_{Nis} associated with the presheaf $X \mapsto W(X)$ is homotopy invariant and all its Nisnevich cohomology are homotopy invariant too. A rather short and self-contained proof of the result is given here.

1 Introduction

A conjecture of Morel states that the motivic group $\pi_{0,0}(k)$ of a field k coincides with the Grothendieck-Witt group $GW(k)$ of quadratic forms over k provided that $char(k) \neq 2$. Morel's proof of the conjecture presented in [M] is based, among other things, on the the following result: the Nisnevich sheaf W_{Nis} associated with the presheaf $X \mapsto W(X)$ is homotopy invariant and all its Nisnevich cohomology are homotopy invariant too. A rather short and self-contained proof of the result is given here. It is inspired by Voevodsky's paper [V] and may be regarded as an extended version of the author's preprint [P]. Other proofs are due to Hornbostel [H] and Fasel [F].

We consider a field of characteristic different from 2. For an affine k-scheme S we write $W(S)$ for the Witt group of quadratic spaces over the ring $k[S]$ of regular functions on S. We consider the big Nisnevich site Sm_{Nis} of k-smooth schemes and the Nisnevich sheaf W_{Nis} associated with the presheaf $X \mapsto W(S)$ on Sm_{Nis}. Furthermore, consider the big Zariski site Sm_{Zar} of k-smooth schemes and the Zariski

I. Panin
St. Petersburg Branch, V.A. Steklov Institute of Mathematics (POMI), Russian Academy of Sciences, 191023 St. Petersburg, Russia, e-mail: paniniv@gmail.com; panin@pdmi.ras.ru

2010 Mathematics subject classification. 18F20, 14F42.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_21,

sheaf W_{Zar} associated with the presheaf $X \mapsto W(S)$ on Sm_{Zar}. The main aim of the preprint is to prove the following result.

Main Theorem 1.1. *The Nisnevich sheaf* W_{Nis} *is strictly homotopy invariant. That is, for each k-smooth variety X one has*

(1) $W_{\mathrm{Nis}}(X) = W_{\mathrm{Nis}}(X \times \mathbf{A}^1)$ *and*
(2) $H^p_{\mathrm{Nis}}(X, W_{\mathrm{Nis}}) = H^p_{\mathrm{Nis}}(X \times \mathbf{A}^1, W_{\mathrm{Nis}})$ *for* $p > 0$.

Moreover

(3) $W_{\mathrm{Zar}} = W_{\mathrm{Nis}}$, *that is for any k-smooth X one has* $W_{\mathrm{Zar}}(X) = W_{\mathrm{Nis}}(X)$,
(4) $H^i_{\mathrm{Zar}}(X, W_{\mathrm{Zar}}) = H^i_{\mathrm{Nis}}(X, W_{\mathrm{Nis}})$ *for any* $i > 0$.

In particular, the sheaf W_{Zar} *is strictly homotopy invariant.*

The proof of the theorem is based on certain known results concerning Witt groups:

(1.2) For each field extension k'/k one has $W(k') = W(\mathbf{A}^1_{k'})$, see [K] or [OP 00].
(1.3) For a point $x \in X$ and the local scheme $U = \mathrm{Spec}(\mathscr{O}_{X,x})$ the Gersten-Witt complex

$$0 \to W(\mathscr{O}_{X,x}) \to W(k(X)) \xrightarrow{\mathrm{res}} \coprod_{y \in U^{(1)}} W(k(y)) \xrightarrow{\mathrm{res}} \coprod_{z \in U^{(2)}} W(k(z)) \xrightarrow{\mathrm{res}} \cdots$$

is exact by [B].
(1.4) For each field extension k'/k and each open $U \subset \mathbf{A}^1_{k'}$ there is an exact sequence of Witt groups (see [L, Thm. IX.3.1])

$$0 \to W(U) \to W(k'(t)) \xrightarrow{\sum \mathrm{res}_{\pi_x}} \coprod_{x \in U} W(k'(x)) \to 0.$$

We first provide a proof of the main theorem under the assumption that the ground field is perfect and infinite. This is done in Sects. 2 to 4. Eventually, in Sects. 5 and 6 we prove the main theorem for an arbitrary ground field. For that we use arguments based on the behavior of the Scharlau trace for odd-degree extensions of fields.

2 Voevodsky Trick

Suppose that the ground field k is perfect and infinite. Let $\mathscr{F}$ be a homotopy invariant Nisnevich sheaf on the big Nisnevich site Sm_{Nis}. Assume furthermore that for an integer $j > 0$ the functors $H^i_{\mathrm{Nis}}(-, \mathscr{F})$ are homotopy invariant for each $i < j$. Finally, assume that for each field extension k'/k one has $H^i_{\mathrm{Nis}}(\mathbf{A}^1_{k'}, \mathscr{F}_{\mathrm{Nis}}) = 0$ for $i > 0$. The following result is extracted from [V, Sect. 4.6].

Theorem 2.1 (Voevodsky trick). *Suppose for each essentially smooth local scheme U and each essentially smooth divisor D on U the map*

$$H^j_{\mathrm{Nis}}(U \times \mathbf{A}^1, \mathscr{F}) \to H^j_{\mathrm{Nis}}((U - D) \times \mathbf{A}^1, \mathscr{F})$$

is injective. Then for each (essentially) k-smooth X

$$\mathrm{Ker}\,[H^j_{\mathrm{Nis}}(X\times\mathbf{A}^1,\mathscr{F})\xrightarrow{i_0^*}H^j_{\mathrm{Nis}}(X,\mathscr{F})]=0.$$

The proof requires auxiliary results.

Lemma 2.2. *The Leray spectral sequence for the projection $p:X\times\mathbf{A}^1\to X$ gives rise to a short exact sequence*

$$\{0\}\to H^j_{\mathrm{Nis}}(X,R^0p_*(\mathscr{F}))\xrightarrow{\alpha}H^j_{\mathrm{Nis}}(X\times\mathbf{A}^1,\mathscr{F})\xrightarrow{\beta}H^0_{\mathrm{Nis}}(X,R^jp_*(\mathscr{F})).$$

Moreover, $R^0p_*(\mathscr{F})=\mathscr{F}$ and $\alpha=p^*$.

Set $\bar{H}^j_{\mathrm{Nis}}(X\times\mathbf{A}^1,\mathscr{F})=\mathrm{Ker}\,[H^j_{\mathrm{Nis}}(X\times\mathbf{A}^1,\mathscr{F})\xrightarrow{i_0^*}H^j_{\mathrm{Nis}}(X,\mathscr{F})]$.

Lemma 2.3. *The map $\beta|_{\bar{H}}:\bar{H}^j_{\mathrm{Nis}}(X\times\mathbf{A}^1,\mathscr{F})\to H^0_{\mathrm{Nis}}(X,R^jp_*(\mathscr{F}))$ is injective.*

This follows from Lemma 2.2.

Lemma 2.4. *Under the hypotheses of Theorem 2.1 for each essentially smooth closed $Z\subset X$ the map*

$$\bar{H}^j_{\mathrm{Nis}}(X\times\mathbf{A}^1,\mathscr{F})\to\bar{H}^j_{\mathrm{Nis}}((X-Z)\times\mathbf{A}^1,\mathscr{F})$$

is injective.

Proof. Consider the commutative diagram

$$\begin{array}{ccc}\bar{H}^j_{\mathrm{Nis}}(X\times\mathbf{A}^1,\mathscr{F}) & \xrightarrow{\beta} & H^0_{\mathrm{Nis}}(X,R^jp_*(\mathscr{F}))\\ \downarrow & & \downarrow\\ \bar{H}^j_{\mathrm{Nis}}((X-Z)\times\mathbf{A}^1,\mathscr{F}) & \xrightarrow{\beta} & H^0_{\mathrm{Nis}}(X-Z,R^jp_*(\mathscr{F})).\end{array}$$

The horizontal arrows are both injective by Lemma 2.3. For each $x\in X$ and $U=\mathrm{Spec}(\mathscr{O}_{X,x})$ there exists an essentially smooth divisor D in U containing $Z\cap U$. Moreover, the map $H^j_{\mathrm{Nis}}(U\times\mathbf{A}^1,\mathscr{F})\to H^j_{\mathrm{Nis}}((U-D)\times\mathbf{A}^1,\mathscr{F})$ is injective. Thus for the open inclusion $j:X-Z\hookrightarrow X$ the adjunction sheaf morphism $R^jp_*(\mathscr{F})\to j_*j^*R^jp_*(\mathscr{F})$ is injective. Taking the global sections we get the injectivity of the right-hand side vertical arrow in the last diagram. The lemma follows. □

Lemma 2.5. *Under the hypotheses of Theorem 2.1 for each closed $Z\subset X$ the map*

$$\bar{H}^j_{\mathrm{Nis}}(X\times\mathbf{A}^1,\mathscr{F})\to\bar{H}^j_{\mathrm{Nis}}((X-Z)\times\mathbf{A}^1,\mathscr{F})$$

is injective.

Proof. Take an element $a \in \bar{H}^j_{\mathrm{Nis}}(X \times \mathbf{A}^1, \mathscr{F})$ with $a|_{(X-Z)\times\mathbf{A}^1} = 0$ and consider the singular locus $\mathrm{Sing}(Z)$ of Z. It is a proper closed subset of Z because the field k is perfect. Applying Lemma 2.4 to the pair $(X^{(1)}, Z^{(1)}) := (X - \mathrm{Sing}(Z), Z - \mathrm{Sing}(Z))$ and the element $a^{(1)} = a|_{X^{(1)}}$ we conclude that $0 = a|_{X-\mathrm{Sing}(Z)} = a^{(1)}$. Replace Z by $\mathrm{Sing}(Z)$ and $\mathrm{Sing}(Z)$ by $\mathrm{Sing}(\mathrm{Sing}(Z))$. Since k is perfect $\mathrm{Sing}(\mathrm{Sing}(Z))$ is a proper closed subset of $\mathrm{Sing}(Z)$. Applying Lemma 2.4 to the pair

$$(X - \mathrm{Sing}(\mathrm{Sing}(Z)), \mathrm{Sing}(Z) - \mathrm{Sing}(\mathrm{Sing}(Z))$$

we conclude that $a|_{X-\mathrm{Sing}(\mathrm{Sing}(Z))} = 0$. Repeating the process several times we get $a = 0$. □

Proof (of Theorem 2.1). Let $a \in \bar{H}^j_{\mathrm{Nis}}(X \times \mathbf{A}^1, \mathscr{F})$. As $H^j_{\mathrm{Nis}}(\mathbf{A}^1_{k(X)}, \mathscr{F}) = 0$ there exists a closed Z in X such that a vanishes on $(X - Z) \times \mathbf{A}^1$. Lemma 2.5 completes the proof of the Theorem. □

3 Auxiliary Results

In this section we prove some auxiliary results.

Lemma 3.1. *For an essentially k-smooth scheme X one has*

$$W_{\mathrm{Zar}}(X) = \bigcap_{x \in X^{(1)}} W(\mathscr{O}_{X,x}) \subseteq W(k(X)),$$

where the intersection is taken over all codimension-one points x in X.

Proof. The proof is immediate from (1.3). □

Corollary 3.2. *For an essentially k-smooth variety X and an open imbedding $U \subset X$ the pull-back map*

$$W_{\mathrm{Zar}}(X) \hookrightarrow W_{\mathrm{Zar}}(U)$$

is injective.

Lemma 3.3. *For each field extension k'/k the restriction of the presheaf W to the affine line $\mathbf{A}^1_{k'}$ is already a Zariski sheaf and even a Nisnevich sheaf.*

Proof. For any open $U \subseteq \mathbf{A}^1_{k'}$ one has an exact sequence of Witt groups (see (1.4))

$$0 \to W(U) \to W(k'(t)) \xrightarrow{\sum \mathrm{res}_{\pi_x}} \coprod_{x \in U} W(k'(x)) \to 0.$$

This sequence and Lemma 3.1 shows that $W(U) = W_{\mathrm{Zar}}(U)$. By Lemma 4.1 $W_{\mathrm{Zar}}(U) = W_{\mathrm{Nis}}(U)$. The lemma follows. □

Corollary 3.4. *The following hold:*

(1) $W(\mathbf{A}^1_{k'}) = W_{\mathrm{Zar}}(\mathbf{A}^1_{k'}) = W_{\mathrm{Nis}}(\mathbf{A}^1_{k'})$.
(2) $H^i_{\mathrm{Zar}}(\mathbf{A}^1_{k'}, W_{\mathrm{Zar}}) = H^i_{\mathrm{Nis}}(\mathbf{A}^1_{k'}, W_{\mathrm{Nis}}) = 0$ *for all* $i > 0$.

Proof. The first assertion is clear. To prove the second one consider the sequence of Zariski sheaves on $\mathbf{A}^1_{k'}$

$$0 \to W_{\mathrm{Zar}} \to W(k'(t)) \xrightarrow{\sum \mathrm{res}_{\pi_x}} \coprod_{x \in U} i_{x,*} W(k'(x)) \to 0.$$

(The middle term here is considered as a constant sheaf.) The sequence is exact by property (1.4), so it can be considered as a flabby resolution of the sheaf W_{Zar} on $\mathbf{A}^1_{k'}$. As the sequence of global sections on $\mathbf{A}^1_{k'}$ is exact too, the Zariski cohomology $H^i_{\mathrm{Zar}}(\mathbf{A}^1_{k'}, W_{\mathrm{Zar}})$ vanishes for $i > 0$. The same arguments work for the Nisnevich sheaf W_{Nis}. □

4 Proof of the Main Theorem

Lemma 4.1. *The Zariski sheaf* W_{Zar} *coincides with the Nisnevich sheaf* W_{Nis}.

Proof. It suffices to prove that for an elementary Nisnevich square (see [MV, Prop. 3.1.4])

$$\begin{array}{ccc} \tilde{X} & \xleftarrow{\tilde{j}} & \tilde{U} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ X & \xleftarrow{j} & U \end{array}$$

the sequence

$$0 \to W_{\mathrm{Zar}}(X) \xrightarrow{p^* + j^*} W_{\mathrm{Zar}}(\tilde{X}) \oplus W_{\mathrm{Zar}}(U) \xrightarrow{q^* - \tilde{j}^*} W_{\mathrm{Zar}}(\tilde{U}) \qquad (1)$$

is exact. Recall that the square is elementary if it is Cartesian with an open inclusion j and an etale morphism p such that p induces an isomorphism of the reduced closed subschemes $\tilde{X} - \tilde{U}$ and $X - U$.

The maps j^* and $\tilde{j}^*$ are injective by Corollary 3.2. So to prove the exactness of the sequence (1) it suffices to check that for a pair $(\tilde{a}, b) \in W_{\mathrm{Zar}}(\tilde{X}) \oplus W_{\mathrm{Zar}}(U)$ with $\tilde{j}^*(\tilde{a}) = q^*(b)$ there exist an $a \in W_{\mathrm{Zar}}(X)$ such that $p^*(a) = \tilde{a}$ and $j^*(a) = b$.

Claim: The element $b \in W_{\mathrm{Zar}}(U) \subset W(k(X))$ *belongs to the subgroup* $W_{\mathrm{Zar}}(X)$. Given the claim, set $a = b \in W_{\mathrm{Zar}}(X)$. Since $\tilde{j}^*$ is injective this a is the required element.

It remains to check that the claim holds. To do that it suffices to check that for any codimension-one point $x \in X$ the element b belongs to $W(\mathcal{O}_{X,x})$ (see Lemma 3.1). This is the case if $x \in U$. So we may assume that $x \in Z \cap X$ and consider the cartesian square

$$\begin{tikzcd}
\mathrm{Spec}(\mathscr{O}_{\tilde{X},x}) \arrow[d, "p"'] & \mathrm{Spec}(k(\tilde{X})) \arrow[l, "\tilde{j}"'] \arrow[d, "q"] \\
\mathrm{Spec}(\mathscr{O}_{X,x}) & \mathrm{Spec}(k(X)) \arrow[l, "j"']
\end{tikzcd}$$

which is the pull back of the square earlier by means of the morphism $\mathrm{Spec}(\mathscr{O}_{X,x}) \to X$. The last square gives rise to a diagram of the Witt groups.

$$\begin{tikzcd}
0 \arrow[r] & W(\mathscr{O}_{\tilde{X},x}) \arrow[r, "\tilde{j}^*"] & W(k(\tilde{X})) \arrow[r, "\mathrm{res}_{\tilde{\pi}}"] & W(k(x)) \arrow[r] & 0 \\
0 \arrow[r] & W(\mathscr{O}_{X,x}) \arrow[r, "j^*"] \arrow[u, "p^*"] & W(k(X)) \arrow[r, "\mathrm{res}_{\pi}"] \arrow[u, "q^*"] & W(k(x)) \arrow[r] \arrow[u, "id"] & 0
\end{tikzcd}$$

The rows in the diagram are short exact sequences. The residue maps are defined by local parameters in the discrete valuation ring $\mathscr{O}_{X,x}$ and $\mathscr{O}_{\tilde{X},x}$. Choosing a local parameter $\pi \in \mathscr{O}_{X,x}$ we get a local parameter $\tilde{\pi} = p^*(\pi) \in \mathscr{O}_{\tilde{X},x}$. This choice of local parameters makes the last diagram commutative. Since $q^*(b) = \tilde{j}^*(\tilde{a})$ one has $\mathrm{res}_{\tilde{\pi}}(q^*(b)) = 0$. Thus $\mathrm{res}_{\pi}(b) = 0$ and b belongs to $W(\mathscr{O}_{X,x})$. The claim follows, whence the lemma. □

Lemma 4.2. *For a k-smooth scheme X and a closed subset $Z \subset X$ let $\mathscr{H}^i_Z(-,W_{\mathrm{Nis}})$ be the Nisnevich sheaf associated with the presheaf $U \mapsto H^i_{Z\cap U}(U,W_{\mathrm{Nis}})$. For each smooth principal divisor $i : D \hookrightarrow X$ one has:*

(1) The sheaves $\mathscr{H}^1_D(X,W_{\mathrm{Nis}})$ and $i_*(W_{\mathrm{Nis}})$ on X are isomorphic.
(2) $\mathscr{H}^i_D(X,W_{\mathrm{Nis}}) = 0$ for $i \neq 1$.

Proof. This proof is the most difficult one in this section. One can give a self-contained proof based on the trace method used in the proof of [OP 99, Thm. B]. However, now we give a proof by a reference to [BGPW, Proof of Thm. 4.4].

Let $GWC(X)$ and $GWC(X,D)$ be the Gersten-Witt complex of X and of X with the supports on D, respectively [BGPW, Def. 3.1]. A choice of the equation defining the divisor D identifies the Gersten-Witt complexes $GWC(X,D)$ and $GWC(D)[1]$ by [BGPW, Lemma 3.3]. Thus, $H^i(GWC(X,D)) = H^{i-1}(GWC(D))$ for all $i \geq 0$. The Gersten-Witt complex $GWC(X)$ (respectively $GWC(D)$) is the complex of the global sections of a flabby resolution of the Nisnevich sheaf W_{Nis} on X (respectively on D) [BGPW, Proof of Lemma 4.2]. Thus

$$H^i_D(X,W_{\mathrm{Nis}}) = H^i(GWC(X,D)) = H^{i-1}(GWC(D)) = H^{i-1}(D,W_{\mathrm{Nis}}).$$

Thus one has $H^i_D(X,W_{\mathrm{Nis}}) = H^{i-1}(D,W_{\mathrm{Nis}})$. In the case of essentially k-smooth local Henselian X and $i \neq 1$ the group $H^{i-1}(D,W_{\mathrm{Nis}})$ vanishes by [B, Theorem 4.2] (use property (1.3)). This proves the second assertion of the lemma. The first one follows from the functoriality of the isomorphisms $H^1_{D\cap U}(U,W_{\mathrm{Nis}}) = H^0(D\cap U,W_{\mathrm{Nis}}) = H^0(U,i_*W_{\mathrm{Nis}})$, where U runs over Zariski open subsets of X. □

Proof (of the main theorem in the case of a perfect and infinite ground field). The outline of our proof follows [V, Proof of Thm. 5.6 or better to say the arguments on pages 122–123]. We check first that the Nisnevich sheaf W_{Nis} is *homotopy invariant*. For a smooth X consider the diagram

$$\begin{array}{ccccc}
W_{\mathrm{Nis}}(X \times \mathbf{A}^1) & \xrightarrow{J^*} & W_{\mathrm{Nis}}(\mathbf{A}^1_{k(X)}) & \xleftarrow{\mathrm{can}} & W(\mathbf{A}^1_{k(X)}) \\
{\scriptstyle i^*_{0,X}}\downarrow & & {\scriptstyle i^*_{0,k(X)}}\downarrow & & \downarrow{\scriptstyle i^*_{0,k(X)}} \\
W_{\mathrm{Nis}}(X) & \xrightarrow{j^*} & W_{\mathrm{Nis}}(k(X)) & \xleftarrow{\mathrm{can}} & W(k(X))
\end{array}$$

with pull-back mappings J^* and j^*. The maps "can" are isomorphisms by Lemma 3.3. The right-hand side $i^*_{0,k(X)}$ is an isomorphism by (1.2). Thus, the middle arrow $i^*_{0,k(X)}$ is an isomorphism too. The map J^* is injective by Corollary 3.2. Thus, the map $i^*_{0,X}$ is injective too. Obviously $i^*_{0,X}$ is surjective. Thus, it is an isomorphism and $p^* : W_{\mathrm{Nis}}(X) \to W_{\mathrm{Nis}}(X \times \mathbf{A}^1)$ is an isomorphism too. The homotopy invariance follows.

We now prove the homotopy invariance of $H^1_{\mathrm{Nis}}(-, W_{\mathrm{Nis}})$. The Leray spectral sequence for the projection $p : X \times \mathbf{A}^1 \to X$ gives rise to a short exact sequence of groups

$$0 \to H^1_{\mathrm{Nis}}(X, R^0 p_*(W_{\mathrm{Nis}})) \xrightarrow{\alpha} H^1_{\mathrm{Nis}}(X \times \mathbf{A}^1, W_{\mathrm{Nis}}) \xrightarrow{\beta} H^0_{\mathrm{Nis}}(X, R^1 p_*(W_{\mathrm{Nis}})).$$

By the homotopy invariance of the sheaf W_{Nis} the group $H^1_{\mathrm{Nis}}(X, R^0 p_*(W_{\mathrm{Nis}}))$ coincides with $H^1_{\mathrm{Nis}}(X, W_{\mathrm{Nis}})$ and $\alpha = p^*$. To show that p^* is an isomorphism it suffices to check that the Nisnevich sheaf $R^1 p_*(W_{\mathrm{Nis}})$ vanishes. For that it remains to show that for a Henselian essentially smooth local scheme X one has $H^1_{\mathrm{Nis}}(X \times \mathbf{A}^1, W_{\mathrm{Nis}}) = 0$.

Since $H^1_{\mathrm{Nis}}(\mathbf{A}^1_{k(X)}, W_{\mathrm{Nis}}) = 0$ by Corollary 3.4, it suffices to check that the map

$$H^1_{\mathrm{Nis}}(X \times \mathbf{A}^1, W_{\mathrm{Nis}}) \to H^1_{\mathrm{Nis}}(\mathbf{A}^1_{k(X)}, W_{\mathrm{Nis}})$$

is injective. By the Voevodsky trick 2.1 it suffices to check that for a smooth divisor $i : D \hookrightarrow X$ the map

$$H^1_{\mathrm{Nis}}(X \times \mathbf{A}^1, W_{\mathrm{Nis}}) \to H^1_{\mathrm{Nis}}((X - D) \times \mathbf{A}^1, W_{\mathrm{Nis}})$$

is injective. For that it suffices to verify that the boundary map

$$H^0_{\mathrm{Nis}}((X - D) \times \mathbf{A}^1, W_{\mathrm{Nis}}) \xrightarrow{\partial_{\mathbf{A}^1}} H^1_{D \times \mathbf{A}^1}(X \times \mathbf{A}^1, W_{\mathrm{Nis}})$$

from the localization sequence is surjective. To prove this we need auxiliary lemmas.

Lemma 4.3. *For any essentially k-smooth scheme S and its closed subscheme Z the map*

$$\gamma : H^1_Z(S, W_{\mathrm{Nis}}) \to H^0(S, \mathscr{H}^1_Z(-, W_{\mathrm{Nis}}))$$

is an isomorphism, where $\mathscr{H}^1_Z(-,W_{\mathrm{Nis}})$ *is the Nisnevich sheaf associated with the presheaf* $U \mapsto H^1_{Z\cap U}(U,W_{\mathrm{Nis}})$.

Proof. In fact, the map γ fits in the exact sequence

$$0 \to H^1(S,\mathscr{H}^0_Z(W_{\mathrm{Nis}})) \to H^1_Z(S,W_{\mathrm{Nis}}) \xrightarrow{\gamma} H^0(S,\mathscr{H}^1_Z(W_{\mathrm{Nis}})) \to H^2(S,\mathscr{H}^0_Z(W_{\mathrm{Nis}}))$$

and the sheaf $\mathscr{H}^0_Z(W_{\mathrm{Nis}}) := \mathscr{H}^0_Z(-,W_{\mathrm{Nis}})$ vanishes by Corollary 3.2. □

Lemma 4.4. *The map* $p^* : H^0(X,\mathscr{H}^1_D(W_{\mathrm{Nis}})) \to H^0(X\times\mathbf{A}^1,\mathscr{H}^1_{D\times\mathbf{A}^1}(W_{\mathrm{Nis}}))$ *is an isomorphism.*

Proof. Let $i : D \hookrightarrow X$ be the closed imbedding. Lemma 4.2, the commutative diagram

$$\begin{tikzcd}
W_{\mathrm{Nis}}(D\times\mathbf{A}^1) \arrow[r, "\cong"] & H^0(X\times\mathbf{A}^1,(i\times id)_*W_{\mathrm{Nis}}) \arrow[r, "\cong"] & H^0(X\times\mathbf{A}^1,\mathscr{H}^1_{D\times\mathbf{A}^1}(W_{\mathrm{Nis}})) \\
W_{\mathrm{Nis}}(D) \arrow[u, "p^*"] \arrow[r, "\cong"] & H^0(X,i_*W_{\mathrm{Nis}}) \arrow[u, "p^*"] \arrow[r, "\cong"] & H^0(X,\mathscr{H}^1_D(W_{\mathrm{Nis}})), \arrow[u, "p^*"]
\end{tikzcd}$$

and the homotopy invariance of the sheaf W_{Nis} prove the lemma. □

Lemma 4.5. *For the Henselian local scheme* X *the boundary map* $\partial : W_{\mathrm{Nis}}(X-D) \xrightarrow{\partial} H^1_D(X,W_{\mathrm{Nis}})$ *is surjective.*

Proof. In fact, the next term in the localization sequence is $H^1_{\mathrm{Nis}}(X,W_{\mathrm{Nis}})$. It vanishes, because X is local for the Nisnevich topology. □

To complete the proof of the homotopy invariance of $H^1_{\mathrm{Nis}}(-,W_{\mathrm{Nis}})$ consider the commutative diagram

$$\begin{tikzcd}
W_{\mathrm{Nis}}((X-D)\times\mathbf{A}^1) \arrow[r, "\partial_{\mathbf{A}^1}"] & H^1_{D\times\mathbf{A}^1}(X\times\mathbf{A}^1,W_{\mathrm{Nis}}) \arrow[r, "\gamma_{\mathbf{A}^1}"] & H^0(X\times\mathbf{A}^1,\mathscr{H}^1_{D\times\mathbf{A}^1}(W_{\mathrm{Nis}})) \\
W_{\mathrm{Nis}}(X-D) \arrow[u, "p^*"] \arrow[r, "\partial"] & H^1_D(X,W_{\mathrm{Nis}}) \arrow[u, "p^*"] \arrow[r, "\gamma"] & H^0(X,\mathscr{H}^1_D(W_{\mathrm{Nis}})). \arrow[u, "p^*"]
\end{tikzcd}$$

The maps γ and $\gamma_{\mathbf{A}^1}$ are isomorphisms by Lemma 4.3. The right-hand side map p^* is an isomorphism by Lemma 4.4. Thus, the middle arrow p^* is an isomorphism too. As ∂ is a surjection the map $\partial_{\mathbf{A}^1}$ is surjective too. The homotopy invariance of $H^1_{\mathrm{Nis}}(-,W_{\mathrm{Nis}})$ is proved.

Now prove the homotopy invariance of $H^i_{\mathrm{Nis}}(-,W_{\mathrm{Nis}})$ for $i>1$. We proceed by induction on i. So assuming that the homotopy invariance holds for all $i<j$ prove it for $i=j$. The Leray spectral sequence for the projection p and the inductive hypothesis give the following short exact sequence

$$\{0\} \to H^j_{\mathrm{Nis}}(X,R^0p_*(W_{\mathrm{Nis}})) \xrightarrow{\alpha} H^j_{\mathrm{Nis}}(X\times\mathbf{A}^1,W_{\mathrm{Nis}}) \xrightarrow{\beta} H^0_{\mathrm{Nis}}(X,R^jp_*(W_{\mathrm{Nis}})).$$

By the homotopy invariance of the sheaf W_{Nis} the group $H^j_{\mathrm{Nis}}(X, R^0 p_*(W_{\mathrm{Nis}}))$ coincides with $H^j_{\mathrm{Nis}}(X, W_{\mathrm{Nis}})$ and $\alpha = p^*$. To show that p^* is an isomorphism it suffices to check that the Nisnevich sheaf $R^j p_*(W_{\mathrm{Nis}})$ vanishes. For that it remains to show that for a Henselian essentially smooth scheme X one has $H^j_{\mathrm{Nis}}(X \times \mathbf{A}^1, W_{\mathrm{Nis}}) = 0$.

As $H^j_{\mathrm{Nis}}(\mathbf{A}^1_{k(X)}, W_{\mathrm{Nis}}) = 0$ by Corollary 3.4, it suffices to check that the map

$$H^j_{\mathrm{Nis}}(X \times \mathbf{A}^1, W_{\mathrm{Nis}}) \to H^j_{\mathrm{Nis}}(\mathbf{A}^1_{k(X)}, W_{\mathrm{Nis}})$$

is injective. By the Voevodsky trick 2.1 it suffices to check that for an essentially smooth divisor $i : D \hookrightarrow X$ on an essentially smooth Henselian scheme X the map

$$H^j_{\mathrm{Nis}}(X \times \mathbf{A}^1, W_{\mathrm{Nis}}) \to H^j_{\mathrm{Nis}}((X - D) \times \mathbf{A}^1, W_{\mathrm{Nis}})$$

is injective. The localization sequence shows that it remains to check the vanishing of the group $H^j_{D\times\mathbf{A}^1}(X \times \mathbf{A}^1, W_{\mathrm{Nis}})$ in this case. The spectral sequence

$$E^2_{p,q} = H^p(X \times \mathbf{A}^1, \mathscr{H}^q_{D\times\mathbf{A}^1}(-, W_{\mathrm{Nis}})) \Rightarrow H^{p+q}_{D\times\mathbf{A}^1}(X \times \mathbf{A}^1, W_{\mathrm{Nis}})$$

shows that the group $H^j_{D\times\mathbf{A}^1}(X \times \mathbf{A}^1, W_{\mathrm{Nis}})$ vanishes if for all pairs (p,q) with $p + q = j$ the group $H^j_{D\times\mathbf{A}^1}(X \times \mathbf{A}^1, W_{\mathrm{Nis}})$ vanishes. The sheaves $\mathscr{H}^q_{D\times\mathbf{A}^1}(W_{\mathrm{Nis}})$ vanish for $q \neq 1$ by (4.2). The sheaf $\mathscr{H}^1_{D\times\mathbf{A}^1}(W_{\mathrm{Nis}}))$ is isomorphic by Lemma 4.2 to the sheaf $(i \times id)_* W_{\mathrm{Nis}}$ on $X \times \mathbf{A}^1$. Thus one has a chain of isomorphisms

$$H^{j-1}(X \times \mathbf{A}^1, \mathscr{H}^1_{D\times\mathbf{A}^1}(W_{\mathrm{Nis}})) \cong H^{j-1}(X \times \mathbf{A}^1, (i \times id)_* W_{\mathrm{Nis}}) = H^{j-1}(D \times \mathbf{A}^1, W_{\mathrm{Nis}}).$$

By the inductive hypothesis, $H^{j-1}(D \times \mathbf{A}^1, W_{\mathrm{Nis}}) = H^{j-1}(D, W_{\mathrm{Nis}})$ and the last group vanishes because D is local Henselian and $j - 1 > 0$. Thus for local essentially smooth Henselian X the group $H^j_{D\times\mathbf{A}^1}(X \times \mathbf{A}^1, W_{\mathrm{Nis}})$ vanishes. The inductive step is checked. The homotopy invariance is proved.

It remains to prove that for any $i \geq 0$ one has $H^i_{\mathrm{Zar}}(X, W_{\mathrm{Zar}}) = H^i_{\mathrm{Nis}}(X, W_{\mathrm{Nis}})$. Since $W_{\mathrm{Nis}} = W_{\mathrm{Zar}}$, this immediately follows from the remark on the flabby Gersten resolution earlier in the proof of Lemma 4.2. $\square$

5 The Case of an Imperfect Ground Field k

Assume k is imperfect. Let K/k be an algebraic extension with K perfect.

Lemma 5.1. *For any k-smooth variety X the map $H^i_{\mathrm{Nis}}(X, W_{\mathrm{Nis}}) \to H^i_{\mathrm{Nis}}(X_K, W_{\mathrm{Nis}})$ is injective.*

Assuming the lemma, we complete the proof of the strict homotopy invariance as follows. Consider the commutative diagram

$$\begin{array}{ccc} H^i_{\mathrm{Nis}}(X\times\mathbf{A}^1,W_{\mathrm{Nis}}) & \xrightarrow{\mathrm{Ex}} & H^i_{\mathrm{Nis}}((X\times\mathbf{A}^1)_K,W_{\mathrm{Nis}}) \\ {\scriptstyle i^*_{0,X}}\downarrow & & \downarrow{\scriptstyle i^*_{0,X_K}} \\ H^i_{\mathrm{Nis}}(X,W_{\mathrm{Nis}}) & \xrightarrow{\mathrm{ex}} & H^i_{\mathrm{Nis}}(X_K,W_{\mathrm{Nis}}), \end{array}$$

where the maps Ex and ex are induced by the scalar extension K/k. The map i^*_{0,X_K} is an isomorphism because the main theorem was proved in Sect. 3 for a perfect field. The map Ex is injective by the lemma. Thus $i^*_{0,X}$ is injective too. Clearly $i^*_{0,X}$ is surjective. Thus $i^*_{0,X}$ is an isomorphism and p^* is an isomorphism too. The strict homotopy invariance follows. It remains to prove the lemma.

Proof (of Lemma 5.1). We may replace the field extension K/k by a finite purely inseparable extension l/k and even by an extension with $l=k(a^{1/p})$ for some $a\in k$. For such an l, set $\alpha=a^{1/p}$ and consider the k-linear map tr: $l\to k$ given by $\alpha^i\mapsto 0$ for $i=0,1,\dots,p-2$ and $\alpha^{p-1}\mapsto 1$. For a k-smooth variety X set

$$\mathrm{Tr}_X=\mathrm{tr}\otimes id: l(X)=l\otimes_k k(X)\to k\otimes_k k(X)=k(X).$$

The map Tr induces [OP 99, Sect. 3] a group homomorphism $\mathrm{Tr}: W(l(X))\to W(k(X))$, which in turn induces a Nisnevich sheaf homomorphism $\mathrm{Tr}:\pi_*(W_{\mathrm{Nis}})\to W_{\mathrm{Nis}}$. A simple computation shows that it takes the class $[\langle 1\rangle_l]$ of the space $\langle 1\rangle_l$ to the class of the space $\langle 1\rangle$.

Let $\pi: X_l\to X$ be the morphism induced by $\mathrm{Spec}(l)\to\mathrm{Spec}(k)$. We claim that the sheaves $R^j\pi_*(W_{\mathrm{Nis}})$ vanish for $j>0$. In fact, the stalk of $R^j\pi_*(W_{\mathrm{Nis}})$ over a point $x\in X$ is the group $H^j_{\mathrm{Nis}}(X^h_x\otimes_k l,W_{\mathrm{Nis}})$, where X^h_x is the Henselization of the local scheme $\mathrm{Spec}(\mathcal{O}_{X,x})$ at its closed point. The scheme $X^h_x\otimes_k l$ is Henselian and semilocal. Thus, it is a disjoint union of local Henselian schemes. These are local for the Nisnevich topology, so their Nisnevich cohomology vanishes.

Since the sheaves $R^j\pi_*(W_{\mathrm{Nis}})$ vanish for $j>0$ the boundary effect

$$H^i_{\mathrm{Nis}}(X,R^0\pi_*(W_{\mathrm{Nis}}))\to H^i_{\mathrm{Nis}}(X_l,W_{\mathrm{Nis}})$$

in the Leray spectral sequence $H^i_{\mathrm{Nis}}(X,R^j\pi_*(W_{\mathrm{Nis}}))\Rightarrow H^{i+j}_{\mathrm{Nis}}(X_l,W_{\mathrm{Nis}})$ is an isomorphism. Composing the inverse isomorphism with the map induced by the trace map $\mathrm{Tr}:\pi_*(W_{\mathrm{Nis}})\to W_{\mathrm{Nis}}$ we get a map $\mathrm{Tr}: H^i_{\mathrm{Nis}}(X_l,W_{\mathrm{Nis}})\to H^i_{\mathrm{Nis}}(X,W_{\mathrm{Nis}})$.

By the projection formulae the composition

$$\mathrm{Tr}\circ\mathrm{ex}: H^i_{\mathrm{Nis}}(X,W_{\mathrm{Nis}})\to H^i_{\mathrm{Nis}}(X,W_{\mathrm{Nis}})$$

coincides with the multiplication by $\langle 1\rangle$. Thus it is the identity and the map $\mathrm{ex}: H^i_{\mathrm{Nis}}(X,W_{\mathrm{Nis}})\to H^i_{\mathrm{Nis}}(X_l,W_{\mathrm{Nis}})$ is injective. The lemma follows. $\square$

6 The Case of a Finite Ground Field k

Let $p > 0$ be the characteristic of the finite field k. Let l be an odd prime number different from p. Let K/k be an infinite Galois extension with Galois group equal to the l-adic integers $\mathbb{Z}_l$. The field K is perfect and infinite. Thus, the main theorem holds for varieties over K. Now applying literally arguments from Sect. 5 we get the main theorem in the case of smooth varieties over the field k. Whence the main theorem.

Acknowledgements The author is very grateful for the financial support to the Ellentuck Fund of the year 2004, to the RTN-Network HPRN-CT-2002-00287, to the grant "Research in the fundamental domains of the modern mathematics" and to the DFG-RFBR grant 09-01-91333-NNIO-a.

References

[B] *P. Balmer.* Witt cohomology, Mayer-Vietoris, homotopy invariance, and the Gersten conjecture, K-Theory, 23 (2001), 15–30.

[BGPW] *P. Balmer, S. Gille, I. Panin, Ch. Walter.* Witt cohomology, Mayer-Vietoris, homotopy invariance, and the Gersten conjecture, K-Theory, 23 (2001), 15–30.

[K] *M. Karoubi* Localisation de formes quadratiques.II, Ann. Sci. Éc. Norm. Sup. vol.8 (1975), 99–155.

[F] *J. Fasel.* Groupes de Chow-Witt, Mém. Soc. Math. Fr (N.S.) No.113 (2008), viii+197.

[H] *J. Hornbostel.* $\mathbf{A}^1$-representability of Hermitian K-theory and Witt groups, Topology 44 (2005), no.3, 661–687.

[L] *T.Y. Lam.* Introduction to quadratic forms over fields, Graduate Studies in Math., vol. 67, American Mathematical Society, Providence, RI, 2004.

[M] *F. Morel.* $\mathbf{A}^1$-algebraic topology over a field. www.math.uiuc.edu/K-theory/0806, 2006.

[MV] *F. Morel, V. Voevodsky.* $\mathbf{A}^1$-homotopy theory of schemes, Publ. IHES. 90 (2001), 45–143.

[OP 99] *M. Ojanguren, I. Panin.* A Purity Theorem for the Witt Group, Ann. Sci. Ecole Norm. Sup., Serie 4, 32 (1999), 71–86.

[OP 00] ———. The Witt group of Laurent polynomials. Enseign. Math. (2) 46 (2000), no. 3–4, 361–383.

[P] *I. Panin.* Homotopy invariance of the sheaf W_{Nis} and of its cohomology. www.math.uiuc.edu/K-theory/0715, 2004.

[V] *V. Voevodsky.* Cohomological theory of presheaves with transfers, In "Cycles, Transfers and Motivic Homology Theories", by Vladimir Voevodsky, Eric M. Friedlander, and Andrei Suslin. pp. 87–135.

Imbedding Quasi-split Groups in Isotropic Groups

M.S. Raghunathan

Summary Borel and Tits have shown that in any isotropic absolutely almost simple simply connected linear algebraic group G over a field k contains a k-split semisimple k-subgroup containing a maximal k-split torus T of G as well as arbitrarily chosen k-points in the root-groups (with respect to T) corresponding to the roots in a simple system of the reduced system of k-roots of G. In this paper we prove that one can in fact imbed somewhat larger quasi-split groups in isotropic groups when the characteristic of k is different from 2.

1 Introduction

Let k be a field of characteristic different from 2. Let G be an absolutely almost simple simply connected linear algebraic group defined over k. Let $\mathfrak{g}$ denote the Lie algebra of G. Let T be a maximal k-split torus in G and $\mathfrak{t}$ the Lie subalgebra of $\mathfrak{g}$ corresponding to T. Let $X^*(T)$ (respectively, $X_*(T)$) denote the character (respectively, co-character) group of T and $\Phi \subset X^*(T)$ denote the k-roots of G with respect to T: $\mathfrak{g}$ decomposes under the adjoint action of T into a direct sum of $\mathfrak{z}(T)$, the space of T-fixed vectors in $\mathfrak{g}$, and the eigenspaces of T corresponding to the (eigen-)characters in Φ. In the sequel we will call the k-roots simply roots (with respect to T). The (k-)root system Φ is irreducible as G is almost simple over an algebraic closure of k [4, 2.5]. For α in Φ, the root-space of α (= eigenspace for T corresponding to α) is denoted $\mathfrak{g}_\alpha$. The groups $X^*(T)$ and $X_*(T)$ are both isomorphic to $\mathbb{Z}^l$ and are canonically dual to each other; here $l = \dim T$ is by definition the k-rank of G . We denote by Φ^+ (respectively, Δ) the set of positive (respectively, simple roots) of G with respect to an ordering on $X^*(T)$. For α in Φ let U_α be the unique

M.S. Raghunathan
School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400 005, India, e-mail: msr@math.tifr.res.in

2010 Mathematics subject classification. 20G.

J.-L. Colliot-Thélène et al. (eds.), *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics 18, DOI 10.1007/978-1-4419-6211-9_22,

unipotent k-subgroup of G normalised by T; it has for its Lie algebra $\mathfrak{u}_\alpha$, the sum of all the root-spaces corresponding to the roots of the form $n.\alpha$, n a positive integer. It is known that for α in Φ, the only positive integral multiples of α that can be roots are α and 2α. A root α is *multipliable* if and only if 2α is a root. Note that if α is not multipliable, $\mathfrak{u}_\alpha = \mathfrak{g}_\alpha$ and the group U_α is abelian. The set Δ contains at most one multipliable root. With this notation we can formulate the main result of this note.

Theorem 1. *Let β be a root in Δ. Assume that it is multipliable if there is a multipliable root in Δ. For each α in Δ, let $u_\alpha \neq 1$, be an element of U_α. Let u'_β be any element of U_β if β is nonmultipliable; if β is multipliable, set $u'_\beta = u_\beta$. Let J be the set $\{u_\alpha \mid \alpha \in \Delta\}$. Then there is a finite extension K of k, an absolutely almost simple quasi-split linear algebraic group H over K and a k-morphism $F : H' = R_{K/k}(H) \to G$ with the following properties: there is a maximal k-split torus T' in H' such that F restricted to T' is an isogeny from T' to T and J as well as u'_β is contained in $F(H'(k))$.*

Remarks. Here $R_{K/k}$ is the Weil restriction of scalars functor from the category of K-varieties to the category of k-varieties. If $u'_\beta = u_\beta$ with β nonmultipliable or if u'_β is in $U_{2\beta}$, we recover a theorem of Borel-Tits [1, Theorem 7.2]; in this case moreover, $k = K$. However the proof in Borel-Tits for this special case is much more satisfactory: unlike the proof here it makes no use of the classification of semisimple groups over k (Tits [4]); nor is there a restriction on the characteristic. Actually, the proof given later for the classical groups works also in characteristic 2 for groups of type other than B_n, $n > 2$ and D_n, $n > 3$. The proof for the exceptional cases is reduced to that of classical groups, sometimes of the earlier two types. It seems likely that the result is true in the case of characteristic 2 as well but would need more delicate arguments. The special case of Theorem 1 when the k-rank of G is 1 is dealt with in Raghunathan [3, Appendix]. One expects that this theorem may be helpful in obtaining refined results about the classification of isotropic groups.

2 Classical Groups

2.1 Notation

We continue with the notation introduced earlier. Further L will denote a field containing k and for an algebraic k-group H, $H(L)$ will denote the L-points of H. An algebraic k-group is uniquely determined if its L-points are specified for every field L containing k. In the sequel we will often define a k-subgroup of G by simply describing its L-points for all L containing k. Also, characters on a k-torus will be defined by specifying their values on L-points of the torus.

If G is quasi-split, there is evidently nothing to prove. In the sequel we assume therefore that G is not quasi-split. We also assume (as we may) the following: if β is nonmultipliable, $u'_\beta \neq u_\beta$ and if 2β is a root, u'_β $(= u_\beta)$ is not contained in $U_{2\beta}$: the case $u'_\beta \in U_{2\beta}$ is covered by [1, Theorem 7.2].

2.2 Type ^1A_n

The assumption char$(k) \neq 2$ is not needed here. Every absolutely almost simple simply connected k-group G of (inner) type ^1A_n (n, a positive integer, is the rank of G over an algebraic closure of k) of k-rank l has the following description. There is a central division algebra D over k of degree d, a divisor of $n+1$ with $l+1 = (n+1)/d$, such that G is isomorphic over k to $SL_{l+1}(D)$. For a field L containing k, the group $G(L)$ is the Special Linear group $SL(l+1, D\otimes L)$ of $(l+1)\times(l+1)$-matrices with entries in $D\otimes L$ of (Dieudonné) determinant 1.

Let T be the torus in G for which the L-points $T(L)$ are the diagonal matrices in $G(L)$ with entries in L; it is a maximal k-split torus of G. The roots of G with respect to T are the characters $\alpha_{i,j}$, $1 \leq i \neq j \leq l+1$, defined as follows: for the diagonal matrix $\tilde{t}$ in $T(L)$ with diagonal entries $t_1, t_2, \ldots, t_l$ put $\alpha_{i,j}(\tilde{t}) = t_i t_j^{-1}$. A positive system is given by the collection $\{\alpha_{i,j} \mid i<j\}$ and the corresponding simple system $\Delta = \{\alpha_{i,i+1} \mid 1 \leq i \leq l\}$. For $i \neq j$, $1 \leq i,j \leq l+1$, the group $U_{\alpha_{i,j}}(L)$ is then precisely $\{1 + b.E_{i,j} \mid b \in D\otimes L\}$ where $E_{i,j}$ is the matrix whose (i,j)-th entry is 1 and all other entries are zero. The elements $u_\alpha, \alpha \in \Delta$, are thus of the form $1 + b_i.E_{i,i+1}$ with b_i in D, $1 \leq i \leq l$. For $1 \leq i \leq l$, set $t_i = b_i.b_{i+1}.b_{i+2}\ldots.b_{l+1}$. Let $\tilde{t}$ be the diagonal matrix whose i-th diagonal entry is t_i. Then if we replace the u_α by their conjugates under $\tilde{t}^{-1}$, we see that they are all in $SL(l+1,k)$. Let $\beta = \alpha_{i,i+1}$ and $u'_\beta = 1 + b.E_{i,i+1}$ with $b \in D$ (after the conjugation by $\tilde{b}^{-1}$).

Let K be the field generated by k and b. Then we take H to be the K-group $SL_{l+1,K}$ and we have an obvious morphism of $R_{K/k}(H)$ in G satisfying the required conditions. This proves the theorem for groups of inner type A_n.

2.3 Type $B_n, n \geq 2$

In this case, the assumption char$(k) \neq 2$ is used. The group G is the Spin Group of a nondegenerate quadratic form q of Witt-index l on a $(2n+1)$-dimensional k-vector space V. Let $B = B_q$ be the bilinear form associated to q: for v, w in V, $2.B(v,w) = q(v+w) - q(v) - q(w)$. Fix a basis $\{e_i \mid 1 \leq i \leq 2n+1\}$ of V such that the following hold:

1. For $1 \leq i,j \leq l$ and $2n+2-l \leq i,j \leq 2n+1$, $B(e_i, e_j) = 0$.
2. For $1 \leq i,j \leq l$, $B(e_i, e_{2n+2-j}) = \delta_{ij}$
3. For $1 \leq i \leq l$ or $2n+2-l \leq i \leq 2n+1$ and $l+1 \leq j \leq 2n+1-l$, $B(e_i, e_j) = 0$.

The basis enables us to identify $G'(L)$ (for G' the Special Orthogonal Group of q) as a subgroup of $GL(2n+1,L)$. Let $\pi : G \to G'$ be the natural map. We take for T the inverse image under π of the subgroup T' of G' for which $T'(L)$ consists of diagonal matrices $\tilde{t}$ (in $G'(L)$) with the i-th entry $t_i = 1$ if $l+1 \leq i \leq 2n+1-l$ and $t_{2n+2-i} = t_i^{-1}$ with $t_i \neq 0$ for $1 \leq i \leq l$. For $1 \leq i < l$, let α_i be the character on T' defined by setting $\alpha_i(\tilde{t}) = t_i/t_{i+1}$ for $\tilde{t}$ in $T(L)$. Also define α_l by $\alpha_l(\tilde{t}) = t_l$. By composing the α_i with π we get characters on T which also we denote by α_i. Then $\Delta = \{\alpha_i \mid 1 \leq i \leq l\}$ is a simple system for an order on $X(T)$. It is easily seen that Δ has no multipliable root.

For $1 \leq i < l$, one has $u_{\alpha_i}(e_j) = e_j$ if $j \neq i+1$ or $2n+2-i$ while $u_{\alpha_i}(e_{i+1}) = e_{i+1} + e_i.x_i$ and $u_{\alpha_i}(e_{2n+2-i}) = e_{2n+2-i} - e_{2n+1-i}.x_i$ with x_i in k. Next, $u_{\alpha_l}(e_j) = e_j$ for $1 \leq j \leq l$ and $2n+1-l < i \leq 2n$. Also, one has $u_{\alpha_l}(e_j) = e_j + e_l.y_j$ for $l+1 \leq j \leq 2n+1-l$ with y_j in k and $u_{\alpha_l}(e_{2n+2-l}) = e_{2n+2-l} + v + e_l.c$ with v in E and c in k. Changing the basis $\{e_i \mid l+1 \leq i \leq 2n+1-i\}$ of E, if necessary, we can assume that $v = e_{l+1}$. It follows then that $u_{\alpha_l}(e_{2n+2-l}) = e_{2n+2-l} + e_{l+1} + e_l.c$ and $y_j = 0$ for $l+2 \leq j \leq 2n+1-l$.

Now if β is one of the α_i with $i < l$ then (since U_{α_i} is 1-dimensional), the Special Orthogonal Group of the restriction of q to the k-linear span W of the $\{e_i \mid 1 \leq i \leq l\}$ and the $\{e_i \mid 2n+2-l \leq i \leq 2n+1\}$ is split and the corresponding Spin Group is the requisite quasi-split subgroup. If $\beta = \alpha_l$ and $u'_\beta(e_{2n+2-l}) = e_{2n+2-l} + w + e_l.c'$, let W be the k-linear span of $\{e_i \mid 1 \leq i \leq e_{l+1}\}$, w and $\{e_i \mid e_{2n+2-l} \leq i \leq 2n+1$. The Special Orthogonal Group of the quadratic form q restricted to W is then quasi-split and its Spin Group is the required H.

2.4 Groups of Type ^2A_n*,* C_n*, and* ^1D_n*,* ^2D_n*,* $n > 3$

Suppose now that G is a classical group but is not of inner type A_n or B_n. We assume that G is not quasi-split. (The proof later works also if char$(k) = 2$, provided that G is not of type D_n, $n > 3$.) One has, in these cases the following uniform description of G. There is an extension field k' of k of degree at most 2, a central division algebra D of degree d over k' with a k-linear involution σ (which is nontrivial if $D \neq k'$) whose restriction to k' is trivial or the Galois conjugation according as $k' = k$ or $[k' : k] = 2$, a right vector space V over D (of dimension N, say, where N is necessarily even when $k = k' = D$) and a nondegenerate σ-hermitian symmetric bilinear form h on V such that G is the simply connected cover of the Special Unitary Group $SU(h)$ of h. Further G is of k-rank l if and only if h has Witt-index l. Our conventions are such that $h : V \times V \to D$ satisfies the following conditions: h is biadditive and $h(v.x, w.y) = \sigma(x).h(v,w).y$ for v,w in V and x,y in D. Note that when $k = k' = D$, G is the spin group of a quadratic form in an even number N of variables. Also when G is of type C_n, $k = k'$ and we assume as we may that $D \neq k$: if $k = D$, the group is split which we have excluded.

Now V admits a basis $\{e_i \mid 1 \le i \le N\}$ (over D) such that the following conditions hold. Set $v_i = e_{l+i}$ for $1 \le i \le m$ where $m = N - 2l$ and for $1 \le i \le l$, $f_i = e_{N+1-i}$. We then have

1. $h(e_i, e_j) = h(f_i, f_j) = 0$ for $1 \le i, j \le l$.
2. $h(e_i, f_j) = \delta_{ij}$ for $1 \le i, j, \le l$.
3. $h(e_i, v_j) = h(f_i, v_j) = 0$ for $1 \le i \le l$ and $1 \le j \le m$.
4. $h(v_i, v_j) = 0$ for $1 \le i, j \le m$ with $i \ne j$.

Further, for any w in the D-linear span W of $\{v_i \mid 1 \le i \le m\}$, $h(w, w) \ne 0$.

In the sequel, elements of $SU(h)(L)$ will be regarded as matrices with entries in $D \otimes_k L$ with respect to this basis. We define a maximal k-split torus T' in $SU(h)$ as follows. An element of $T'(L)$ is a $(D \otimes L)$-linear automorphism $\tilde{b}$ of $V \otimes L$ for which we have $\tilde{b}(e_i) = e_i.b_i$ with b_i in L; further $b_i = 1$ for $l+1 \le i \le l+m$ and for $1 \le i \le l$, $b_{N+1-i} = \sigma(b_i)^{-1}$.

For $1 \le i < l$, let α_i denote the character on T' defined by setting $\alpha_i(\tilde{b}) = b_i/b_{i+1}$ for $\tilde{b}$ in $T(L)$. Let $\alpha_l(\tilde{b}) = b_l$ or b_l^2 according as $m > 0$ or $m = 0$. Let $\pi : G \to SU(h)$ be the natural projection and T the inverse image of T' in G under π. Then T is a maximal k-split torus in G. We treat characters on T' as characters on T by composing them with π. Then $\Delta = \{\alpha_i \mid 1 \le i \le l\}$ is a simple system of k-roots of G with respect to T for a suitable order on $X(T)$. We note that if $m > 0$, the root α_l is multipliable (and $2\alpha_l$ is a root). Also, if $m = 0$, no root in Δ is multipliable.

Suppose now that i is such that $1 \le i < l$ and $u_{\alpha_i} \ne 1$. Then one has $u_{\alpha_i}(e_j) = e_j$ for $j \ne i+1$ or $N - i + 1$ while $u_{\alpha_i}(e_{i+1}) = e_{i+1} + e_i.x_i$ for some $x_i \ne 0$ in D and $u_{\alpha_i}(e_{N-i+1}) = e_{N-i+1} - e_{N-i}.\sigma(x_i)$. Next, when $m = 0$ one has $u_{\alpha_l}(e_i) = e_i$ if $i \ne l+1$ and $u_{\alpha_l}(e_{l+1}) = e_{l+1} + e_l.x_l$ with $x_l \in D$. Also in this case no root is multipliable. If $m > 0$, $2\alpha_l$ is a root and we have $u_{\alpha_l}(e_i) = e_i$ unless $l+1 \le i \le l+m+1$ while $u_{\alpha_l}(e_{l+j}) = e_{l+j} + e_l.y_j$ for $1 \le j \le m$ and $u_{\alpha_l}(e_{l+m+1}) = e_{l+m+1} + w_0 + e_l.c$ with $y_j \in D$ and w_0 a vector in the D-linear span W of $\{e_i \mid l+1 \le i \le l+m\}$.

Assume now that $m = 0$ so that $N = 2l$. Let $\tilde{b}$ be the diagonal matrix in $U(h)$ whose i-th entry $b_i = 1.x_1.x_2.\ldots.x_{i-1}$ for $1 \le i \le l$ (and $b_{N+1-i} = \sigma(b_i)^{-1}$). Replacing the u_{α_i} by their conjugates under $\tilde{b}$ we see that we may assume that $x_i = 1$ for $1 \le i \le l-1$. We set $x_l = x$. Relative to the basis $\{e_i' = e_i.x \mid 1 \le i \le l\} \cup \{f_i \mid l+1 \le i \le N\}$, the elements u_{α_i} are seen to be in $GL(N,k)$. The element x is a symmetric or antisymmetric element in D and the assignment of $x^{-1}.\sigma(b).x$ to each b in D is again an involution $'\sigma$ and $'h(v,w) = x^{-1}.h(v,w)$, for v, w in V, is a hermitian or antihermitian form on V with respect to the involution $'\sigma$. If x is symmetric (respectively, antisymmetric) for σ, $'h$ is symmetric or antisymmetric (respectively, antisymmetric or symmetric) according as h is symmetric or antisymmetric.

Now G' is also the Special Unitary Group $SU('h)$. One now has $'h(e_i', e_j') = {'h}(f_i, f_j) = 0$, for $1 \le i, j \le l$ and $'h(e_i, f_j) = \delta_{ij}$. The form $'h$ is thus obtained as an extension of a split nondegenerate symmetric or antisymmetric bilinear form B (over k) on $W = k^N$, the k-span of $\{e_i' \mid 1 \le i \le l\}$ and $\{f_j \mid 1 \le j \le l\}$ (we have $N = 2l$, since $m = 0$) as a hermitian-symmetric or antisymmetric form to $V = D^N$. The elements u_{α_i} are now easily seen to be k-points in the quasi-split group over k that preserves B.

Let $\beta = \alpha_i$, $1 \le i \le l$. We assume, as we may, that $u_\beta \ne u_{\alpha_i}$. Then $u_\beta(e_j) = e_j$ for $j \ne i+1$ and $j \ne N-i$ while $u_\beta(e_{i+1}) = e_{i+1} + e_i.y$ and $u_\beta(e_{N-i}) = e_{N-i} - e_{N-i-1}.y$ with y a symmetric or antisymmetric element in D for $'\sigma$. Let L be the field generated by y over k. Then L is $'\sigma$ stable and we denote by K the fixed field of $'\sigma$ in L. Clearly $L = K$ or L is a quadratic extension of K. Let $'V$ be the L vector space spanned by the e'_i and the f_j, $1 \le i, j \le l$. Then $'h$ restricted to $'V$ $(= h^*$, say) is a nondegenerate hermitian symmetric or antisymmetric bilinear form if L/K is quadratic – this is the case if char$(k) \ne 2$ and y is antisymmetric. If $L = K$ (which is the case if char$(k) = 2$), $'h$ is a non-degenerate alternating form on $'V$ (denoted h^*). We can now take for H the Special Unitary or the Symplectic Group of h^* (over K).

We now take up the case $m > 0$. In this case, we have $u_{\alpha_l}(e_i) = e_i$ unless $l + 1 \le i \le l + m + 1$ while $u_{\alpha_l}(e_{l+j}) = e_{l+j} + e_l.y_j$ with y_j in D for $1 \le j \le m$ and $u_{\alpha_l}(e_{l+m+1}) = e_{l+m+1} + w_0 + e_l.c$ with c in D and w a vector in the D-linear span W of $\{e_i \mid l+1 \le i \le l+m\}$. We assume (as we may by changing the basis $\{v_i = e_{l+i} \mid 1 \le i \le m\}$ of W) that $v_1 = e_{l+1} = w_0$. Let $\lambda = h(e_{l+1}, e_{l+1})$. Define $'\sigma : D \to D$ by $'\sigma(x) = \lambda^{-1}.\sigma(x).\lambda$; then $'\sigma$ is again an involution of D. Consider now the form $'h : V \times V \to D$ defined by setting $'h(v, v') = h(v, v')$ for v, v' in V. Then $'h$ is a hermitian symmetric or antisymmetric form on V for the involution $'\sigma$ and G is also the Special Unitary group of this hermitian form. In the sequel we replace σ and h by $'\sigma$ and $'h$ and thus denote the latter by σ and h, respectively.

We now have $u_{\alpha_l}(e_{l+m+1}) = e_{l+m+1} + e_{l+1} + e_l.c$ and $u_{\alpha_l}(e_{l+1}) = e_{l+1} - e_l.y_l$. That u_{α_l} leaves h invariant implies that $y_l = -1$ and $c + \sigma(c) + 1 = 0$ or $c - \sigma(c) = 0$ according as h is symmetric or antisymmetric and char$(k) \ne 2$. Now let $\tilde{b}$ be the diagonal matrix in the Unitary Group $U(h)$ of H whose i-th diagonal entry is b_i where $b_i = 1$ for $l \le i \le l+m+1$ and for $1 \le i < l$, $b_i = x_i.x_{i+1}.x_{i+2}.\dots.x_{l-1}$. Replacing the u_{α_i} by their conjugates by $\tilde{b}^{-1}$, we see that we may assume that $x_i = 1$ for $1 \le i < l$ (while $y_l = -1$ and c remain unchanged). Note that since α_l is multipliable, $u'_\beta = u_{\alpha_l}$. Let L be the field generated by c over k and K the fixed field for σ in L (note that L is σ-stable). As $\sigma(c) \ne c$, L is a quadratic extension of K. Let W be the L-linear span of the $\{e_i \mid 1 \le i \le l+1\}$ and f the restriction of h to W (note that f takes values in L). We can take H to be the Special Unitary Group $SU(f)$ of the hermitian form f over L – this is a quasi-split group over K.

3 Exceptional Groups

3.1 Further Notation

We denote by M the anisotropic kernel of G (with respect to T). This is the k-subgroup $[Z(T), Z(T)].A$ where $Z(T)$ is the centraliser of T in G and A is the maximal anisotropic torus in the centre of $Z(T)$. If Δ' is a subset of Δ, by *the k-subgroup corresponding to Δ'*, we mean the subgroup generated by the $\{U_\alpha \mid \alpha \in \Delta'\}$ and the $\{U_\alpha \mid -\alpha \in \Delta\}$. It is a connected simply connected semisimple k-subgroup of

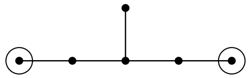
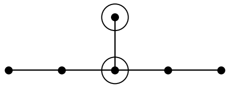
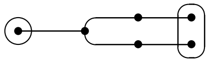
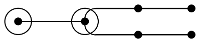
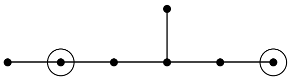
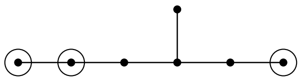
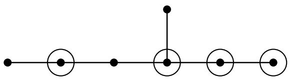
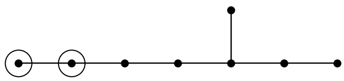
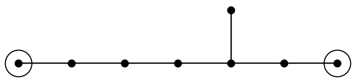
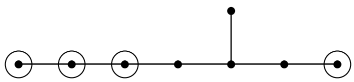
symbol	type Φ_k	Tits index
${}^1E_{6,2}^{28}$	A_2	
${}^1E_{6,2}^{16}$	G_2	
${}^2E_{6,2}^{16'}$	BC_2	
${}^2E_{6,2}^{16''}$	G_2	
$E_{7,2}^{31}$	BC_2	
$E_{7,3}^{28}$	C_3	
$E_{7,4}^{9}$	F_4	
$E_{8,2}^{78}$	G_2	
$E_{8,2}^{66}$	BC_2	
$E_{8,4}^{28}$	F_4	

Table 1 Tits indices for non-quasi-split exceptional simple groups of k-rank ≥ 2, together with the type of the relative root system.

G of k-rank the cardinality of Δ'. The intersection of T with this group has for its identity connected component a maximal k-split torus in the group. We will now establish the following result which yields our main theorem for exceptional groups by an obvious induction argument. The lemma itself will be proved by a case-by-case check using Tits' classification together with an induction on $\dim G$ and assuming the result for k-rank 1 groups: the case when the k-rank is 1 is dealt with in Raghunathan [3]. Table 1 lists the Tits indices for nonquasi-split exceptional groups of k-rank ≥ 2. The facts that are used in proving Lemma 2 for these exceptional groups can be read off easily from the Tits indices.

Lemma 2. *Assume that G is an exceptional group over k. Then either there is a semisimple element X in $\mathfrak{m}(k)$ where $\mathfrak{m}$ is the Lie algebra of M such that X is centralised by u_{α_i}, $1 \le i \le l$ and u'_β, but is not centralised by all of G or there is a k-torus S contained in the anisotropic kernel which centralises the u_{α_i}, $1 \le i \le l$ and u'_β. The centraliser of X (respectively, S) is reductive and is of strictly lower dimension than G.*

3.2

We now spell out the induction argument needed to deduce Theorem 1 for exceptional groups using Lemma 2. We assume that Theorem 1 holds for all exceptional groups of dimension $< \dim G$ over all fields. Let then G be exceptional. According to the lemma, the u_{α_i}, $1 \le i \le l$ and u'_β are all in the centraliser G' of X or S as the case may be. Let G_1 be the commutator subgroup of G'. Then G_1 is semisimple simply connected and of dimension strictly lower than that of G. Further G and G_1 have T as a common maximal k-split torus. Moreover, as the u_{α_i}, $1 \le i \le l$ and u'_β are contained in G_1 as well, it follows that G and G_1 have the same k-root system viz. Φ. As Φ is irreducible, the group G_1 is k-simple, i.e., it has no proper connected normal algebraic subgroup defined over k. It follows that G_1 is of the form $R_{K/k}(G'_1)$ where K/k is a finite separable extension of k and G'_1 is an absolutely almost simple group over K [4, 3.1.2]. Either G'_1 is classical or it is exceptional and $\dim_K(G'_1) < \dim_k(G)$; thus (in either case) there exists a finite separable extension L/K, a quasi-split group H''_1 over L, and a K-morphism $F : H'_1 = R_{L/K}(H'') \to G_1$ with a split torus mapping isomorphically onto a maximal split torus and with the u_{α_i}, $1 \le i \le l$ and u'_β in the image of F_1. We can now take for H the group $R_{K/k}(H'_1) = R_{L/k}(H'')$.

3.3 Type ${}^1E^{28}_{6,2}$

The k-rank of the group is 2. One reads off from the Tits index that both the simple roots are nonmultipliable. The centraliser $Z(T)$ of a maximal k-split torus T is of the form $T.M$ where the isotropic kernel M is a group of type D_4 – it can in fact be identified (assuming that G is simply connected) with the Spin Group $\mathrm{Spin}(q)$ of an anisotropic quadratic form q in eight variables over k; moreover the groups U_α for α in Δ are k vector spaces with the action of M on them being the two half-spin representations. Alternatively, one may think of one of them as the natural representation of $SO(q)$ and the other as one of the half-spin representations. We assume (as we may) that $\beta = \alpha_1$ and that the representation on U_β is the natural representation of $SO(q)$. If u_{α_1} and u'_β are not linearly independent we are in the special case dealt with in Borel-Tits [1]. We assume then that they are linearly independent. Let M'

denote the centraliser of u_{α_1} in M. Then one sees immediately that it can be identified with $\mathrm{Spin}(q')$ where q' is the restriction of q to the (codimension 1) k-subspace V of U_{α_1} which is the orthogonal complement of u_{α_1} in U_{α_1}. Now the representation of M' on U_{α_2} is the spin representation of this Spin Group $\mathrm{Spin}(q')$.

3.4

We now examine the spin representation of M' more closely. Fix a maximal torus S in M'. Then over an algebraic closure $\bar{k}$ of k, the representation space $W = U_{\alpha_2}$ decomposes into 1-dimensional eigenspaces for S. We fix a simple system of (absolute) roots (of M' with respect to S) $\{\theta_i \mid 1 \leq i \leq 3\}$ and let B_+ denote the Borel subgroup determined by this simple system. Let λ_+ denote the highest weight in W for this simple root-system and e a nonzero highest weight vector. Let X denote the orbit of e under M' and $f : M' \to X$ the orbit map. One checks easily that the map has rank 7 (everywhere) on M'. Now if v is any nonzero vector in $W(\bar{k})$, the set $\bar{k}^*.B_+(v)$ contains e in its closure. A semicontinuity argument now shows that the rank of the orbit map for any nonzero vector in $W(\bar{k})$ is greater than equal to 7.

Now there is a nondegenerate anisotropic quadratic form $'q$ (over k) on W which is invariant under M, hence under M'. Thus the orbit of v is contained in the set $\{w \in W \mid {}'q(w) = {}'q(v)\}$, a subvariety of codimension 1 (hence of dimension 7). It follows now that the isotropy subgroup H_v in M' for any $v \neq 0$ in $M'(k)$ is defined over k and has dimension 14. Moreover over $\bar{k}$ the isotropy groups at all points in $\Omega = \{w \in W \mid {}'q(w) \neq 0\}$ are all conjugates. One concludes from this that the group H_v is semisimple of type G_2; and setting $H = H_{u_{\alpha_2}}$, we see that H is an anisotropic group of type G_2 over k. Moreover, the representation of H on V is a k-form of the Weyl module corresponding to the unique irreducible representation of dimension 7 of the split G_2 in characteristic 0. This representation is irreducible except when $\mathrm{char}(k) = 2$. (When $\mathrm{char}(k) = 2$, the vector u_{α_1} is invariant under M' and hence under H and the representation on the quotient 6-dimensional space V' is irreducible.)

For a detailed analysis of the earlier facts, see for example [2].

3.5

Now we can analyse the orbits of H acting on V entirely analogously to what we did for the spin representation of M' to arrive at the following conclusion. The isotropy subgroup I of H at u'_β is defined over k and has dimension 8. As any maximal connected unipotent subgroup of H (over $\bar{k}$) has dimension 6, we see that I contains a nontrivial k-torus C. This group C evidently centralises the u_{α_i}, $i = 1, 2$ and u'_β. This settles the case of ${}^1E^{28}_{6,2}$.

3.6 Groups of Type ${}^1E_{6,2}^{16}$ and ${}^2E_{6,2}^{16''}$

In these cases too, the k-rank is 2 and both the simple k-roots α_1 and α_2 are nonmultipliable. The anisotropic kernel M commutes with one of the U_{α_i}, $i = 1,2$, say U_{α_1} which is of dimension 1. It follows that M is the anisotropic kernel of the k-rank 1 group G' corresponding to α_2. By the result for k-rank 1 groups, there is a nontrivial torus S in M or a semisimple element X in $\mathfrak{m}$ which is not central in G'. Hence the lemma in this case.

3.7 Groups of Type ${}^2E_{6,2}^{16'}$

The anisotropic kernel M is isomorphic to $U(h)$, the unitary group of an anisotropic hermitian form h in four variables over a quadratic extension k' of k. We take the simple root α_1 to be the multipliable root – this corresponds to the two roots in the Dynkin diagram that are encircled together. The group U_{α_1} is 2-step nilpotent. The representation of $M = U(h)$ on V $(= U_{\alpha_1}/U_{2\alpha_1})$ is the natural representation of $U(h)$ (on the 4-dimensional vector space over k'). The group $U_{2\alpha_1}$ is of dimension 1 and the representation of M on this vector space is trivial. The group $Z(T)$ is isomorphic over k to the almost direct product $(M \times T)/\mu_2$ where μ_2 is the group scheme $\mathrm{Spec}(k[t,t^{-1}]/(t^2-1))$ imbedded diagonally in $M \times T$. If u_{α_1} maps to zero in V, the result is the Borel-Tits theorem.

Assume then that u_{α_1} has a nonzero image v in V. The isotropy group M_0 at v for the action of $U(h) = M$ on V is the unitary group $U(h')$ of the restriction h' of h to a codimension 1 subspace V' (= orthogonal complement of v with respect to h) of the k'-vector space V. Further, the representation of M on U_{α_2} when restricted to M_0 is easily seen to be the natural 3-dimensional representation of $M_0 = U(h')$ over k'. The subgroup M_1 of M_0 which fixes u_{α_2} (assumed to be nontrivial) is then evidently k-isomorphic to $U(h'')$, h'' being the restriction of h' to a suitable codimension one (over k') k'-subspace V'' of V'.

Now let S be a maximal k-torus in $SU(h'')$; then u_{α_2} and T are in the centraliser G' of S. Moreover, if W is the inverse image of the 1-dimensional k-subspace spanned by v in U_{α_1} then W is S-stable and S acts trivially on $W/U_{2\alpha_1}$ and $U_{2\alpha_1}$. As S is a torus this means that it acts trivially on W. Thus, S centralises u_{α_i} for $i = 1,2$. Evidently S satisfies the requirement of the lemma.

3.8 Groups of Type $E_{7,2}^{31}$

We take α_1 to be the multipliable root; then α_2 is the circled root at the (short) end of the Dynkin diagram. The anisotropic kernel M is k-isomorphic to the product $\mathrm{Spin}(q) \times \mathrm{Spin}(q')$ where q (respectively, q') is an anisotropic quadratic form in eight (respectively, three) variables over k. The representation of M in U_{α_2} may be taken as the natural representation of the quotient $SO(q)$ of $\mathrm{Spin}(q)$ (treated as a representation of $\mathrm{Spin}(q)$) composed with the projection p_1 of M on $\mathrm{Spin}(q)$. That on V_{α_1} is the tensor product of $\sigma.p_1$ and $\tau.p_2$ where σ is a half-spin (respectively, spin) representation of $\mathrm{Spin}(q)$ (respectively, $\mathrm{Spin}(q')$) and p_2 is the projection of M on $\mathrm{Spin}(q')$).

This representation has another description: V_{α_1} has a natural structure of a right vector space of dimension 4 over a quaternion division algebra D with the factor $\mathrm{Spin}(q')$ acting as the group of reduced norm 1 elements in D and the factor $\mathrm{Spin}(q)$ acts (D-linearly) as the Special Unitary Group $SU(h)$ of of a nondegenerate anisotropic hermitian form h on V with respect to an involution of D with a fixed point set of dimension 3. The representation in $U_{2\alpha_1}$ is the trivial one-dimensional representation.

If u_{α_1} is in $U_{2\alpha_1}$ we are in the case treated by Borel-Tits. Assume then that the image v of $U_{2\alpha_1}$ in V_{α_1} is nonzero. Then the isotropy M_0 at v for the action of M on V_{α_1} is $SU(h')$ where h' is the restriction of h (respectively, q) to V', the orthogonal complement of v with respect to h in V. This anisotropic group $SU(h')$ of type $D_3 = A_3$ has an alternative description: it is the Special Unitary Group $SU(f)$ of an anisotropic nondegenerate hermitian form f on a four-dimensional vector space E over a quadratic extension k' of k; and in this description U_{α_2} is isomorphic as an M_0-module to E over k. In the sequel we set $E = U_{\alpha_2}$. The isotropy group M_1 at $u_{\alpha_2}(\in E)$ for this action of M_0 on E evidently contains $SU(f')$, the Special Unitary Group of the restriction f' of h to E', the (3-dimensional) orthogonal complement of u_{α_2}. Suppose now that S is a maximal k-torus in the k-group M_1; then the inverse image of the 1-dimensional k-subspace of V spanned by v is S-stable and S acts unipotently hence trivially on it. Thus, S is the torus with the desired properties.

3.9 Groups of Type $E^{28}_{7,3}$ and $E^{9}_{7,4}$

The k-rank of the groups of the first type is 3. In this case the anisotropic kernel M centralises one of the U_{α_i}, $1 \le i \le 3$ which we take to be α_1. We see that M is also the anisotropic kernel of the k-rank 2 subgroup H determined by α_2 and α_3; and since $\dim H < \dim G$, by the induction hypothesis there is a nontrivial k-torus S centralising u_{α_i} for $i = 2,3$. Thus, we have a torus centralising T as well as the three unipotent elements.

The groups of the second type have rank 4. The anisotropic kernel here centralises two of the U_{α_i}, say U_{α_1} and U_{α_2} which are both of dimension 1; thus M is also the anisotropic kernel of the k-rank 2 group H corresponding to the pair of roots α_3 and α_4. By the induction hypothesis there is a torus in M that centralises u_{α_i} for $i = 3,4$ and u'_{β}. Hence the result for groups of the second type as well.

3.10 Groups of Type $E_{8,2}^{78}$ and $E_{8,4}^{28}$

In both these cases there is a k-root α_1, say, such that U_{α_1} is of dimension 1 and commutes with the anisotropic kernel M. It follows that M is the anisotropic kernel of the k-group H corresponding to the subset $\{\alpha_i \mid i \neq 1\}$ as well. Further, $\beta = \alpha_i$ for some $i \neq 1$. As $\dim H < \dim G$, the induction hypothesis yields the desired result.

3.11 Groups of Type $E_{8,2}^{66}$

Here the k-rank is 2 and one of the roots, say α_1, is multipliable. The anisotropic kernel M is $\mathrm{Spin}(q)$, the Spin group of an anisotropic quadratic form q on a k-vector space of dimension 12 which may be taken to be $U_{\alpha_1}/U_{2\alpha_1}$, which we denote by V in the sequel. The subgroup of M that fixes u_{α_1} is the group $M' = \mathrm{Spin}(q')$ where q' is the restriction of q to a codimension 1 k-subspace V' of V. The representation of M' on U_{α_2} is then the spin representation of $\mathrm{Spin}(q')$. An analysis of the orbit structure of the action of $\mathrm{Spin}(q')$ in the spin representation shows that the orbit map for any orbit is a separable morphism and there are three kinds of orbits (over the algebraic closure of k): the trivial orbit of 0; the orbits for which the isotropy is the unique codimension-1 subgroup of a parabolic subgroup conjugate to the parabolic subgroup determined by the spin representation; and generic orbits for which the isotropy is the semisimple part of the Levi subgroup of a parabolic subgroup conjugate to the parabolic subgroup determined by the spin representation. Since M' is anisotropic over k, it follows that the isotropy H at u_{α_2} for the action of M' on U_{α_2} is defined over k and semisimple of type A_4 over an algebraic closure of k. Let S be a maximal k-torus in H. Let U' be the inverse image in U_{α_1} of the 1-dimensional k-subspace spanned by the image v of u_{α_1} in V under the natural map $U_{\alpha_1} \to V$. The group $U_{2\alpha}$ is of dimension 1 and (hence), M acts trivially on this group. It follows that S acts trivially on U'. Thus S centralises u_{α_i} for $i = 1, 2$.

Once again a more detailed analysis of the action of M on the U_{α_i} can be found in [2].

Acknowledgements My thanks are due to Skip Garibaldi who pointed out a gap in the proof in 3.3 in an earlier version.

References

1. A. Borel and J. Tits, Groupes réductifs. Publ. Math. IHES **27** (1965), 55–151.
2. J. Igusa, A classification of spinors up to dimension twelve. Am. J. Math., **92** (1970) 997–1028.
3. M.S. Raghunathan, On the congruence subgroup problem, II. Inv. Math. **85** (1986), 73–117.
4. J. Tits, Classification of semisimple algebraic groups. Algebraic groups and discontinuous groups, Proc. Symp. Pure Math. **9** (1966), 33–62.