Distribution Agreement

Signature:

______________________________ _______________

Reed Leon Gordon-Sarney Date

Zero-Cycles on Torsors under Linear Algebraic Groups

By

Reed Leon Gordon-Sarney

Doctor of Philosophy

Mathematics

Raman Parimala

Advisor

Suresh Venapally

Committee Member

David Zureick-Brown

Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.

Dean of the James T. Laney School of Graduate Studies

Date

Zero-Cycles on Torsors under Linear Algebraic Groups

By

Reed Leon Gordon-Sarney

B.A., Wesleyan University, 2012

M.Sc., Emory University, 2015

Advisor: Raman Parimala, Ph.D.

An abstract of

A dissertation submitted to the Faculty of the

James T. Laney School of Graduate Studies of Emory University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in Mathematics

2017

Abstract

Zero-Cycles on Torsors under Linear Algebraic Groups

By Reed Leon Gordon-Sarney

Let k be a field, let G be a smooth connected linear algebraic group over k, and let X be a G-torsor. Totaro asked: if X admits a zero-cycle of degree $d \geq 1$, does X have a closed étale point of degree dividing d? We give a positive answer in two cases:

1. G is an algebraic torus of rank ≤ 2 and $\mathrm{char}(k)$ is arbitrary, and

2. G is an absolutely simple adjoint group of type A_1 or A_{2n} and $\mathrm{char}(k) \neq 2$.

We also give the first known examples where Totaro's question has a negative answer. In particular, we exhibit failures via tori over number fields, p-adic fields, and complete discrete valuation fields k with global residue fields of $\mathrm{char}(\overline{k}) \neq 2$ and show that Totaro's question has a negative answer in general for tori of all ranks ≥ 3.

Zero-Cycles on Torsors under Linear Algebraic Groups

By

Reed Leon Gordon-Sarney

B.A., Wesleyan University, 2012

M.Sc., Emory University, 2015

Advisor: Raman Parimala, Ph.D.

A dissertation submitted to the Faculty of the

James T. Laney School of Graduate Studies of Emory University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in Mathematics

2017

Acknowledgments

This thesis is foremost a product of Parimala's warm mentorship, soft-spoken brilliance, and endless patience over the past five years, for which I am eternally grateful. I owe no fewer thanks to Suresh, whose remarkable kindness and ability to produce counterexamples in constant time have been vital to my graduate career. To my academic siblings–Nivedita, Wu, Bastian, and Sumit–you taught me half the mathematics I've learned at Emory and have my sincere appreciation.

To the village it took to raise me as a mathematician, I would be remiss to omit my profound gratitude: to DZB, for your abundance of advice, anecdotes, and empathy; to Jean-Louis, for your unwavering generosity and thoroughness; to David, for your insights, guidance, and confidence; to Danny, for giving me a roadmap of mathematical aspirations; and to Frederique, for agreeing to take on a curious student halfway across the world. You have my utmost thanks and admiration.

Of course, there's simply no way I'd be here without my friends who kept me going for five years. To Bill and Hayley, to SZB, to Ashley, Alex, and Alex, to Will, Daniel, Jordan, and David, to Brad and Mari, to Linus, to Blake, to Jon, and to Ariel, to everyone at Highwire, and to the staff of Falafel King: you're the best. If I somehow forgot to mention you, then you're certainly within your rights to think I think you're the second best. But you'd be mistaken. You're also the best.

To my mother, whose unconditional love and wholehearted support throughout my life has led me here; to my father, who showed me that *mathematician* was a thing I could be; and to Buffy, my muse and bane: thank you, and I love you.

Reed

Contents

Chapter 1

Introduction

Central simple algebras are the subject of some of the most elegant work in twentieth-century algebra and number theory. Consider the Schur index of a central simple algebra, defined to be the greatest common divisor among finite degrees of the algebra's splitting fields over the ground field; it is a result of Schur and Noether that it is also the *minimal* degree of such an extension, which we can further take to be separable. In view of the correspondence between central simple algebras and forms of projective space, the Schur index of a central simple algebra corresponds to the minimal positive degree of a zero-cycle on its Severi–Brauer variety. The stated result then says that this variety has a closed étale point of the same degree.

In general, one can define the index of a quasi-projective variety X over a field by

$$\mathrm{ind}(X) := \min\{\deg(Z) \geq 1 : Z \text{ is a zero-cycle on } X\}$$

and ask whether X admits a closed étale point of that degree. The answer, of course, is a resounding "no," and the literature is rich with striking examples in the index 1 case. Colliot-Thélène–Coray produced a conic bundle over $\mathbb{P}^1_{\mathbb{Q}_p}$, a rational surface, admitting a zero-cycle of degree 1 but having no rational points [CTC79]. Florence constructed affine homogeneous spaces under smooth connected linear algebraic groups over $\mathbb{C}((x))((y))$ and over local or global fields (with finite stabilizers in the latter case) with this same property [Flo04]. Parimala gave as an example a projective homogeneous space under a smooth connected linear algebraic group over $\mathbb{Q}_p((t))$ [Par05], settling a long-standing conjecture of Veĭsfeĭler in the negative [Veĭ69].

In the setting of torsors under linear algebraic groups, the index 1 variant of this question is due to Serre, dates back to the '60s, and is still open in general (cf. [Ser62, Question 5.3.(ii)], [Ser95, Question 2.4.2], [Ser, Appendix 2.4]).

Serre's Question. Let G be a smooth connected linear algebraic group over a field. If a G-torsor X has index 1, does X have a rational point?

In 2004, with the results on Severi–Brauer varieties–torsors under projective general linear groups–in mind, Totaro generalized Serre's question in another natural way: does every quasi-projective homogeneous space under a smooth connected linear algebraic group have a closed étale point of degree equal to its index [Tot04]? Florence's and Parimala's constructions were published shortly after Totaro's paper and sharpened Totaro's question to the torsor case, which remained open.

Totaro's Question. Let G be a smooth connected linear algebraic group over a field. Does every G-torsor have a closed étale point of degree equal to its index?

The research in this thesis was embarked upon under the belief that this question had a positive answer in general, and my graduate work concludes having constructed the first known counterexamples with Suresh. Contributing to a limited body of work attacking the question directly, including only the results of Totaro [Tot04], Garibaldi–Hoffman [GH06], and Black–Parimala [BP14], we answer Totaro's question affirmatively in two special cases and give two classes of examples where the question has a negative answer. Specifically, we prove the following results.

Theorem 1.0.1 ([GSb, Theorem 1.1], cf. Chapter 4)**.** *Let k be a field, and let T be a torus over k of rank ≤ 2. Then Totaro's question has an affirmative answer for T.*

Corollary 1.0.2 ([GSb, Corollary 1.2], cf. Chapter 4)**.** *Let X be a del Pezzo surface of degree 6. Then X has a closed étale point of degree equal to* $\operatorname{ind}(X)$*.*

Theorem 1.0.3 ([GSa, Theorem 1.1], cf. Chapter 5)**.** *Let k be a field of characteristic not equal to 2, and let G be an absolutely simple classical adjoint group over k of type A_1 or A_{2n}. Then Totaro's question has an affirmative answer for G.*

Theorem 1.0.4 (cf. Chapter 6)**.** *Let k be a p-adic field. Then there are smooth connected linear algebraic groups G over k such that every non-trivial G-torsor X has index p but has no closed points of degree p.*

Corollary 1.0.5 (cf. Chapter 6)**.** *For every $r \geq 8$, there is a semisimple linear algebraic group G (and a torus T) of rank r over $\mathbb{Q}$ such that every non-trivial G-torsor (and T-torsor) has index 2 but has no closed points of degree 2.*

Theorem 1.0.6 (cf. Chapter 6)**.** *Let k be a complete discrete valuation field whose residue field is a global field of characteristic not equal to 2. Then for every $r \geq 3$, there is a smooth connected linear algebraic group G of rank r over k such that every non-trivial G-torsor X has index 2 but has no closed points of degree 2.*

Corollary 1.0.7 (cf. Chapter 6)**.** *For every $r \geq 3$, there are semisimple linear algebraic groups G (and tori T) of rank r over $\mathbb{Q}(t)$ and $\mathbb{Q}_p(t)$ such that every non-trivial G-torsor (and T-torsor) has index 2 but has no closed points of degree 2.*

Chapter 2

Fundamental Objects

We start by introducing the central objects of study in this thesis. For the reader's benefit, only select essential results will be isolated and cited, and many non-trivial results will be stated in passing as black boxes. Each subsection will begin with comprehensive references where the omitted details and proofs can be found.

2.1. Central Simple Algebras

For a thorough exposition of the classical structure theory, refer to Chapters 12 and 13 of Pierce [Pie82]. For a more modern and expedited treatment, refer to Chapter 2 of Gille-Szamuely [GS06]. For an exhaustive resource on the theory with involutions in mind, begin with Chapter I of Knus–Merkurjev–Rost–Tignol [KMRT98].

2.1.1 The Brauer Group

Let k be a field. A finite-dimensional associative unital k-algebra is called **central** if its center is k and **simple** if it has no non-trivial two-sided ideals. A central simple algebra is called **division** if every non-zero element has a multiplicative inverse.

Theorem 2.1.1 (Wedderburn, [GS06, Theorem 2.1.3])**.** *Let A be a central simple algebra over k. Then $A \cong M_n(D)$ for a unique $n \geq 1$ and a unique (up to isomorphism) division algebra D over k.*

Two central simple algebras A and B over k are said to be **Brauer equivalent** if they identify the same division algebra. Brauer equivalence is an equivalence relation on the set of central simple algebras over k, and each equivalence class is determined by the unique division algebra it contains. The set of equivalence classes admits an abelian group structure with operation induced by taking tensor products, inversion induced by taking opposite algebras, and identity given by the equivalence class of k. This group is called the **Brauer group** of k and is denoted $\mathrm{Br}(k)$. Define the **period** of a central simple algebra A over k, denoted $\mathrm{per}(A)$, to be the order of $[A] \in \mathrm{Br}(k)$. It is immediate that the period is well-defined for elements of $\mathrm{Br}(k)$.

2.1.2 Splitting Fields

Fix a central simple algebra A over k, and let k^{s} denote a separable closure of k. There is a unique $d \geq 1$ such that $A \otimes_k k^{\mathrm{s}} \cong M_d(k^{\mathrm{s}})$, which means that there is some (non-unique) finite separable field extension L/k such that $A \otimes_k L \cong M_d(L)$. Any field extension E/k such that $A \otimes_k E \cong M_d(E)$ is called a **splitting field** of (and is said to **split**) A. The dimension of A over k is then a square, whose square root we call the **degree** of A and denote by $\deg(A)$. If $A \cong M_n(D)$ as in Wedderburn's Theorem, then $\deg(A) = n \deg(D)$, hence $\deg(D) \mid \deg(A)$. Define the **Schur index** of A, denoted $\mathrm{ind}_{\mathrm{Sch}}(A)$, to be $\deg(D)$. Since Brauer equivalence classes parametrize division algebras over k, the Schur index is well-defined for elements of $\mathrm{Br}(k)$.

A subfield of A that is maximal with respect to containment is called a **maximal subfield**. Every maximal subfield of A has degree over k equal to $\deg(A)$ and splits A. In fact, the splitting fields of A of finite degree over k are precisely the maximal subfields of central simple algebras that are Brauer equivalent to A. Since any central simple algebra that is Brauer equivalent to a split algebra is itself split, the notion of a splitting field is therefore well-defined for elements of $\mathrm{Br}(k)$. We can then define the **relative Brauer group** associated to any field extension L/k, denoted $\mathrm{Br}(L/k)$, to be the subgroup of $\mathrm{Br}(k) \cong \mathrm{Br}(k^{\mathrm{s}}/k)$ whose elements are split by L.

The following theorem gives three consequences of this rich structure theory.

Theorem 2.1.2 ([Pie82, Propositions 13.4, 13.5])**.** *Let* $[A] \in \mathrm{Br}(k)$*.*

1. $\mathrm{ind}_{\mathrm{Sch}}(A) = \gcd\{[L : k] : L/k \text{ is a finite field extension and } L \text{ splits } A\}$.
2. $\mathrm{ind}_{\mathrm{Sch}}(A) = \min\{[L : k] : L/k \text{ is a finite field extension and } L \text{ splits } A\}$.
3. $\mathrm{ind}_{\mathrm{Sch}}(A) = \min\{[L : k] : L/k \text{ is a finite separable field extension and } L \text{ splits } A\}$.

2.1.3 Involutions

Suppose now that k has characteristic $\neq 2$. Let K/k be an étale quadratic extension and A be a central simple algebra over K. An antiautomorphism σ on A is called an **involution** if $\sigma^2 = \mathrm{id}$; it is called an involution **of the first kind** if $[K : K^\sigma] = 1$ and **of the second kind** or **unitary** if $[K : K^\sigma] = 2$. If σ is unitary with fixed field $K^\sigma = k$, then for clarity, we call σ a K/k–**involution**, and we define the automorphisms of (A, σ) to be the K-automorphisms of A that commute with σ.

2.2. Linear Algebraic Groups

For an elegant overview of the classification of linear algebraic groups, begin with Chapter 3 of Bhaskhar's thesis [Bha16]. For a deep, functorial approach, refer to Chapter VI of Knus–Merkurjev–Rost–Tignol [KMRT98]. The geometrically-inclined reader who is interested in tori should consider Voskresenskiĭ [Vos98].

For us, a **variety** over k will be an integral separated scheme of finite type over

Spec(k). An **algebraic group** G over k is a variety over k where the maps

$$\begin{aligned} m : G \times_k G \to G &\quad \text{“multiplication”} \\ i : G \to G &\quad \text{“inversion”} \\ e : \mathrm{Spec}(k) \to G &\quad \text{“identity”} \end{aligned}$$

are morphisms over Spec(k). A **linear algebraic group** is an algebraic group that admits a Zariski-closed embedding into some $\mathrm{GL}_n : (\det(x_{ij})y - 1 = 0) \subseteq \mathbb{A}_{\mathbb{Z}}^{n^2+1}$ over k^{s}. Equivalently, linear algebraic groups are precisely the affine algebraic groups.

2.2.1 Algebraic Tori

For any étale algebra A over k, let $\mathbb{G}_{m,A}$ (or just $\mathbb{G}_m$ when the base is understood) be the abelian group scheme Spec $A[t, t^{-1}]$. A connected linear algebraic group T over k is called an **algebraic torus**, **k-torus**, or simply a **torus** if

$$T_{k^{\mathrm{s}}} := T \times_k k^{\mathrm{s}} \cong \mathbb{G}_{m,k^{\mathrm{s}}}^r$$

for some $r \geq 1$, which is called the **rank** of the torus. If E/k is a field extension such that $T_E \cong \mathbb{G}_{m,E}^r$, then E is called a **splitting field** of (and is said to **split**) T.

For any finite étale algebra A over k, let $R_{A/k}$ denote the **Weil restriction** functor (also called the **restriction of scalars** functor), which takes A-schemes to k-schemes and, in particular, takes A-tori to k-tori. Then for any finite separable field extension L/k and any L-torus T, $R_{L/k}T$ is a k-torus. A k-torus T is called **quasi-trivial** if it is isomorphic to a finite product of tori of the form $R_{L_i/k}\,\mathbb{G}_m$ where each L_i/k is a finite separable field extension. For any finite separable field extension L/k, call

$$R_{L/k}^{(1)}\,\mathbb{G}_m := \ker[R_{L/k}\,\mathbb{G}_m \xrightarrow{N_{L/k}} \mathbb{G}_m]$$

the **norm torus** associated to that extension; $R^{(1)}_{L/k}\,\mathbb{G}_m$ evidently has rank $[L:k]-1$.

2.2.2 Adjoint Groups of Type A_n

Let k be a field of characteristic $\neq 2$, let K/k be an étale quadratic extension, let A be a central simple algebra over K, and let σ be a K/k–involution on A. Then the automorphisms of (A,σ) are the K-automorphisms of A that commute with σ, and $\mathrm{Aut}(A,\sigma)$ is a linear algebraic group with k-points

$$\mathrm{Aut}(A,\sigma)(k) \cong \{\mathrm{Int}(a) \in \mathrm{Aut}_K(A) : a \in A^\times, \sigma(a)a \in k^\times\},$$

where $\mathrm{Int}(a) : A \to A$ is given by $\mathrm{Int}(a)(x) = axa^{-1}$. The elements $a \in A^\times$ such that $\sigma(a)a \in k^\times$, called the **similitudes** of (A,σ), form a group denoted $\mathrm{Sim}(A,\sigma)(k)$; it is clear that they only determine the automorphisms of (A,σ) up to scalars from $K^\times$. Viewed functorially, we have a short exact sequence of linear algebraic groups over k

$$1 \to R_{K/k}\,\mathbb{G}_m \to \mathrm{Sim}(A,\sigma) \xrightarrow{\mathrm{Int}} \mathrm{Aut}(A,\sigma) \to 1.$$

Adjoint groups appear as images of adjoint representations $\mathrm{Ad} : G \to \mathrm{Aut}(\mathrm{Lie}(G))$ where $\mathrm{Lie}(G)$ is the Lie algebra associated to a semisimple linear algebraic group G. The classification of **absolutely simple** (i.e., simple over a separable closure) linear algebraic groups separates **classical** groups from **exceptional** groups where absolutely simple classical groups are classified into types A_n, B_n, C_n, and D_n (trialitarian D_4 excluded). By work of Weil, classical adjoint groups can be interpreted in the language of algebras with involution; in particular, an absolutely simple classical adjoint group of type A_n over k is isomorphic to $\mathrm{Aut}(A,\sigma)$ for a central simple algebra A of degree $n+1$ over an étale quadratic extension K/k and σ a K/k-involution on A.

2.2.3 Torsors and Zero-Cycles

Let G be a linear algebraic group over k, and let k^{s} denote the separable closure of k. A non-empty variety X over k equipped with a right G-action is called a right G-**torsor** over k or a **principal homogeneous space** under G if the right $G(k^{\mathrm{s}})$-action on $X(k^{\mathrm{s}})$ is simply transitive. In other words, X is a right G-torsor if the morphism $X \times_k G \to X \times_k X$ given by $(x, g) \mapsto (x, xg)$ becomes an isomorphism over k^{s}. If $X \times_k G \cong X \times_k X$ as varieties over k, then X is said to be the trivial torsor. (The definition is similar for left G-torsors, and these two definitions coincide when G is abelian. From here on, every torsor will be a right torsor.) The following theorem is an easy exercise but a crucial fact in the study of torsors and rational points.

Theorem 2.2.1. *A G-torsor X over k is trivial if and only if $X(k) \neq \varnothing$.*

Now, let X be a scheme and $x \in X$ be a closed point. We define the **residue field** x, denoted $k(x)$, to be the quotient $\mathcal{O}_{X,x}/m_x$ of the local ring at x by its corresponding maximal ideal. Suppose further that X is a quasi-projective variety over a field k. Then $k(x)$ is a finite extension of k, whose degree we call the **degree** of x. (If $k(x)/k$ is a finite *separable* field extension, then we say that $x \in X$ is a closed **étale** point.) For any finite field extension L/k, $X(L) \neq \varnothing$ if and only if there is a morphism $\mathrm{Spec}(L) \to X$ over $\mathrm{Spec}(k)$ if and only if there is a closed point $x \in X$ whose residue field $k(x)$ is k-isomorphic to a subfield of L. So $X(k(x)) \neq \varnothing$.

Let $Z_0(X)$ denote the free abelian group on closed points of X, whose elements we call **zero-cycles** on X. The degree map on closed points of X extends linearly to a group homomorphism $\deg\colon Z_0(X) \to \mathbb{Z}$, and so we say that the **degree** of a zero-cycle $Z = \sum_{i=1}^{m} n_i x_i$ is $\deg(Z) = \sum_{i=1}^{m} n_i [k(x_i) : k]$. Define the **index** of X by

$$\mathrm{ind}(X) := \min\{\deg(Z) \geq 1 : Z \in Z_0(X)\}.$$

If $X(k) \neq \varnothing$, then $\mathrm{ind}(X) = 1$. But the converse need not hold.

Chapter 3

Galois Cohomology

Galois cohomology is a toolkit to probe the arithmetic behavior of objects over fields. The standard text is Serre [Ser], but it is dense for a first treatment. For a gentler introduction, refer to Chapter 3 of Gille–Szamuely [GS06]. Explicit computations in the Brauer group setting can be found in Chapter 14 of Pierce [Pie82].

3.1. Finite Group Cohomology

Let G be a finite group. If an abelian group M has a (left) G-action, then we say that M is a (left) G-**module**. Equivalently, M is a G-module if it is a module over the group ring $\mathbb{Z}[G]$. If the G-action on M is trivial, then we say that M is a trivial G-module. We say that a G-module P is a **projective** G-module if for any surjection of G-modules $A \to B$, the map $\mathrm{Hom}_G(P, A) \to \mathrm{Hom}_G(P, B)$ induced by composition are onto. A **projective resolution** of a G-module M is an infinite exact sequence

$$\cdots \xrightarrow{p_3} P_2 \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} M \xrightarrow{p_{-1}} 0$$

where each P_i is a projective G-module.

Now, fix a G-module M and a projective resolution of the trivial G-module $\mathbb{Z}$

$$\cdots \xrightarrow{p_3} P_2 \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} \mathbb{Z} \xrightarrow{p_{-1}} 0.$$

Since $\mathrm{Hom}_G(-, M)$ is a contravariant left exact functor from the category of G-modules to the category of sets, we have an induced left exact sequence

$$\mathrm{Hom}_G(P_0, M) \xrightarrow{d_1} \mathrm{Hom}_G(P_1, M) \xrightarrow{d_2} \mathrm{Hom}_G(P_2, M) \xrightarrow{d_3} \cdots$$

For each $i \geq 1$, define $H^i(G, M) := \ker(d_{i+1})/\mathrm{im}(d_i)$ and $H^0(G, M) := \mathrm{Hom}_G(\mathbb{Z}, M)$. Maps in $\mathrm{Hom}_G(P_i, M)$, $\ker(d_{i+1})$, and $\mathrm{im}(d_i)$ are called i-**cochains**, i-**cocycles**, and i-**coboundaries**, respectively. It turns out that these $H^i(G, M)$ do not depend on the choice of projective resolution, and so they are well-defined *abelian groups* associated to the G-module M that we call **cohomology groups** (with coefficients in M).

Theorem 3.1.1 ([GS06, Proposition 3.1.9])**.**

(a) If M is a G-module, then $H^0(G, M) \cong M^G$.

(b) For any G-module homomorphism $A \to B$, there is a canonical group homomorphism $H^i(G, A) \to H^i(G, B)$ for each $i \geq 0$.

(c) Given a short exact sequence of G-modules

$$0 \to A \to B \to C \to 0,$$

there is a canonical long exact sequence of abelian groups

$$\cdots \to H^i(G, A) \to H^i(G, B) \to H^i(G, C) \xrightarrow{\delta} H^{i+1}(G, A) \to \cdots$$

beginning with $i = 0$.

If M is not a G-module but a non-abelian group with G-action, then techniques similar to those above may be used only to construct $H^0(G, M) \cong M^G$ and $H^1(G, M)$. These will be pointed sets rather than abelian groups–called **cohomology sets**–which means that exactness as in Theorem 3.1.1.(c) should be reinterpreted in terms of the point. Nevertheless, one can still obtain an exact sequence of cohomology sets. If we have a short exact sequence of (not all abelian) groups with G-action

$$1 \to A \to B \to C \to 1,$$

then the exact sequence of pointed sets is

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C).$$

If A is a G-module and central in B, then the sequence extends to $H^2(G, A)$.

3.2. Profinite Group Cohomology

Let k be a field, and let $\Gamma = \mathrm{Gal}(k^{\mathrm{s}}/k)$ be the **absolute Galois group** of k. Our ultimate goal is understand Γ-modules (or sets) $G(k^{\mathrm{s}})$ for some linear algebraic groups G by constructing cohomology groups (or sets) $H^i(\Gamma, G(k^{\mathrm{s}}))$. We can exploit that Γ is “assembled from” finite groups to define cohomology as in the previous section.

An **inverse system** of sets consists of a partially ordered set I such that for every $i, j \in I$, there is an $l \in I$ such that $i \le l$ and $j \le l$, a collection of sets G_i indexed by I, and a collection of maps $\rho_{ij} : G_j \to G_i$ for each $i \le j$ such that each ρ_{ii} is the identity and $\rho_{ij} \circ \rho_{jl} = \rho_{il}$ whenever $i \le j \le l$. For example, let I be the index set for the collection of finite Galois extensions L_i/k, let $i \le j$ if and only if $L_i \le L_j$, let $G_i = \mathrm{Gal}(L_i/k)$, and for each $i \le j$, let $\rho_{ij} = \mathrm{res}_{L_j/L_i} : \mathrm{Gal}(L_j/k) \to \mathrm{Gal}(L_i/k)$. It is clear that this data defines an inverse system. Define its **inverse limit** by

$$\varprojlim_n \operatorname{Gal}(L_n/k) := \{(g_i) \in \prod_i \operatorname{Gal}(L_i/k) : \rho_{ij}(g_j) = g_i \text{ whenever } i \leq j\}.$$

Not only is it clear that $\Gamma \cong \varprojlim_n \operatorname{Gal}(L_n/k)$, but this construction suggests a topology on Γ: give each $\operatorname{Gal}(L_n/k)$ the discrete topology, give $\prod_n \operatorname{Gal}(L_n/k)$ the product topology, and then give $\Gamma \hookrightarrow \prod_n \operatorname{Gal}(L_n/k)$ the subspace topology. In general, inverse limits of finite groups equipped with a topology in this way are called **profinite groups** with the **profinite topology**. The open subgroups of Γ are precisely the closed subgroups of finite index, which correspond to finite field extensions of k.

Now, let M be a Γ-module (or set) with the discrete topology. We say that Γ acts **continuously** on M if the stabilizer of each $m \in M$ is open in Γ. If Γ acts continuously on M, then our cohomology construction in terms of *continuous* cocycles and coboundaries is compatible with the inverse limit in the sense that

$$H^i(\Gamma, M) \cong H^i(\varprojlim_n \operatorname{Gal}(L_n/k), M) := \varinjlim_n H^i(\operatorname{Gal}(L_n/k), M^{\operatorname{Gal}(L_n/k)})$$

where the right-hand side is a **direct limit** of the **directed system** of cohomology groups (or sets) $H^i(\operatorname{Gal}(L_n/k), M^{\operatorname{Gal}(L_n/k)})$, whose constructions are similar (but "opposite") to those in the inverse setting. If our Γ-module is $G(k^{\mathrm{s}})$ for some abelian linear algebraic group G over k–or if we are considering the Γ-action on the non-abelian group $G(k^{\mathrm{s}})$ if G is not abelian–we define $H^i(k, G) := H^i(\Gamma, G(k^{\mathrm{s}}))$ to be the ith **Galois cohomology group** (or **Galois cohomology set**) associated to G.

Theorem 3.2.1.

(a) If G is a linear algebraic group over k, then $H^0(k, G) \cong G(k^{\mathrm{s}})^\Gamma = G(k)$.

(b) For any homomorphism $A \to B$ of abelian linear algebraic groups over k, there is a canonical group homomorphism $H^i(k, A) \to H^i(k, B)$ for each $i \geq 0$.

(c) Given a short exact sequence of abelian linear algebraic groups over k

$$0 \to A \to B \to C \to 0,$$

there is a canonical long exact sequence of groups

$$\cdots \to H^i(k, A) \to H^i(k, B) \to H^i(k, C) \xrightarrow{\delta} H^{i+1}(k, A) \to \cdots$$

beginning with $i = 0$.

The same caveats as before apply when G–hence $G(k^s)$–is not abelian.

3.3. Some Important Maps

Given a homomorphism $f : H \to G$ of finite groups, any G-module M can be made into an H-module via the action $h \cdot m = f(h)m$. This procedure takes projective G-modules to projective H-modules and thus induces maps on cohomology $f_i^*\colon H^i(G, M) \to H^i(H, M)$ for each $i \geq 0$. If f is simply the inclusion map of a subgroup $H \leq G$, then we call the associated maps on cohomology **restriction** maps. As before, we can construct restriction maps in the non-abelian case by viewing G-sets as H-sets. The notion of restriction extends to profinite group cohomology.

Proposition 3.3.1 ([GS06, Construction 4.2.8])**.** *Let L/k be a finite field extension, and let G be a linear algebraic group over k. Then for each $i \geq 0$ where cohomology is defined, there is a restriction map induced by the inclusion of absolute Galois groups*

$$\text{res}\colon H^i(k, G) \to H^i(L, G_L).$$

This is a group homomorphism if G is abelian and a map of pointed sets otherwise.

In the abelian case, if $H \leq G$ has finite index, then there is a procedure to take projective H-modules to projective G-modules, yielding **corestriction** maps $g_i^*\colon H^i(H,M) \to H^i(G,M)$. This notion also extends to the profinite setting.

Proposition 3.3.2 ([GS06, Construction 4.2.8]). *Let L/k be a finite field extension, and let G be an abelian linear algebraic group over k. Then for each $i \geq 0$, there is a corestriction homomorphism*

$$\mathrm{cor}\colon H^i(L, G_L) \to H^i(k, G).$$

With this same notation in force, we note that for any G-torsor X over k, $\mathrm{res}([X]) = [X_L]$, but the corestriction is very much not an inverse of the restriction.

Proposition 3.3.3 ([GS06, Proposition 4.2.10]). *Let L/k be a finite field extension of degree n, and let G be an abelian linear algebraic group over k. Then for each $i \geq 0$, the composition*

$$\mathrm{cor} \circ \mathrm{res}\colon H^i(k,G) \to H^i(k,G)$$

is the multiplication-by-n map.

3.4. Some Important Computations

The following theorem in Galois cohomology underpins the work in this thesis.

Theorem 3.4.1 ([Ser, Proposition I.5.33]). *Let G be a linear algebraic group over k. Then there is a bijection between the set of classes of G-torsors over k and the pointed set $H^1(k,G)$ that identifies the class of the trivial torsor with the point in $H^1(k,G)$.*

Recall Theorem 2.2.1: a G-torsor X over k is trivial if and only if $X(k) \neq \varnothing$. These theorems tell us that proving the existence or lack thereof of rational points on torsors under linear algebraic groups, a task that appears to fall squarely under the umbrella of geometry, amounts to demonstrating the triviality or non-triviality of a Galois cohomology class, which is more amenable to algebraic techniques.

Nevertheless, understanding $H^1(k, G)$ via Theorem 3.2.1 ultimately requires some prior understanding of other "related" Galois cohomology groups and sets. In this section, we mention a number of results that will help us in this vein. To begin, we will often cite a fundamental result of Hilbert, commonly referred to as Hilbert Theorem 90 or just Hilbert 90, of which we give two useful interpretations.

Theorem 3.4.2 ([CF67, Section V.2.7])**.**

(a) If L/k is a finite cyclic extension such that $\mathrm{Gal}(L/k) \cong \langle\sigma\rangle$ and $a \in L^\times$ such that $N_{L/k}(a) = 1$, then there is some $b \in L^\times$ such that $a = \sigma(b)b^{-1}$.

(b) $H^1(k, \mathbb{G}_m) = 0$.

Recalling that $\mathbb{G}_m = \mathrm{GL}_1(k)$, the cohomological Hilbert 90 can be generalized.

Theorem 3.4.3 ([GS06, Lemma 2.7.4])**.** *If $[A] \in \mathrm{Br}(k)$, then $H^1(k, \mathrm{GL}_1(A)) = 1$.*

An easy consequence of Hilbert 90 is the following basic result of Kummer theory.

Theorem 3.4.4 ([GS06, Proposition 4.3.6])**.** *If $\mathrm{char}(k) \nmid n$, then $H^1(k, \mu_n) \cong k^\times/(k^\times)^n$.*

Furthermore, we will also repeatedly identify isomorphism classes of central simple algebras and elements of the Brauer group with special Galois cohomology classes.

Theorem 3.4.5 ([GS06, Theorem 2.4.3])**.** *There is a bijection between the set of isomorphism classes of central simple algebras of degree n over k and the pointed set $H^1(k, \mathrm{PGL}_n)$ that identifies $[M_n(k)]$ with the point in $H^1(k, \mathrm{PGL}_n)$.*

Theorem 3.4.6 ([GS06, Theorem 4.4.7])**.** *If L/k is a Galois extension, then $\mathrm{Br}(L/k) \cong H^2(\mathrm{Gal}(L/k), \mathbb{G}_m)$. In particular, if $L = k^{\mathrm{s}}$, then $\mathrm{Br}(k) \cong H^2(k, \mathbb{G}_m)$.*

Finally, we cite an essential property of the Weil restriction functor.

Theorem 3.4.7 ([Ser, Section I.5.b])**.** *If L/k is a finite field extension and G is a linear algebraic group over L, then $H^1(k, R_{L/k}(G)) \cong H^1(L, G)$.*

3.5. Totaro's Question, Revisited

Let G be a smooth connected linear algebraic group over a field k, and let X be a G-torsor over k. As in Section 2.2.3, each closed point $x \in X$ identifies a finite field extension L/k such that $X(L) \neq \varnothing$, in which case X_L identifies the trivial torsor in $H^1(L, G_L)$ by Theorem 3.4.1. This last condition can be restated as

$$[X] \in \ker[H^1(k,G) \xrightarrow{\text{res}} H^1(L, G_L)],$$

and so any $Z \in Z_0(X)$ yields some finite field extensions $L_1, \ldots, L_m/k$ such that

$$[X] \in \ker[H^1(k,G) \xrightarrow{\prod_{i=1}^m \text{res}} \prod_{i=1}^m H^1(L_i, G_{L_i})].$$

We can now reformulate Totaro's question in the language of Galois cohomology.

Totaro's Question. Let G be a smooth connected linear algebraic group over a field k, and let $[X] \in H^1(k, G)$. If $L_1, \ldots, L_m/k$ are finite field extensions with $\gcd\{[L_i : k]\} = \mathrm{ind}(X)$ such that

$$[X] \in \ker[H^1(k,G) \xrightarrow{\prod_{i=1}^m \text{res}} \prod_{i=1}^m H^1(L_i, G_{L_i})],$$

then is there a separable field extension F/k with $[F : k] = \mathrm{ind}(X)$ such that

$$[X] \in \ker[H^1(k,G) \xrightarrow{res} H^1(F, G_F)]?$$

Chapter 4

Totaro's Question for Tori of Low Rank

This chapter is largely excerpted from the author's paper of the same name to appear in *Transactions of the American Mathematical Society* [GSb].

Theorem 4.0.1. *Let k be a field, and let T be a torus over k of rank ≤ 2. Then Totaro's question has an affirmative answer for T.*

We remark that the theorem is true even if the ground field is not perfect. Define the **separable index** of a variety X over a field, denoted $\mathrm{ind}_{\mathrm{s}}(X)$, to be the minimal positive degree of a zero-cycle of closed étale points on X. The question of equality between $\mathrm{ind}(X)$ and $\mathrm{ind}_{\mathrm{s}}(X)$ was raised by Lang–Tate and answered affirmatively by recent work of Gabber–Liu–Lorenzini when X is a generically smooth and non-empty scheme of finite type over a field [GLL13, Theorem 9.2]. Since torsors under tori over fields satisfy these hypotheses, we only need to consider *separable* field extensions in the proof of Theorem 4.0.1.

Now, if X is regular over a field and $U \subseteq X$ is open and dense, then $\mathrm{ind}(X) = \mathrm{ind}(U)$ by a general moving lemma for zero-cycles. So the index is a birational invariant among regular varieties over a given field. Together with Theorem 4.0.1, we obtain from this a result on points of toric varieties (cf. Section 4.4).

Corollary 4.0.2. *Let X be a regular variety over a field containing a principal homogeneous space of a smooth torus of rank ≤ 2 as a dense open subset. If X admits a zero-cycle of degree $d \geq 1$, then X has a closed étale point of degree dividing d.*

In particular, Manin proved that del Pezzo surfaces of degree 6 are toric varieties as in Corollary 4.0.2 [Man72]. So the following is a special case of the corollary.

Corollary 4.0.3. *Let X be a del Pezzo surface of degree 6. If X admits a zero-cycle of degree $d \geq 1$, then X has a closed étale point of degree dividing d.*

4.1. Lemmata

In order to prove Theorem 4.0.1, a number of key lemmas will be cited repeatedly.

Lemma 4.1.1. *Serre's question has a positive answer for abelian algebraic groups.*

Proof. Let G be an abelian algebraic group defined over a field k. By Proposition 3.3.3, the composition of the natural restriction and corestriction maps associated to any finite field extension L/k is the multiplication-by-$[L:k]$ map. Now, fix $[X] \in H^1(k, G)$, whose order as a group element we call the **period** of X and denote by $\mathrm{per}(X)$. If $[X_L] = 0 \in H^1(L, G_L)$ for some finite field extension L/k, then

$$[L:k][X] = (\mathrm{cor} \circ \mathrm{res})([X]) = \mathrm{cor}(0) = 0 \in H^1(k, G),$$

and so $\mathrm{per}(X) \mid [L:k]$. Since L is arbitrary, $\mathrm{per}(X) \mid \mathrm{ind}(X)$. If $\mathrm{ind}(X) = 1$, then $\mathrm{per}(X) = 1$, meaning that $[X] = 0 \in H^1(k, G)$. So $X(k) \neq \varnothing$. □

Lemma 4.1.2. *Let L/k be a finite separable field extension and $T = R^{(1)}_{L/k}\, \mathbb{G}_m$.*

(a) $H^1(k, T) \cong k^\times / N_{L/k}(L^\times)$.

(b) *If L/k is cyclic, then* $H^1(k,T) \cong \mathrm{Br}(L/k)$.

(c) $H^1(L,T_L) = 0$. *In particular,* $\mathrm{ind}(X) \mid [L:k]$ *for all* $[X] \in H^1(k,T)$.

Proof. From the short exact sequence of k-tori

$$0 \to R^{(1)}_{L/k}\,\mathbb{G}_m \to R_{L/k}\,\mathbb{G}_m \xrightarrow{N_{L/k}} \mathbb{G}_m \to 0,$$

Theorems 3.2.1.(c), 3.4.2, and 3.4.7 yield the exact sequence of abelian groups

$$L^\times \xrightarrow{N_{L/k}} k^\times \to H^1(k,T) \to 0,$$

yielding (a). Now, for any finite cyclic field extension L/k with $\mathrm{Gal}(L/k) \cong \langle\sigma\rangle$, we have a canonical isomorphism (see [GS06, Corollary 4.4.10])

$$k^\times/N_{L/k}(L^\times) \cong \mathrm{Br}(L/k)$$

given by

$$\gamma \mapsto (L/k,\sigma,\gamma)$$

where $(L/k,\sigma,\gamma)$ is the cyclic algebra generated over L by u with relations $ux = \sigma(x)u$ for any $x \in L$ and $u^{[L:k]} = \gamma$. From this, (b) follows immediately. Finally, if $L \cong k[x]/\left(p(x)\right)$ and $a_1,\ldots,a_m$ are the roots of $p(x)$ in L, then

$$p(x) = q(x)\prod_{i=1}^{m}(x-a_i)$$

for some $q(x) \in L[x]$. By the Chinese Remainder Theorem,

$$\begin{aligned} L\otimes_k L &\cong L\otimes_k k[x]/\left(p(x)\right) \\ &\cong L[x]/\left(q(x)\right) \times \prod_{i=1}^{m} L[x]/\left(x-a_i\right) \\ &\cong L \times A \end{aligned}$$

where A/L is a finite étale algebra. So the following diagram commutes.

$$\begin{array}{ccc} L \otimes_k L & \xrightarrow{\sim} & L \times A \\ & \searrow^{N_{L\otimes_k L/L}} \quad {}^{\mathrm{id}\cdot N_{A/L}}\swarrow & \\ & L & \end{array}$$

In particular, $N_{L\otimes_k L/L}$ is surjective since

$$(\mathrm{id}\cdot N_{A/L})(\lambda, 1, \ldots, 1) = \lambda$$

for any $\lambda \in L$. Then

$$H^1(L, T_L) \cong L^\times / N_{L\otimes_k L/L}\left((L \otimes_k L)^\times\right) = 0,$$

hence (c). □

Lemma 4.1.3. *Let T be a k-torus with a (not necessarily minimal) splitting field E of finite degree over k, and let $[X] \in H^1(k, T)$.*

(a) $\mathrm{ind}(X) \mid [E : k]$.

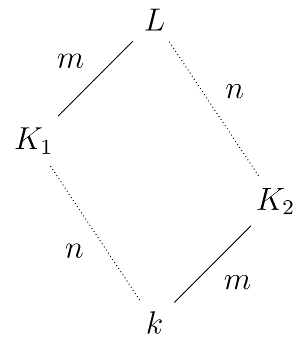
(b) *If $[E : k]$ is prime, then Totaro's question has a positive answer for T.*

Proof. Since T_E is split, $H^1(E, T_E) = 0$ by Theorem 3.4.2. Then $\mathrm{ind}(X) \mid [E : k]$, proving (a). If $[E : k]$ is prime, then by (a), $\mathrm{ind}(X) = 1$ or $[E : k]$. If $\mathrm{ind}(X) = 1$, then $[X] = 0 \in H^1(k, T)$ by Lemma 4.1.1. Otherwise, $[X_E] \in H^1(E, T_E) = 0$. □

Now, for any finite extension of étale algebras A/B, define

$$(A^\times)^{(1)}_B := \{a \in A^\times : N_{A/B}(a) = 1\}.$$

Lemma 4.1.4. *Consider the following diagram of separable field extensions*



for some $m, n > 1$, *and let* $T = R_{K_1/k}\left(R^{(1)}_{L/K_1}\,\mathbb{G}_m\right) \cap R_{K_2/k}\left(R^{(1)}_{L/K_2}\,\mathbb{G}_m\right)$.

(a) *The following sequences of* k*-tori are exact.*

$$0 \to T \to R_{K_1/k}(R^{(1)}_{L/K_1}\,\mathbb{G}_m) \xrightarrow{N_{L/K_2}} R^{(1)}_{K_2/k}\,\mathbb{G}_m \to 0$$

$$0 \to T \to R_{K_2/k}(R^{(1)}_{L/K_2}\,\mathbb{G}_m) \xrightarrow{N_{L/K_1}} R^{(1)}_{K_1/k}\,\mathbb{G}_m \to 0$$

(b) *The following sequences of abelian groups are exact.*

$$(L^\times)^{(1)}_{K_1} \xrightarrow{N_{L/K_2}} (K_2^\times)^{(1)}_k \to H^1(k,T) \xrightarrow{\delta_1} K_1^\times/N_{L/K_1}(L^\times)$$

$$(L^\times)^{(1)}_{K_2} \xrightarrow{N_{L/K_1}} (K_1^\times)^{(1)}_k \to H^1(k,T) \xrightarrow{\delta_2} K_2^\times/N_{L/K_2}(L^\times)$$

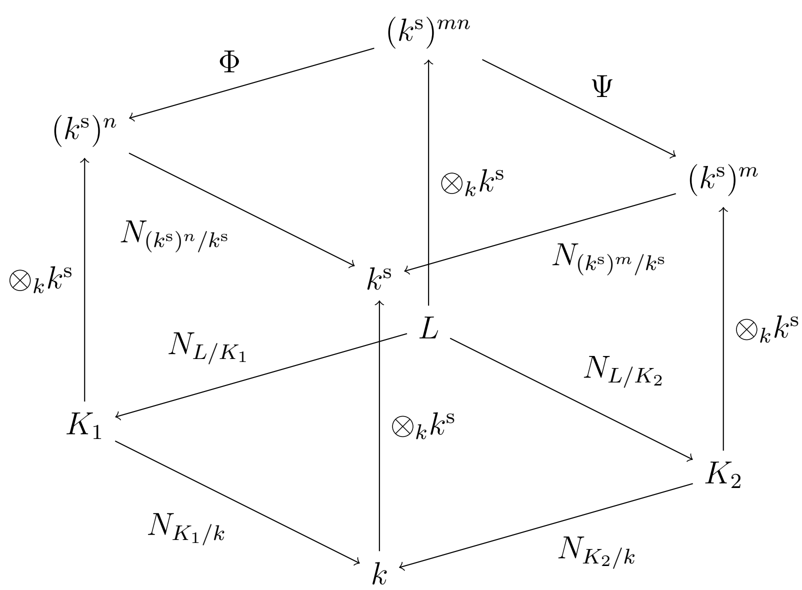
Proof. Left exactness of both sequences is clear from the construction of T, so proving (a) amounts to showing that N_{L/K_2} and N_{L/K_1} are surjective after extending scalars to k^{s}. If $\Phi : (k^{\mathrm{s}})^{mn} \to (k^{\mathrm{s}})^n$ and $\Psi : (k^{\mathrm{s}})^{mn} \to (k^{\mathrm{s}})^m$ are the maps defined by

$$\Phi(x_{ij} : 1 \le i \le m, 1 \le j \le n) = \left(\prod_{i=1}^{m} x_{i1}, \ldots, \prod_{i=1}^{m} x_{in}\right)$$

and

$$\Psi(x_{ij} : 1 \leq i \leq m, 1 \leq j \leq n) = \left(\prod_{j=1}^{n} x_{1j}, \ldots, \prod_{j=1}^{n} x_{mj} \right),$$

then the following diagram commutes.



Any $a \in (R^{(1)}_{K_2 \otimes_k k^{\mathrm{s}}/k^{\mathrm{s}}} \mathbb{G}_m)(k^{\mathrm{s}})$ then corresponds to an m-tuple $(a_1, \ldots, a_m) \in (k^{\mathrm{s}})^m$ such that $\prod_{i=1}^{m} a_i = 1$. But Ψ is surjective: if $x_{ij} = a_i$ when $j = 1$ and $x_{ij} = 1$ otherwise, then

$$\begin{aligned} \Psi(x_{ij} : 1 \leq i \leq m, 1 \leq j \leq n) &= \Psi(a_1, \underbrace{1, \ldots, 1}_{n-1 \text{ times}}, a_2, \underbrace{1, \ldots, 1}_{n-1 \text{ times}}, \ldots, a_m, \underbrace{1, \ldots, 1}_{n-1 \text{ times}}) \\ &= (a_1, \ldots, a_m), \end{aligned}$$

and in fact,

$$\begin{aligned} \Phi(x_{ij} : 1 \leq i \leq m, 1 \leq j \leq n) &= \Phi(a_1, \underbrace{1, \ldots, 1}_{n-1 \text{ times}}, a_2, \underbrace{1, \ldots, 1}_{n-1 \text{ times}}, \ldots, a_m, \underbrace{1, \ldots, 1}_{n-1 \text{ times}}) \\ &= (\underbrace{1, \ldots, 1}_{n \text{ times}}). \end{aligned}$$

So this mn-tuple yields a k^{s}-point of $R^{(1)}_{L \otimes_k k^{\mathrm{s}}/K_1 \otimes_k k^{\mathrm{s}}} \mathbb{G}_m$ mapping to $a \in R^{(1)}_{K_2 \otimes_k k^{\mathrm{s}}/k^{\mathrm{s}}}(k^{\mathrm{s}})$.

Then N_{L/K_2} is surjective as a map of algebraic groups. By a symmetric argument, N_{L/K_1} is surjective too, proving (a). (b) follows from (a), Theorem 3.2.1.(c), and Lemma 4.1.2. $\square$

4.2. Technical Results

Two technical propositions are needed for the proof of Theorem 4.0.1.

Proposition 4.2.1. *Let $L/K/k$ be a tower of separable quadratic extensions with no intermediate fields between k and L other than K, and let*

$$T = R_{K/k}(R^{(1)}_{L/K}\,\mathbb{G}_m).$$

Then Totaro's question has a positive answer for T.

Proof. Let M be the Galois closure of L/k in k^{s} and $G = \mathrm{Gal}(M/k)$. Either $M = L$, in which case $G \cong \mathbb{Z}/4\mathbb{Z}$, or $[M : L] = 2$, in which case $G \cong D_4$. Suppose that $M = L$. Then

$$K \otimes_k L \cong L \times L$$

as $K \subseteq L$, $[K : k] = 2$, and K/k is separable, and

$$L \otimes_k L \cong (L \times L) \times (L \times L)$$

as $[L : k] = 4$ and L/k is Galois. So the following diagram commutes.

$$\begin{array}{ccc} L \otimes_k L & \xrightarrow{\sim} & (L \times L) \times (L \times L) \\ {\scriptstyle N_{L\otimes_k L/K\otimes_k L}}\downarrow & & \downarrow{\scriptstyle N_{L\times L/L} \times N_{L\times L/L}} \\ K \otimes_k L & \xrightarrow{\sim} & L \times L \end{array}$$

Since $N_{L\times L/L} \times N_{L\times L/L}$ is surjective, so is $N_{L\otimes_k L/K\otimes_k L}$, and so by Lemma 4.1.2.(a),

$$H^1(L, T_L) \cong (K \otimes_k L)^\times / N_{L\otimes_k L/K\otimes_k L}\left((L \otimes_k L)^\times\right) = 0.$$

If $[M : L] = 2$, then since D_4 contains three distinct subgroups of order 2, there is another tower of separable extensions $M/L'/k$ such that $[M : L'] = 2$,

$$K \otimes_k L' \cong M,$$

and

$$L \otimes_k L' \cong M \times M.$$

So the following diagram commutes.

$$\begin{array}{ccc} L \otimes_k L' & \xrightarrow{\sim} & M \times M \\ {\scriptstyle N_{L\otimes_k L'/K\otimes_k L'}} \downarrow & & \downarrow {\scriptstyle N_{M\times M/M}} \\ K \otimes_k L' & \xrightarrow{\sim} & M \end{array}$$

Since $N_{M\times M/M}$ is surjective, so is $N_{L\otimes_k L'/K\otimes_k L'}$, and so by Lemma 4.1.2.(a),

$$H^1(L', T_{L'}) \cong (K \otimes_k L')^\times / N_{L\otimes_k L'/K\otimes_k L'}\left((L \otimes_k L')^\times\right) = 0.$$

So $\operatorname{ind}(X) \mid 4$ for any $[X] \in H^1(k, T)$, and if $\operatorname{ind}(X) = 4$, then either $F = L$ or L' will suffice.

Suppose now that $\operatorname{ind}(X) = 2$. Identify $[X]$ with $[\beta]$ for some $\beta \in K^\times$ that is not a norm from $L^\times$. Since $\operatorname{ind}(X) = 2$, it can be assumed by [GLL13, Theorem 9.2] using standard Galois theory reductions (cf. [GH06, Lemma 1.5]) that there is a tower of separable field extensions $E'/E/k$ such that $[E' : E] = 2$, $[E : k] = m$ for some odd m, and

$$\beta \in N_{L\otimes_k E'/K\otimes_k E'}\left((L\otimes_k E')^\times\right).$$

Write

$$E' \cong \begin{cases} E[x]/(x^2+x+a) & \text{if } \operatorname{char}(k)=2 \\ E[x]/(x^2-a) & \text{if } \operatorname{char}(k)\neq 2 \end{cases}$$

for some $a \in E^\times$. In both cases, identify the class of x with $i \in E'$. Then there are $u_0, v_0 \in LE$ not both zero such that

$$\begin{aligned} \beta &= N_{L\otimes_k E'/K\otimes_k E'}(u_0+v_0 i) \\ &= \big(N_{LE/KE}(u_0)+aN_{LE/KE}(v_0)\big)+T_E(u_0,v_0)i \end{aligned}$$

where

$$T_K(u,v) = \begin{cases} \operatorname{tr}_{L/K}(u\overline{v})+N_{L/K}(v) & \text{if } \operatorname{char}(k)=2 \\ \operatorname{tr}_{L/K}(u\overline{v}) & \text{if } \operatorname{char}(k)\neq 2 \end{cases}$$

Since $\beta \in K^\times$, $T_E(u_0,v_0)=0$, and so

$$\beta = N_{LE/KE}(u_0)+aN_{LE/KE}(v_0).$$

If $v_0=0$, then $\beta = N_{LE/KE}(u_0)$, in which case $\beta \in K^\times$ is represented by the K-quadratic form $N_{L/K}$ after extending scalars to KE. But $[KE:K]=[E:k]=m$ is odd. Then by Springer's Theorem [Spr52], $\beta \in N_{L/K}(L^\times)$, a contradiction. So $v_0 \neq 0$.

Now, write

$$K \cong \begin{cases} k[y]/(y^2+y+b) & \text{if } \operatorname{char}(k)=2 \\ k[y]/(y^2-b) & \text{if } \operatorname{char}(k)\neq 2 \end{cases}$$

for some $b \in k^\times$. In both cases, identify the class of y with $j \in K$. Then there are

$\beta_1, \beta_2 \in k$ not both zero such that

$$\beta = \beta_1 + \beta_2 j.$$

Let $N^1, N^2 : L \to k$ and $Q^1, Q^2 : L^2 \to k$ be the k-quadratic forms defined by

$$N_{L/K} = N^1 + N^2 j,$$

$$Q^1(u,v) = \beta_1 N^1(u) + b\beta_2 N^2(u) - N^1(v),$$

and

$$Q^2(u,v) = \begin{cases} (\beta_1+\beta_2)N^2(u) + \beta_2 N^1(u) + N^2(v) & \text{if } \operatorname{char}(k) = 2 \\ \beta_1 N^2(u) + \beta_2 N^1(u) - N^2(v) & \text{if } \operatorname{char}(k) \neq 2 \end{cases}$$

Then setting $x_0 = v_0^{-1}$ and $y_0 = u_0 v_0^{-1}$,

$$\begin{aligned} a &= \beta N_{LE/KE}(x_0) - N_{LE/KE}(y_0) \\ &= (\beta_1 + \beta_2 j)(N^1_{LE} + N^2_{LE} j)(x_0) - (N^1_{LE} + N^2_{LE} j)(y_0) \\ &= Q^1_E(x_0, y_0) + Q^2_E(x_0, y_0) j. \end{aligned}$$

Since $a \in E^\times$, $Q^1_E(x_0, y_0) = a$ and $Q^2_E(x_0, y_0) = 0$. Now, case by $\operatorname{char}(k)$.

First, suppose that $\operatorname{char}(k) \neq 2$. Since $\operatorname{tr}_{LE/KE}(y_0) = 0$, the isotropic vector for Q^2_E comes from the subspace

$$LE \oplus (LE)^0 \cong (L \oplus L^0) \otimes_k E$$

where $L^0 = \ker \operatorname{tr}_{L/K} \subseteq L$. But as $[E : k] = m$ is odd, Q^2 is isotropic by Springer's Theorem [Spr52]. So there is some $(x_1, y_1) \in L \oplus L^0$ such that

$$Q^2(x_1, y_1) = \beta_1 N^2(x_1) + \beta_2 N^1(x_1) - N^2(y_1) = 0.$$

If $x_1 = 0$, then y_1 is an isotropic vector for N^2. But isotropic quadratic forms are universal. So for any x, there is a y such that $N^2(y) = \beta_1 N^2(x) + \beta_2 N^1(x)$, i.e., $Q^2(x,y) = 0$. Then we can assume that $x_1 \neq 0$. So

$$\begin{aligned} \alpha &= Q^1(x_1, y_1) \\ &= Q^1(x_1, y_1) + Q^2(x_1, y_1)j \\ &= \beta N_{L/K}(x_1) - N_{L/K}(y_1) \end{aligned}$$

means that

$$N_{L/K}(x_1^{-1})(N_{L/K}(y_1) + \alpha) = \beta.$$

With $F = k(\sqrt{\alpha})$, $[F : k] = 2$, and since $y_1 \in L^0$,

$$N_{L\otimes_k F/K\otimes_k F}\left(\frac{y_1 + \sqrt{\alpha}}{x_1}\right) = \beta.$$

Then $[X_F] = 0 \in H^1(F, T_F)$, as desired.

Now, suppose that $\mathrm{char}(k) = 2$. Let $T^1, T^2 : L \to k$ be the k-linear maps defined by

$$\mathrm{tr}_{L/K} = T^1 + T^2 j.$$

Since

$$\begin{aligned} (T_E^1(y_0) + 1) + T_E^2(y_0)j &= \mathrm{tr}_{LE/KE}(y_0) + 1 \\ &= \mathrm{tr}_{LE/KE}(u_0 v_0^{-1}) + 1 \\ &= N_{LE/KE}(v_0)\left(\mathrm{tr}_{LE/KE}(u_0\overline{v_0}) + N_{LE/KE}(v_0)\right) \\ &= 0, \end{aligned}$$

$T_E^2(y_0) = 0$, and so the isotropic vector for Q_E^2 comes from the subspace

$$LE \oplus (LE)^{\#} \cong (L \oplus L^{\#}) \otimes_k E$$

where $L^{\#} = \ker T^2 \subseteq L$. But as $[E : k] = m$ is odd, Q^2 is isotropic by Springer's Theorem [Spr52]. So there is some $(x_1, y_1) \in L \oplus L^{\#}$ such that

$$Q^2(x_1, y_1) = (\beta_1 + \beta_2)N^2(x_1) + \beta_2 N^1(x_1) + N^2(y_1) = 0.$$

If $x_1 = 0$, then y_1 is an isotropic vector for N^2. But the symmetric bilinear form

$$b_{N^2} : L^2 \to k$$

defined by

$$b_{N^2}(x, y) := N^2(x + y) - N^2(x) - N^2(y) = T^2(x\overline{y})$$

is non-degenerate. Then N^2 is regular and isotropic, hence universal [EKM08, Proposition 7.13]. So as before, we can assume that $x_1 \neq 0$. Let $\gamma = T^1(y_1)$. If $\gamma = 0$, then $y_1 = 0$ as $y_1 \in L^{\#}$. Setting $\alpha = Q^1(x_1, 0)$ and $F = k[z]/(z^2 + z + \alpha)$ and identifying the class of z with $\lambda \in F$ yields that

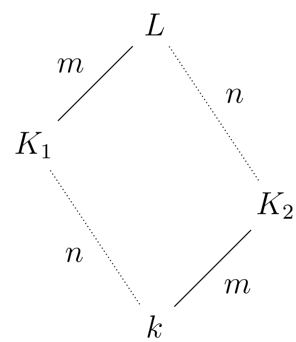
$$N_{L\otimes_k F/K\otimes_k F}\left(\frac{\lambda}{x_1}\right) = \beta.$$

If $\gamma \neq 0$, then

$$N_{L\otimes_k F/K\otimes_k F}\left(\frac{y_1 + \gamma\lambda}{\gamma x_1}\right) = \beta.$$

In both cases, $[F : k] = 2$ and $[X_F] = 0 \in H^1(F, T_F)$, as desired. □

Proposition 4.2.2. *Consider the following diagram of separable field extensions*



for some coprime $m, n > 1$*, and let*

$$T = R_{K_1/k}\left(R^{(1)}_{L/K_1}\,\mathbb{G}_m\right) \cap R_{K_2/k}\left(R^{(1)}_{L/K_2}\,\mathbb{G}_m\right).$$

Then Totaro's question has a positive answer for $[X] \in H^1(k, T)$ *of index* m*,* n*, and* mn*. Furthermore, if* $(\mathrm{ind}(X), m) = 1$*, then* $\mathrm{ind}(X) \mid n$*, and if* $(\mathrm{ind}(X), n) = 1$*, then* $\mathrm{ind}(X) \mid m$*.*

Proof. By Lemma 4.1.4.(b), the following sequences of abelian groups are exact.

$$(L^\times)^{(1)}_{K_1} \xrightarrow{N_{L/K_2}} (K_2^\times)^{(1)}_k \to H^1(k, T) \xrightarrow{\delta_1} K_1^\times / N_{L/K_1}(L^\times)$$

$$(L^\times)^{(1)}_{K_2} \xrightarrow{N_{L/K_1}} (K_1^\times)^{(1)}_k \to H^1(k, T) \xrightarrow{\delta_2} K_2^\times / N_{L/K_2}(L^\times)$$

The proof will proceed according to the index.

First, suppose that $\mathrm{ind}(X) = m$. Since $[L : K_2] = n$, $K_2^\times / N_{L/K_2}(L^\times)$ is n-torsion. But $(m, n) = 1$, and $\mathrm{per}(X) \mid \mathrm{ind}(X)$. So $\delta_2([X]) = 0$. Then $[X]$ lifts to some $\beta \in (K_1^\times)^{(1)}_k$. Now,

$$K_2 \otimes_k K_2 \cong K_2 \times B$$

where B/K_2 is an étale algebra as K_2/k is separable,

$$K_1 \otimes_k K_2 \cong L$$

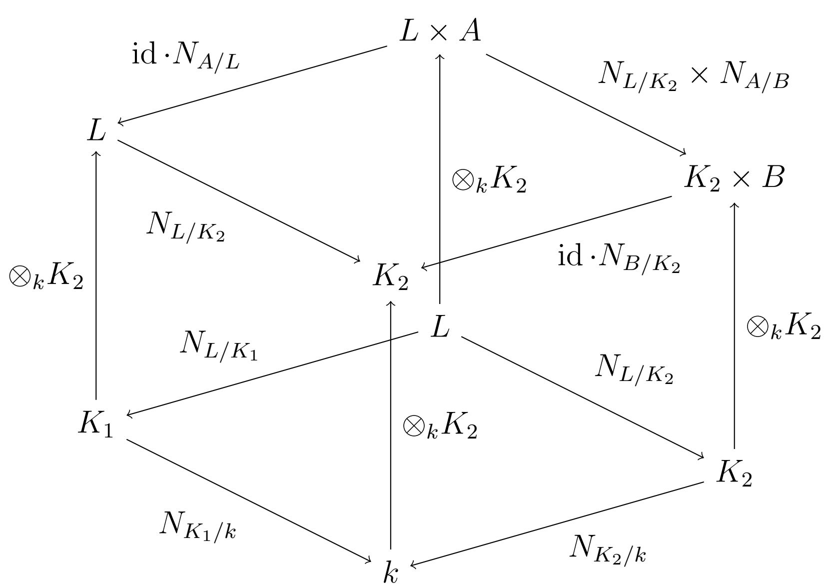
as $K_1, K_2 \subseteq L$ have coprime degrees and are therefore k-linearly disjoint such that

$$[K_1 : k][K_2 : k] = mn = [L : k],$$

and

$$L \otimes_k K_2 \cong L \times A$$

where $A \cong B \otimes_{K_2} L/L$ is an étale algebra as $K_2 \subseteq L$ and K_2/k is separable. After identifying through the natural isomorphisms, the following diagram commutes.



Observe that

$$(\mathrm{id} \cdot N_{A/L})(\beta, 1) = \beta$$

and

$$(N_{L/K_2} \times N_{A/B})(\beta, 1) = \big(N_{K_1/k}(\beta), N_{A/B}(1)\big) = (1, 1),$$

meaning that $[X_{K_2}] = 0 \in H^1(K_2, T_{K_2})$. Since $\operatorname{ind}(X) = [K_2 : k] = m$, it suffices to take $F = K_2$. But only that $(\operatorname{ind}(X), n) = 1$ is needed to show that $[X_{K_2}] = 0$. So $(\operatorname{ind}(X), n) = 1$ implies that $\operatorname{ind}(X) \mid m$. By a symmetric argument, $F = K_1$ suffices when $\operatorname{ind}(X) = n$, and $(\operatorname{ind}(X), m) = 1$ implies that $\operatorname{ind}(X) \mid n$.

Now, suppose that $\operatorname{ind}(X) = mn$. Since the sequence of k-tori

$$0 \to T \to R_{K_1/k}(R^{(1)}_{L/K_1} \mathbb{G}_m) \xrightarrow{N_{L/K_2}} R^{(1)}_{K_2/k} \mathbb{G}_m \to 0$$

is short exact, so is the sequence of K_2-tori

$$0 \to T_{K_2} \to R_{L/K_2}(R^{(1)}_{L\times A/L} \mathbb{G}_m) \xrightarrow{N_{L\times A/K_2\times B}} R^{(1)}_{K_2\times B/K_2} \mathbb{G}_m \to 0.$$

Since K_2^{s}-points of $R^{(1)}_{K_2\times B/K_2} \mathbb{G}_m$ take the form $(N_{B\otimes_{K_2} K_2^{\mathrm{s}}/K_2^{\mathrm{s}}}(\beta^{-1}), \beta)$ for $\beta \in (B \otimes_{K_2} K_2^{\mathrm{s}})^\times$,

$$R^{(1)}_{K_2\times B/K_2} \mathbb{G}_m \cong \mathbb{G}_{m,B}\,.$$

By a similar argument,

$$R_{L/K_2}(R^{(1)}_{L\times A/L} \mathbb{G}_m) \cong R_{L/K_2} \mathbb{G}_{m,A}\,.$$

So

$$0 \to T_{K_2} \to R_{L/K_2} \mathbb{G}_{m,A} \xrightarrow{N_{A/B}} \mathbb{G}_{m,B} \to 0$$

is a short exact sequence of K_2-tori. Since A/L is an étale algebra, $H^1(L, \mathbb{G}_{m,A}) = 0$ by Theorem 3.4.2. Theorem 3.2.1.(c) then yields the exact sequence of abelian groups

$$A^\times \xrightarrow{N_{A/B}} B^\times \to H^1(K_2, T_{K_2}) \to 0.$$

So $[X_{K_2}]$ lifts to some $\beta \in B^\times$. Let C/L be the étale algebra such that

$$L \otimes_{K_2} L \cong L \times C.$$

Then since

$$\begin{aligned} A \otimes_{K_2} L &\cong B \otimes_{K_2} L \otimes_{K_2} L \\ &\cong B \otimes_{K_2} (L \times C) \\ &\cong A \times (B \otimes_{K_2} C), \end{aligned}$$

the following diagram commutes.

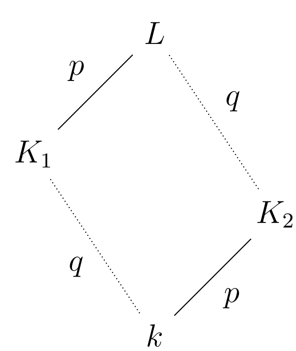
$$\begin{array}{ccc} A \otimes_{K_2} L & \xrightarrow{\sim} & A \times (B \otimes_{K_2} C) \\ {\scriptstyle N_{A\otimes_{K_2}L/A}}\downarrow & & \downarrow{\scriptstyle \mathrm{id}\cdot N_{B\otimes_{K_2}C/A}} \\ B \otimes_{K_2} L & \xrightarrow{\sim} & A \end{array}$$

But

$$(\mathrm{id} \cdot N_{B\otimes_{K_2}C/A})(\beta, 1) = \beta,$$

meaning that $[X_L] = [(X_{K_2})_L] = 0 \in H^1(L, T_L)$. Since $[L : k] = mn$, $F = L$ suffices. $\square$

Corollary 4.2.3. *Consider the following diagram of separable field extensions*



for some distinct primes p and q, and let

$$T = R_{K_1/k}\left(R^{(1)}_{L/K_1}\,\mathbb{G}_m\right) \cap R_{K_2/k}\left(R^{(1)}_{L/K_2}\,\mathbb{G}_m\right).$$

Then Totaro's question has a positive answer for T.

Proof. The claim follows immediately from Proposition 4.2.2. □

4.3. Proof of Theorem 4.0.1

Let $\Gamma = \mathrm{Gal}(k^{\mathrm{s}}/k)$. For any rank r k-torus T, define its **character module** to be

$$\mathbf{X}(T) := \mathrm{Hom}(T_{k^{\mathrm{s}}}, \mathbb{G}_{m,k^{\mathrm{s}}})\ [\,\cong \mathrm{Hom}(\mathbb{G}^r_{m,k^{\mathrm{s}}}, \mathbb{G}_{m,k^{\mathrm{s}}}) \cong \mathbb{Z}^r\,].$$

Then $\mathbf{X}(T)$ is a rank r Γ-module. The association $T \mapsto \mathbf{X}(T)$ is an antiequivalence between the categories of k-tori and finitely-generated Γ-modules; in fact, it is an antiequivalence between the categories of k-tori split by a finite Galois extension E/k and finitely-generated $\mathrm{Gal}(E/k)$-modules. The Γ-action on $\mathbf{X}(T)$ yields a continuous representation

$$\Gamma \to \mathrm{Aut}(\mathbf{X}(T)) \cong \mathrm{Aut}(\mathbb{Z}^r) \cong \mathrm{GL}_r(\mathbb{Z})$$

whose kernel $\mathfrak{h} \trianglelefteq \Gamma$ corresponds to the minimal splitting field of T, a finite Galois extension E/k. The group $\mathrm{GL}_r(\mathbb{Z})$ contains the image of this representation, a copy of $\Gamma/\mathfrak{h} \cong \mathrm{Gal}(E/k)$. Call this the **Galois group of** T. On the other hand, an embedding $\mathrm{Gal}(E/k) \to \mathrm{GL}_r(\mathbb{Z})$ lifts to a continuous representation $\Gamma \to \mathrm{GL}_r(\mathbb{Z})$, which determines a Γ-action on $\mathbf{X}(\mathbb{G}^r_m)$, identifying the rank r k-torus $\mathrm{Spec}\left(E[\mathbf{X}(\mathbb{G}^r_m)]^{\Gamma}\right)$

whose Galois group is $\mathrm{Gal}(E/k)$. Explicitly,

$$\begin{aligned}\{\text{rank } r\ k\text{-tori}\}/\cong \;&\leftrightarrow\; \{\text{rank } r\ \Gamma\text{-modules}\}/\cong\\ &\leftrightarrow\; H^1(k, \mathrm{Aut}(\mathbf{X}(\mathbb{G}_m^r)))\\ &\leftrightarrow\; H^1(k, \mathrm{Aut}(\mathbb{Z}^r))\\ &\leftrightarrow\; H^1(k, \mathrm{GL}_r(\mathbb{Z}))\\ &=\; \mathrm{Hom}(\Gamma, \mathrm{GL}_r(\mathbb{Z}))/\!\sim\end{aligned}$$

where $\rho \sim \rho'$ if and only if $\rho(\Gamma)$ and $\rho'(\Gamma)$ are conjugate in $\mathrm{GL}_r(\mathbb{Z})$.

To classify rank r tori, it is necessary to count the conjugacy classes of finite subgroups of $\mathrm{GL}_r(\mathbb{Z})$. There are 13 such classes in $\mathrm{GL}_2(\mathbb{Z})$; in [Vos65], however, Voskresenskiĭ gave explicit representations of *15* finite groups in terms of matrix generators along with their associated rank 2 tori. He later corrected this in a short geometric proof that rank 2 tori are rational [Vos98]; here, he noted that there are only two distinct maximal finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$ up to conjugacy, D_4 and D_6, whereas he produced two faithful representations of each of these groups in $\mathrm{GL}_2(\mathbb{Z})$ in his earlier classification paper.

For the convenience of the cross-referencing reader, the proof of Theorem 4.0.1 will follow Voskresenskiĭ's original classification and will proceed according to $\mathrm{Gal}(E/k)$ where E is the minimal splitting field of the torus. Recall that for a given group, there may be multiple isomorphism classes of tori associated to that group (over suitably general fields) depending on how many conjugacy classes represent its isomorphism class in $\mathrm{GL}_2(\mathbb{Z})$. Finally: by Lemma 4.1.1 and Lemma 4.1.3, one can reduce $\mathrm{ind}(X)$ to be a non-trivial proper divisor of $[E : k]$.

4.3.1 Rank 1 Tori

There are only two (conjugacy classes of) finite subgroups of $\mathrm{GL}_1(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$: (1) and $\mathbb{Z}/2\mathbb{Z}$. These correspond to the two classes of rank 1 tori. For both types, a positive answer to Totaro's question is a trivial consequence of the previous reductions.

1. $\mathrm{Gal}(E/k) \cong (1)$ and $T \cong \mathbb{G}_m$

Proof. T is quasi-trivial, and so we are done by Theorem 3.4.2. □

2. $\mathrm{Gal}(E/k) \cong \mathbb{Z}/2\mathbb{Z}$ and $T \cong R^{(1)}_{E/k}\,\mathbb{G}_m$

Proof. $[E:k]$ is prime, and so we are done by Lemma 4.1.3.(b). □

4.3.2 Rank 2 Tori

There are 9 isomorphism classes and 15 conjugacy classes of finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$.

1. $\mathrm{Gal}(E/k) \cong (1)$ and $T \cong \mathbb{G}_m \times \mathbb{G}_m$

Proof. T is quasi-trivial, and so we are done by Theorem 3.4.2. □

2. $\mathrm{Gal}(E/k) \cong \mathbb{Z}/2\mathbb{Z}$

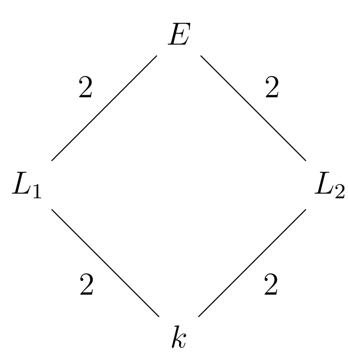
(a) $T \cong R^{(1)}_{E/k}\,\mathbb{G}_m \times R^{(1)}_{E/k}\,\mathbb{G}_m$

(b) $T \cong \mathbb{G}_m \times R^{(1)}_{E/k}\,\mathbb{G}_m$

(c) $T \cong R_{E/k}\,\mathbb{G}_m$

Proof. $[E:k]$ is prime, and so we are done by Lemma 4.1.3.(b). □

3. $\mathrm{Gal}(E/k) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$



(a) $T \cong R_{L_1/k}\left(R^{(1)}_{E/L_1}\,\mathbb{G}_m\right)$

Proof. Since $[E:k]=4$, we can assume that $\mathrm{ind}(X)=2$. Then

$$H^1(k,T)\cong H^1(L_1,R^{(1)}_{E/L_1}\,\mathbb{G}_m)\cong \mathrm{Br}(E/L_1)$$

by Lemma 4.1.2.(b). Let $\delta : H^1(k,T)\to \mathrm{Br}(E/L_1)$ denote the composition. Since

$$\begin{aligned}\delta([X_{L_2}]) &\cong [\delta([X])\otimes_k L_2]\\ &\cong [\delta([X])\otimes_{L_1} L_1\otimes_k L_2]\\ &\cong [\delta([X])\otimes_{L_1} E]\\ &= 0\in \mathrm{Br}(E/L_1)\end{aligned}$$

and $[L_2:k]=2$, it suffices to take $F=L_2$. □

(b) $T\cong R^{(1)}_{L_1/k}\,\mathbb{G}_m\times R^{(1)}_{L_2/k}\,\mathbb{G}_m$

Proof. Since $[E:k]=4$, we can assume that $\mathrm{ind}(X)=2$. As

$$\begin{aligned}H^1(k,T) &\cong H^1(k,R^{(1)}_{L_1/k}\,\mathbb{G}_m\times R^{(1)}_{L_2/k}\,\mathbb{G}_m)\\ &\cong H^1(k,R^{(1)}_{L_1/k}\,\mathbb{G}_m)\times H^1(k,R^{(1)}_{L_2/k}\,\mathbb{G}_m)\\ &\cong \mathrm{Br}(L_1/k)\times\mathrm{Br}(L_2/k)\end{aligned}$$

by Lemma 4.1.2.(b), $[X]\in H^1(k,T)$ can be identified with a pair of division algebras D_1 and D_2 where $[D_1]\in\mathrm{Br}(L_1/k)$ and $[D_2]\in\mathrm{Br}(L_2/k)$. Since D_1 and D_2 are both split over quadratic extensions L_1 and L_2, respectively, each is either a field or a quaternion division algebra. If either of D_1 or D_2 is a field, then it suffices to take either $F=L_2$ or L_1, respectively. So we can assume that both D_1 and D_2 are quaternion division algebras.

Let $D=D_1\otimes_k D_2$. By Albert's Theorem [Alb72], either D is a division algebra or D_1 and D_2 have a common subfield F separable over k such that $[F:k]=2$

that necessarily splits both algebras. Suppose that D is a division algebra. Then

$$\mathrm{ind}_{\mathrm{Sch}}(D) = \deg(D) = \deg(D_1)\deg(D_2) = 4.$$

But since $\mathrm{ind}(X) = 2$, it can be assumed by [GLL13, Theorem 9.2] using standard Galois theory reductions (cf. [GH06, Lemma 1.5]) that there is a tower of separable field extensions $K'/K/k$ such that $[K' : K] = 2$, $[K : k]$ is odd, and ${D_1}_{K'}$ and ${D_2}_{K'}$ (hence $D_{K'}$) are split. Since $[K : k]$ is odd and $\mathrm{ind}_{\mathrm{Sch}}(D) = 4$, D_K is a division algebra. But as $D_{K'}$ is split and $[K' : K] = 2$,

$$\mathrm{ind}_{\mathrm{Sch}}(D) = \mathrm{ind}_{\mathrm{Sch}}(D_K) = 2,$$

a contradiction. So D_1 and D_2 have a common subfield F separable over k such that $[F : k] = 2$ that necessarily splits both algebras, completing the proof. □

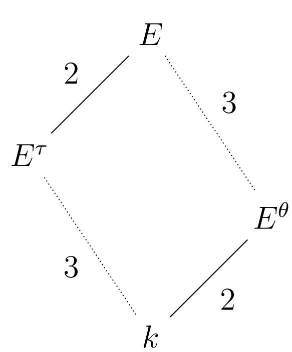
4. $\mathrm{Gal}(E/k) \cong \mathbb{Z}/3\mathbb{Z}$ and $T \cong R^{(1)}_{E/k}\,\mathbb{G}_m$

Proof. $[E : k]$ is prime, and so we are done by Lemma 4.1.3.(b). □

5. $\mathrm{Gal}(E/k) \cong \mathbb{Z}/4\mathbb{Z} = \langle \phi \rangle$ and $T \cong R_{E^{\phi^2}/k}\left(R^{(1)}_{E/E^{\phi^2}}\,\mathbb{G}_m\right)$

Proof. We are done by Proposition 4.2.1. □

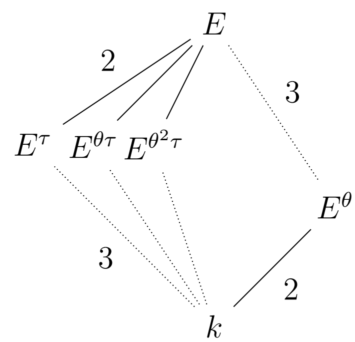
6. $\mathrm{Gal}(E/k) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle \theta \rangle \times \langle \tau \rangle$



$$T = R_{E^\tau/k}\left(R^{(1)}_{E/E^\tau}\,\mathbb{G}_m\right) \cap R_{E^\theta/k}\left(R^{(1)}_{E/E^\theta}\,\mathbb{G}_m\right)$$

Proof. We are done by Corollary 4.2.3. □

7. $\mathrm{Gal}(E/k) \cong S_3 = \langle\theta\rangle \rtimes \langle\tau\rangle$



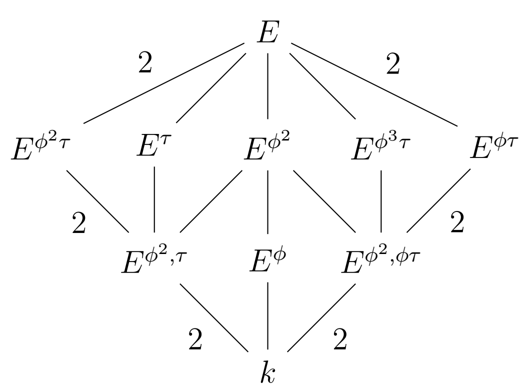
(a) $T \cong R^{(1)}_{E^\tau/k}\,\mathbb{G}_m$.

Proof. Since $[E:k]=6$, the only cases to consider are $\mathrm{ind}(X)=2$ and 3. But by Lemma 4.1.2.(c), only $\mathrm{ind}(X)=3$ is possible, and $F=E^\tau$ suffices by Lemma 4.1.2.(c). □

(b) $T \cong R_{E^\tau/k}\left(R^{(1)}_{E/E^\tau}\,\mathbb{G}_m\right) \cap R_{E^\theta/k}\left(R^{(1)}_{E/E^\theta}\,\mathbb{G}_m\right)$.

Proof. We are done by Corollary 4.2.3. □

8. $\mathrm{Gal}(E/k) \cong D_4 \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \langle\phi\rangle \rtimes \langle\tau\rangle$



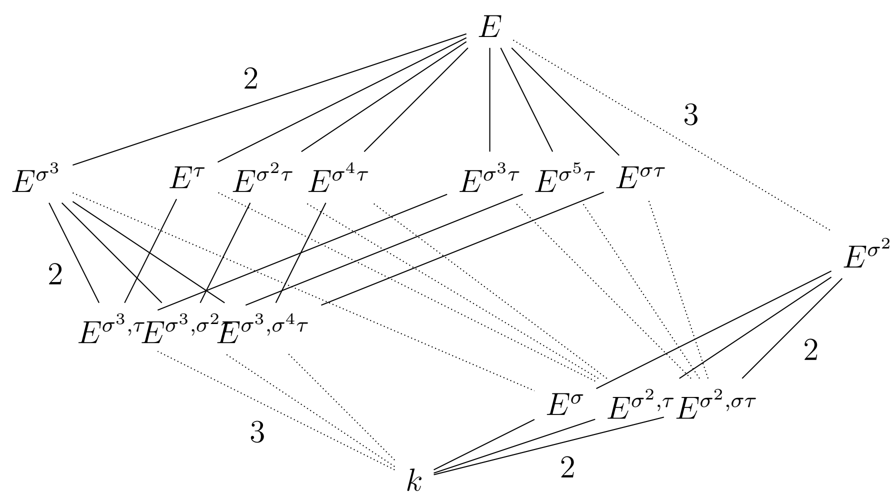
(a) $T \cong R_{E^{\phi^2,\tau}/k}\left(R^{(1)}_{E^\tau/E^{\phi^2,\tau}}\,\mathbb{G}_m\right)$

Proof. We are done by Proposition 4.2.1. □

(b) $T \cong R_{E^{\phi^2,\phi\tau}/k}\left(R^{(1)}_{E^{\phi\tau}/E^{\phi^2,\phi\tau}}\,\mathbb{G}_m\right)$

Proof. T is isomorphic to the torus from (a). □

9. $\mathrm{Gal}(E/k) \cong D_6 \cong \mathbb{Z}/6\,\mathbb{Z} \rtimes \mathbb{Z}/2\,\mathbb{Z} = \langle\sigma\rangle \rtimes \langle\tau\rangle$



(a) $T \cong R_{E^{\sigma^2}/k}\left(R^{(1)}_{E/E^{\sigma^2}}\,\mathbb{G}_m\right) \cap R_{E^{\sigma^3}/k}\left(R^{(1)}_{E/E^{\sigma^3}}\,\mathbb{G}_m\right) \cap R_{E^{\tau}/k}\,\mathbb{G}_m$

Proof. Observe that $t \in T(A)$ for a k-algebra A if and only if

$$\begin{aligned} t^{\sigma^2}t^{\sigma^4}t &= 1 \\ t^{\sigma^3}t &= 1 \\ t^{\tau} &= t, \end{aligned}$$

which means that

$$T \cong R_{E^{\sigma^2,\tau}/k}\left(R^{(1)}_{E^{\tau}/E^{\sigma^2,\tau}}\,\mathbb{G}_m\right) \cap R_{E^{\sigma^3,\tau}/k}\left(R^{(1)}_{E^{\tau}/E^{\sigma^3,\tau}}\,\mathbb{G}_m\right).$$

So we are done by Proposition 4.2.1. □

(b) $T \cong R_{E^{\sigma^2}/k}\left(R^{(1)}_{E/E^{\sigma^2}}\,\mathbb{G}_m\right) \cap R_{E^{\sigma^3}/k}\left(R^{(1)}_{E/E^{\sigma^3}}\,\mathbb{G}_m\right) \cap R_{E^{\tau}/k}\left(R^{(1)}_{E/E^{\tau}}\,\mathbb{G}_m\right)$

Proof. T is isomorphic to the torus from (a). □

This exhausts Voskresenskiĭ's classification and thus completes the proof of Theorem 4.0.1.

4.4. del Pezzo Surfaces

We now prove a general consequence of Theorem 4.0.1.

Corollary 4.4.1. *Let X be a regular variety over a field containing a principal homogeneous space of a smooth torus of rank ≤ 2 as a dense open subset. If X admits a zero-cycle of degree $d \geq 1$, then X has a closed étale point of degree dividing d.*

Proof. Write $X = \overline{Y}$ for some principal homogeneous space Y under a torus T of rank ≤ 2. By a general moving lemma for zero-cycles (cf. [GLL13, Theorem 6.8]), given a closed point of X of degree n, there is a zero-cycle on Y of degree n. So given a zero-cycle on X of degree d, there is a zero-cycle on Y of degree d. By Theorem 4.0.1, $Y \subseteq X$ has a closed étale point of degree dividing d. □

A **del Pezzo surface** is a smooth projective surface X over a field k whose anticanonical bundle ω_X^{-1} is ample. Its **degree** is the self-intersection number $D = (K_X, K_X)$ of its canonical divisor K_X and lies between 1 and 9. If $D = 8$, then $X_{k^{\mathrm{s}}}$ is isomorphic to either $\mathbb{P}^2_{k^{\mathrm{s}}}$ blown up at a point or $\mathbb{P}^1_{k^{\mathrm{s}}} \times \mathbb{P}^1_{k^{\mathrm{s}}}$; otherwise, $X_{k^{\mathrm{s}}}$ is isomorphic to $\mathbb{P}^2_{k^{\mathrm{s}}}$ blown up at $9 - D$ points in general position. Manin [Man86] is a standard reference for these results; in fact, it is a theorem of Manin that del Pezzo surfaces of degree 6 contain torsors of rank 2 tori as dense open subsets (cf. [Man72, Teorema 8.6], [Man86, Theorem 30.3.1]). This gives us the following result.

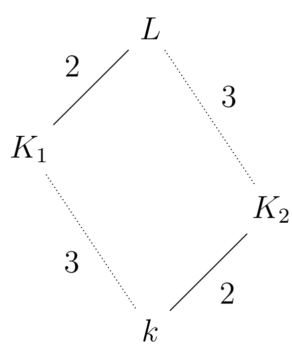
Corollary 4.4.2. *Let X be a del Pezzo surface of degree 6. If X admits a zero-cycle of degree $d \geq 1$, then X has a closed étale point of degree dividing d.*

Proof. This follows immediately from Corollary 6.1. □

Of independent interest are the particular rank 2 tori that arise from del Pezzo surfaces of degree 6 within Voskresenskiĭ's classification. By the explicit algebraic computations of Blunk [Blu10], over a non-separably-closed field k, each such torus takes the form

$$T = R_{K_2/k}\left(R^{(1)}_{L/K_2}\,\mathbb{G}_m\right)/R^{(1)}_{K_1/k}\,\mathbb{G}_m$$

for some diagram of separable field extensions



Lemma 4.4.3. $T \cong R_{K_1/k}\left(R^{(1)}_{L/K_1}\,\mathbb{G}_m\right) \cap R_{K_2/k}\left(R^{(1)}_{L/K_2}\,\mathbb{G}_m\right)$.

Proof. Let $\mathrm{Gal}(L/K_1) \cong \mathbb{Z}/2\,\mathbb{Z} = \langle\sigma\rangle$ and

$$S = R_{K_1/k}\left(R^{(1)}_{L/K_1}\,\mathbb{G}_m\right) \cap R_{K_2/k}\left(R^{(1)}_{L/K_2}\,\mathbb{G}_m\right).$$

It suffices to show that the sequence of k-tori

$$0 \to R^{(1)}_{K_1/k}\,\mathbb{G}_m \xrightarrow{\iota} R_{K_2/k}\left(R^{(1)}_{L/K_2}\,\mathbb{G}_m\right) \xrightarrow{\varphi} S \to 0$$

where ι is the inclusion map and φ is defined functorially for any k-algebra A by

$$\begin{array}{rcl} R_{K_2/k}\left(R^{(1)}_{L/K_2}\mathbb{G}_m\right)(A) & \xrightarrow{\varphi(A)} & S(A) \\ a & \mapsto & \sigma(a)a^{-1} \end{array}$$

is short exact. Left exactness is clear since $K_1 = L^\sigma$, so all that remains is to show that φ is surjective after passing to the separable closure k^{s}. Let $\beta \in S(k^{\mathrm{s}})$. Then

$$N_{L\otimes_k k^{\mathrm{s}}/K_1\otimes_k k^{\mathrm{s}}}(\beta) = 1 = N_{L\otimes_k k^{\mathrm{s}}/K_2\otimes_k k^{\mathrm{s}}}(\beta).$$

By Theorem 3.4.2, $\beta = \sigma(\gamma)\gamma^{-1}$ for some $\gamma \in (L \otimes_k k^{\mathrm{s}})^\times$. Set $\lambda = N_{L\otimes_k k^{\mathrm{s}}/K_2\otimes_k k^{\mathrm{s}}}(\gamma)$. Then

$$\sigma(\lambda)\lambda^{-1} = N_{L\otimes_k k^{\mathrm{s}}/K_2\otimes_k k^{\mathrm{s}}}(\beta) = 1,$$

i.e., $\lambda \in ((K_2 \otimes_k k^{\mathrm{s}})^\sigma)^\times = (k^{\mathrm{s}})^\times$. Since K_1/k is separable and k^{s} is separably closed, $K_1 \otimes_k k^{\mathrm{s}} \cong (k^{\mathrm{s}})^3$. So there is some $\eta \in (K_1 \otimes_k k^{\mathrm{s}})^\times$ such that $\lambda = N_{K_1\otimes_k k^{\mathrm{s}}/k^{\mathrm{s}}}(\eta)$. Set $\alpha = \eta^{-1}\gamma$. Then

$$N_{L\otimes_k k^{\mathrm{s}}/K_2\otimes_k k^{\mathrm{s}}}(\alpha) = N_{L\otimes_k k^{\mathrm{s}}/K_2\otimes_k k^{\mathrm{s}}}\left(\eta^{-1}\gamma\right) = \lambda^{-1}N_{L\otimes_k k^{\mathrm{s}}/K_2\otimes_k k^{\mathrm{s}}}(\gamma) = 1,$$

i.e., $\alpha \in R_{K_2/k}\left(R^{(1)}_{L/K_2}\mathbb{G}_m\right)(k^{\mathrm{s}})$, and

$$\varphi(\alpha) = \varphi\left(\eta^{-1}\gamma\right) = \sigma\left(\eta^{-1}\gamma\right)\left(\eta^{-1}\gamma\right)^{-1} = \sigma(\gamma)\gamma^{-1} = \beta,$$

completing the proof. $\square$

Chapter 5

Totaro's Question for Adjoint Groups of Types A_1 and A_{2n}

This chapter is largely excerpted from the author's paper of the same name to appear in *Proceedings of the American Mathematical Society* [GSa].

Theorem 5.0.4. *Let k be a field of characteristic not equal to 2, and let G be an absolutely simple classical adjoint group over k of type A_1 or A_{2n}. Then Totaro's question has an affirmative answer for G.*

Theorem 5.0.4 has a concrete interpretation in terms of algebras with unitary involution. Let K/k be an étale quadratic extension, let A and B be central simple algebras over K of degree 2 or odd degree, and let σ and τ be K/k-involutions on A and B. If $L_1, \ldots, L_m/k$ are finite field extensions with $\gcd\{[L_i : k]\} = d$ such that $(A, \sigma)_{L_i} \cong (B, \tau)_{L_i}$ for $i = 1, \ldots, m$, then there is a separable field extension F/k with $[F : k] \mid d$ such that $(A, \sigma)_F \cong (B, \tau)_F$.

5.1. Lemmata

Proceeding with the notation from section 2.2.2, let K/k be an étale quadratic extension, let A be a central simple algebra over K, and let σ be a K/k–involution on A. If A is Brauer–equivalent to a division algebra D, then D also admits a K/k–involution δ by the following existence criterion.

Theorem 5.1.1 (Albert–Riehm–Scharlau [Sch75, p. 31])**.** *A central simple algebra D over K admits a K/k–involution if and only if $[D] \in \ker[\operatorname{Br} K \xrightarrow{\text{cor}} \operatorname{Br} k]$.*

Since Totaro's question asks about the existence of a *separable* field extensions over which a given torsor has a point, the following classical theorem will prove essential.

Theorem 5.1.2 (Jacobson [Jac96, Theorem 5.3.18])**.** *Let D be a central division algebra over K with K/k–involution δ. Then there exists a maximal subfield $E \subseteq D$, separable over k, such that $\delta(E) = E$ and $E = KE^{\delta}$.*

If $G \cong \operatorname{Aut}(A, \sigma)$ is absolutely simple and adjoint of type A_n, then $H^1(k, G)$ classifies isomorphism classes of algebras of degree $n+1$ over K with unitary involution. Since this Galois cohomology set has trivial element $[(A, \sigma)]$, for any field extension L/k,

$$\begin{aligned}
[(B,\tau)]_L = 1 \in H^1(L, G_L) \quad &\Longleftrightarrow \quad (A,\sigma) \otimes_k L \cong (B,\tau) \otimes_k L \\
&\Longleftrightarrow \quad A \otimes_k L \cong B \otimes_k L \text{ and } \sigma \otimes \mathrm{id}_L \cong \tau \otimes \mathrm{id}_L \\
&\Longleftrightarrow \quad L \text{ splits } A \otimes_K B^{\mathrm{op}} \text{ and } \sigma \otimes \mathrm{id}_L \cong \tau \otimes \mathrm{id}_L\,.
\end{aligned}$$

Our objective then is to find minimal separable field extensions of k that split $A \otimes_K B^{\mathrm{op}}$ followed by minimal separable field extensions to make the involutions isomorphic. In fact, σ is the adjoint involution of some hermitian form on (D, δ) determined up to similarity in $k^{\times}$, and two unitary involutions on A are isomorphic if and only if their associated hermitian forms are similar. So once the underlying algebras are isomorphic, it suffices to find a minimal separable field extension to make the corresponding hermitian forms similar.

Write $W(k)$ for the Witt ring of quadratic forms over k, and let $W(D,\delta)$ denote the Witt group of hermitian forms over (D,δ). The tensor product of forms induces a $W(k)$–module structure on $W(D,\delta)$. The next two claims will be critical to the proof of Theorem 5.0.4.

Lemma 5.1.3. *If σ and τ are K/k–involutions on A, then $(A,\sigma)\otimes_k K \cong (A,\tau)\otimes_k K$.*

Proof. By [KMRT98, Proposition 2.4], $(A,\sigma)\otimes_k K \cong (A\times A^{\mathrm{op}},\varepsilon)$ where ε is the **exchange** involution on $A\times A^{\mathrm{op}}$. The same holds for $(A,\tau)\otimes_k K$. □

Proposition 5.1.4. *Let σ and τ be K/k–involutions on A, and let L/k be a field extension of odd degree. If $(A,\sigma)\otimes_k L \cong (A,\tau)\otimes_k L$, then $(A,\sigma)\cong(A,\tau)$.*

Proof. By the above remarks, it suffices to show that if h and h' are hermitian forms over (D,δ) such that $h\otimes_k L \cong \lambda(h'\otimes_k L)$ for some $\lambda \in L^\times$, then $h \cong \nu h'$ for some $\nu \in k^\times$. We first assume that $L = k(\lambda)$ is a simple field extension of odd degree over k. There is a natural embedding of modules (cf. [BFL90, Proposition 1.2])

$$r^* : W(A,\sigma) \to W((A,\sigma)\otimes_k L)$$

induced by the extension of scalars, and any non-vanishing k–linear functional $s : L \to k$ induces a homomorphism of modules called the **Scharlau transfer** with respect to s

$$s_* : W((A,\sigma)\otimes_k L) \to W(A,\sigma),$$

sending a class of hermitian forms $[\eta]$ on $D\otimes_k L$ over L with respect to $\delta\otimes 1$ to the class of

$$s\circ\eta : (D\otimes_k L)\times(D\otimes_k L) \xrightarrow{\eta} L \xrightarrow{s} k.$$

Arguing as in [Sch85, Lemma 2.5.8] and [BFL90, Proposition 1.2], given the linear functional defined by $s(1) = 1$ and $s(\lambda) = \cdots = s(\lambda^{[L:k]-1}) = 0$, the Scharlau transfer with respect to s satisfies the projection formulas

$$s_*([h \otimes_k L]) = s_*(r^*([h])) = s_*(r^*([1])) \cdot [h] = [h]$$

and

$$s_*([\lambda(h' \otimes_k L)]) = s_*([\lambda] \cdot r^*([h'])) = s_*([\lambda]) \cdot [h'] = [N_{L/k}(\lambda)h'].$$

Since $h \otimes_k L \cong \lambda(h' \otimes_k L)$, comparing dimensions yields that $h \cong N_{L/k}(\lambda)h'$.

Now, if $k(\lambda) \subsetneq L$, then we can filter $L/k(\lambda)$ as a tower of simple field extensions

$$k(\lambda, \lambda_1, \ldots, \lambda_{n-1}, \lambda_n) \supsetneq k(\lambda, \lambda_1, \ldots, \lambda_{n-1}) \supsetneq \cdots \supsetneq k(\lambda),$$

each of odd degree. Let $L_0 = k(\lambda)$ and $L_i = k(\lambda, \lambda_1, \ldots, \lambda_i)$ for $i = 1, \ldots, n$. For each field extension L_i/L_{i-1} of degree d_i, define an L_{i-1}–linear functional $s^i : L_i \to L_{i-1}$ by $s^i(1) = 1$ and $s^i(\lambda_i) = \cdots = s^i(\lambda_i^{d_i-1}) = 0$. Each of of these linear functionals is also $k(\lambda)$–linear, and so each associated Scharlau transfer satisfies $s^i_*([\lambda]) = [\lambda]$ by the projection formulas. Then

$$s^i_*([h \otimes_k L_i]) = [h \otimes_k L_{i-1}]$$

and

$$s^i_*([\lambda(h' \otimes_k L_i]) = [\lambda(h' \otimes_k L_{i-1})]$$

for each $i = 1, \ldots, n$. By comparing dimensions, the result is immediate. □

5.2. Proof of Theorem 5.0.4

The étale quadratic extension K is isomorphic to $k \times k$ or a quadratic field extension of k.

Case 1. $K \cong k \times k$.

In fact, Totaro's question has a positive answer for adjoint groups of type A_n for *any* n in this case. By [KMRT98, Proposition 2.4], $(A, \sigma) \cong (B \times B^{\mathrm{op}}, \varepsilon)$ where B is a central simple algebra of degree $n+1$ over k and ε is the exchange involution on $B \times B^{\mathrm{op}}$. So $G \cong \mathrm{Aut}(A, \sigma) \cong \mathrm{PGL}_1(B)$. Since $H^1(k, \mathrm{GL}_1(B)) = 1$ by Theorem 3.4.3, the short exact sequence

$$1 \to \mathbb{G}_m \to \mathrm{GL}_1(B) \to \mathrm{PGL}_1(B) \to 1$$

of linear algebraic groups over k yields an injection $H^1(k, \mathrm{PGL}_1(B)) \hookrightarrow \mathrm{Br}\, k$ via Theorems 3.2.1 and 3.4.6. A $\mathrm{PGL}_1(B)$–torsor is a Severi–Brauer variety X associated to some central simple algebra C of degree $\deg(B)$ over k, and the injection $H^1(k, \mathrm{PGL}_1(B)) \hookrightarrow \mathrm{Br}\, k$ is given by $[X] \mapsto [C \otimes_k B^{\mathrm{op}}]$. So $\mathrm{ind}([X]) = \mathrm{ind}_{\mathrm{Sch}}(C \otimes_k B^{\mathrm{op}})$, and the claim follows from Theorem 2.1.2.(b).

Case 2.1. K/k is a separable quadratic field extension and G is adjoint of type A_1.

$G \cong \mathrm{Aut}(A, \sigma)$ where A is a quaternion algebra over K and σ is a K/k-involution on A. The following theorem of Albert says that quaternion algebras with K/k–involutions are completely determined by certain quaternion subalgebras over k.

Theorem 5.2.1 (Albert [Alb61, p. 61])**.** *Let Q be a quaternion division algebra over*

K with K/k–involution σ. Then there exists a unique quaternion division subalgebra $Q_0 \subseteq Q$ over k with its canonical (symplectic) involution σ_0 such that $Q \cong Q_0 \otimes_k K$ and $\sigma \cong \sigma_0 \otimes {}^-$ where $\mathrm{Gal}(K/k) = \{\mathrm{id}, {}^-\}$.

So there is a unique quaternion algebra A_0 over k with canonical involution σ_0 such that $(A, \sigma) \cong (A_0, \sigma_0) \otimes_k K$. Given any $[(B, \tau)] \in H^1(k, G)$ with descent $[(B_0, \tau_0)]$, (A, σ) and (B, τ) are completely determined by A_0 and B_0, and for any field extension L/k,

$$\begin{aligned}
[(B,\tau)]_L = 1 \in H^1(L, G_L) &\iff (A,\sigma)\otimes_k L \cong (B,\tau)\otimes_k L \\
&\iff A\otimes_k L \cong B \otimes_k L \text{ and } \sigma\otimes \mathrm{id}_L \cong \tau \otimes \mathrm{id}_L \\
&\iff A_0 \otimes_k L \cong B_0 \otimes_k L \\
&\iff L \text{ splits } A_0 \otimes_k B_0.
\end{aligned}$$

So the field extensions trivializing $[(B, \tau)] \in H^1(k, G)$ are precisely the splitting fields of the central simple algebra $A_0 \otimes_k B_0$. In particular, $\mathrm{ind}_{\mathrm{Sch}}(A_0 \otimes_k B_0) = \mathrm{ind}([B, \tau])$. By Theorem 2.1.2.(b), there is a separable splitting field of $A_0 \otimes_k B_0$ of degree $\mathrm{ind}_{\mathrm{Sch}}(A_0 \otimes_k B_0)$ over k, yielding the result.

Case 2.2. K/k is a separable quadratic field extension and G is adjoint of type A_{2n}.

$G \cong \mathrm{Aut}(A, \sigma)$ where A is a central simple algebra odd degree $2n + 1$ over K. Fix $[(B, \tau)] \in H^1(k, G)$, and let D be the division algebra Brauer–equivalent to $A \otimes_K B^{\mathrm{op}}$. If D is split by some field extension L/k, then so is $A \otimes_K B^{\mathrm{op}}$, in which case $A \otimes_k L \cong B \otimes_k L$. Then either σ and τ become isomorphic over L, in which case we are done, or σ and τ become isomorphic over KL by Lemma 5.1.3. Since every field extension that trivializes $[(B, \tau)]$ necessarily splits D, we see that $\mathrm{ind}([(B, \tau)]) = 2^\theta\, \mathrm{ind}_{\mathrm{Sch}}(A \otimes_K B^{\mathrm{op}})$ where $\theta = 0$ or 1.

Suppose first that $\operatorname{ind}([(B,\tau)]) = \operatorname{ind}_{\mathrm{Sch}}(A \otimes_K B^{\mathrm{op}})$. Since $K^\sigma = K^\tau = k$,

$$\operatorname{cor}(D) = \operatorname{cor}(A)\operatorname{cor}(B^{\mathrm{op}}) = 0 \in \operatorname{Br} k.$$

So D admits a unitary involution δ such that $K^\delta = k$ by Theorem 5.1.1. By Theorem 5.1.2, D contains a maximal subfield E, separable over k, such that $\delta(E) = E$ and $E = KE^\delta$. Since

$$\operatorname{ind}_{\mathrm{Sch}}(A \otimes_K B^{\mathrm{op}}) = \deg(D) = [E : K] = [E^\delta : k]$$

and $D \otimes_k E^\delta \cong D \otimes_K E$ is split, $A \otimes_k E^\delta \cong B \otimes_k E^\delta$. Then $\operatorname{ind}([(B,\tau)])$ is odd as

$$\operatorname{ind}([(B,\tau)]) = \operatorname{ind}_{\mathrm{Sch}}(A \otimes_K B^{\mathrm{op}}) \mid \deg(A \otimes_k B^{\mathrm{op}}) = (2n+1)^2.$$

So there is a field extension L/k of odd degree such that $(A,\sigma) \otimes_k L \cong (B,\tau) \otimes_k L$, hence

$$((A,\sigma) \otimes_k E^\delta) \otimes_{E^\delta} (E^\delta \otimes_k L) \cong ((B,\tau) \otimes_k E^\delta) \otimes_{E^\delta} (E^\delta \otimes_k L).$$

In particular, σ and τ (viewed as involutions on the isomorphic algebras $A \otimes_k E^\delta$ and $B \otimes_k E^\delta$) become isomorphic over $E^\delta \otimes_k L$. Since $[L : k]$ is odd, $E^\delta \otimes_k L$ is isomorphic to a direct product of field extensions of E^δ, at least one of which must have odd degree, else $\dim_{E^\delta}(E^\delta \otimes_k L)$ would be even. Call this extension M. Then σ and τ become isomorphic over M. As $[M : E^\delta]$ is odd, σ and τ become isomorphic over E^δ by Proposition 5.1.4, meaning that $(A,\sigma) \otimes_k E^\delta \cong (B,\tau) \otimes_k E^\delta$. Since $[E^\delta : k] = \operatorname{ind}([(B,\tau)])$, it suffices to take $F = E^\delta$.

Finally, suppose that $\operatorname{ind}([(B,\tau)]) = 2\operatorname{ind}_{\mathrm{Sch}}(A \otimes_K B^{\mathrm{op}})$. Proceed exactly as above to obtain the separable field extension E^δ/k of degree $\operatorname{ind}_{\mathrm{Sch}}(A \otimes_K B^{\mathrm{op}})$ such that $A \otimes_k E^\delta \cong B \otimes_k E^\delta$. By Lemma 5.1.3, $(A,\sigma) \otimes_k KE^\delta \cong (B,\tau) \otimes_k KE^\delta$. Since

$\mathrm{ind}_{\mathrm{Sch}}(A \otimes_K B^{\mathrm{op}})$ is odd,

$$[KE^\delta : k] = [K : k][E^\delta : k] = 2\,\mathrm{ind}_{\mathrm{Sch}}(A \otimes_K B^{\mathrm{op}}) = \mathrm{ind}([(B, \tau)]),$$

and so it suffices to take $F = KE^\delta$, completing the proof. $\square$

Chapter 6

Negative Answers to Totaro's Question

This chapter is largely excerpted from the author's paper with V. Suresh entitled "Totaro's Question on Zero-Cycles on Torsors." We give two classes of smooth connected linear algebraic groups G for which Totaro's question has a negative answer: one over any p-adic field and one over complete discrete valuation fields whose residue field is a global field of characteristic not equal to 2 (e.g., $\mathbb{Q}((t))$). We then use approximation arguments to produce examples over $\mathbb{Q}$, $\mathbb{Q}(t)$, and $\mathbb{Q}_p(t)$. The techniques involved are class-field-theoretic and fundamental to algebraic number theory, and so the reader should refer to Chapters VI and VII of Cassels–Fröhlich [CF67].

In the first case, the ranks of the constructed groups depend on their chosen p-adic ground field, but their non-trivial torsors all have index p and no closed points of degree p. To illustrate this first construction, we give an explicit example of a rank 8 group–a torus, even–over $\mathbb{Q}_2$ satisfying the desired properties. In the second case, we produce groups of rank p for any odd prime p and torsors of index 2 having no closed points of degree 2. Finally, by an observation of Colliot-Thélène, we produce failures of Totaro's question in all higher ranks given each primitive example.

6.1. Examples over p-adic Fields

To produce the first class of examples, we begin with a number of lemmas.

Lemma 6.1.1. *Let k be a field, and let p be a prime not equal to* $\mathrm{char}(k)$*. Then for any $a \in k^\times - (k^\times)^p$, the kernel of the natural homomorphism*

$$k^\times/(k^\times)^p \to k(\sqrt[p]{a})^\times/(k(\sqrt[p]{a})^\times)^p$$

is generated by the class of a.

Proof. Let $\zeta \in k^{\mathrm{s}}$ be a primitive pth root of unity. Then $p \nmid [k(\zeta) : k]$, and so $\ker[k^\times/(k^\times)^p \to k(\zeta)^\times/(k(\zeta)^\times)^p]$ is trivial. So by replacing k with $k(\zeta)$, we can assume that $\zeta \in k$. Then by Kummer theory, the field extension $k(\sqrt[p]{a})/k$ is cyclic with $\mathrm{Gal}(k(\sqrt[p]{a})/k) \cong \langle\sigma\rangle$ where $\sigma(\sqrt[p]{a}) = \zeta^i \sqrt[p]{a}$ for some i coprime to p. Let $b \in k^\times$ such that $b = c^p$ for some $c \in (k(\sqrt[p]{a})^\times)^p$. Then $\sigma(c) = \zeta^j c$ for some j. Since $p \nmid i$, there is some i' such that $ii' \equiv j \bmod p$. Then $\sigma(\sqrt[p]{b}/(\sqrt[p]{a})^{i'}) = \sqrt[p]{b}/(\sqrt[p]{a})^{i'}$, hence $\sqrt[p]{b}/(\sqrt[p]{a})^{i'} \in k$. So $b = a^{i'}d^p$ for some $d \in k^\times$. □

Lemma 6.1.2. *Let k be a field, and let p be a prime not equal to char(k). Then for any finite field extension L/k of degree n, the kernel of the natural homomorphism*

$$k^\times/(k^\times)^p \to L^\times/(L^\times)^p$$

has order at most $p^{\nu_p(n)}$.

Proof. Write $n = p^d m$ where $d = \nu_p(n)$ and $p \nmid m$. We proceed by induction on d. First, suppose that $d = 0$. Then $p \nmid [L : k]$, and so $\ker[k^\times/(k^\times)^p \to L^\times/(L^\times)^p]$ is trivial. Now, suppose that $d \geq 1$. Fix $a \in k^\times - (k^\times)^p$ with $a \in (L^\times)^p$, and let $E = k(\sqrt[p]{a}) \subseteq L$. By Lemma 6.1.1, $\ker[k^\times/(k^\times)^p \to E^\times/(E^\times)^p]$ has order p. Since $[L : E] = p^{d-1}m$, by the induction hypotheses, $\ker[E^\times/(E^\times)^p \to L^\times/(L^\times)^p]$ has order at most p^{d-1}. So the order of $\ker[k^\times/(k^\times)^p \to L^\times/(L^\times)^p]$ is at most p^d. □

Lemma 6.1.3. *If $k/\mathbb{Q}_p$ is a field extension of degree d, then $|k^\times/(k^\times)^p| \geq p^{d+1}$.*

Proof. Let q be the number of elements in the residue field of k. By [Neu99, Proposition II.5.7], we have $k^\times \cong \mathbb{Z} \oplus (\mathbb{Z}/(q-1)\mathbb{Z}) \oplus (\mathbb{Z}/p^a\mathbb{Z}) \oplus \mathbb{Z}_p^d$ for some $a \geq 0$. Then $(\mathbb{Z}/p\mathbb{Z})^{d+1}$ is isomorphic to a subgroup of $k^\times/(k^\times)^p$. □

Now, recall from local class field theory that for any p-adic field k and any $n \geq 1$, there are only finitely many extension of k of degree n–see [Lan94, Proposition II.5.14]–and there is always at least one such extension.

Lemma 6.1.4. *Let k be a p-adic field, and let E/k be a finite field extension containing all of the degree p field extensions of k. Let D be a division algebra of degree p over E. Then for sufficiently large M, there exist a degree M field extension L/k and an $a \in L^\times \setminus (L^\times)^p$ such that $D \otimes_E (E \otimes_k L(\sqrt[p]{a}))$ is split.*

Proof. Let $N = [E : k]$. Let $\rho_1, \ldots, \rho_s$ denote the distinct partitions of N. For each $i = 1, \ldots, s$, let $m_i = \sum_{n \in \rho_i} \nu_p(n)$, and choose any $M > \max_{i=1,\ldots,s} \{m_i\}$. Since k is a p-adic field, there exists a field extension L/k of degree M. Then $E \otimes_k L \cong \prod_{j=1}^{t} L_j$ for some field extensions L_j/L each of degree at most N. In fact, $\sum_{j=1}^{t} [L_j : L] = [E : k] = N$, and so these degrees form a partition of N. For each $j = 1, \ldots, t$, let

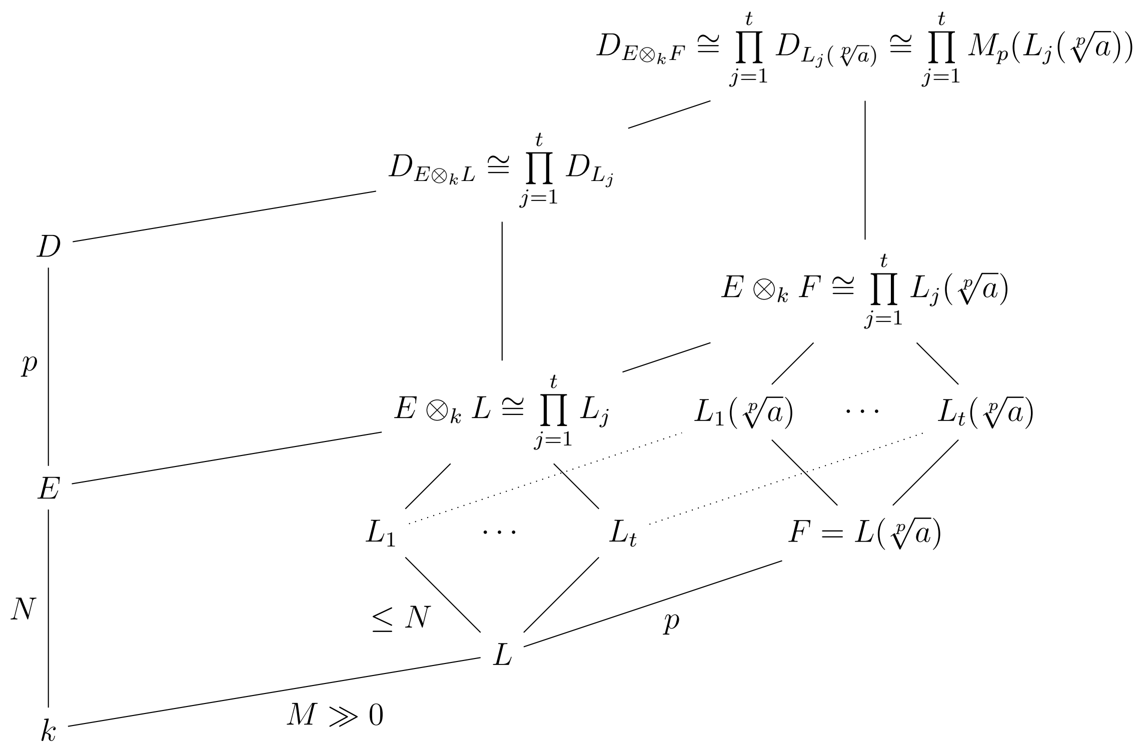
$$H_j = \ker[L^\times/(L^\times)^p \to L_j^\times/(L_j^\times)^p].$$

By Lemma 6.1.2, the order of each H_j is at most $p^{\nu_p([L_j:L])}$. So

$$\sum_{|H_j|>1} |H_j| \leq \prod_{|H_j|>1} |H_j| = \prod_{j=1}^{t} |H_j| \leq \prod_{j=1}^{t} p^{\nu_p([L_j:L])} \leq p^{\sum_{j=1}^{t} \nu_p([L_j:L])} < p^M.$$

Since $|L^\times/(L^\times)^p| \geq p^{M+1}$ by Lemma 6.1.3, there exists some $a \in L^\times \setminus (L^\times)^p$ such that $a(L^\times)^p \notin H_j$ for all j, i.e., such that $a \notin (L_j^\times)^p$ for all j. As each L_j is a p-adic field and D is a central simple algebra of degree p over E, $D \otimes_E L_j(\sqrt[p]{a})$ is split by

[CF67, Corollary VI.1.1]. Let $F = L(\sqrt[p]{a})$. Then $[L : k] = M$, $[F : L] = p$, and $E \otimes_k F \cong \prod_{j=1}^{t} L_j(\sqrt[p]{a})$, hence $D \otimes_E (E \otimes_k F)$ is split. □



Theorem 6.1.5. *Let k be a p-adic field, and let E/k be a finite field extension containing all of the degree p field extensions of k. Then every non-trivial $R_{E/k}(\mathrm{PGL}_p)$-torsor has index p but has no closed point of degree p.*

Proof. Let $G = R_{E/k}(\mathrm{PGL}_p)$, and let X be a non-trivial G-torsor over k. Since $H^1(k, G)$ classifies G-torsors over k by Theorem 3.4.1, X corresponds to an element of $H^1(k, G)$. By Theorem 3.4.7, we have $H^1(k, G) \leftrightarrow H^1(E, \mathrm{PGL}_p)$, the latter of which classifies central simple algebras of degree p over E up to isomorphism by Theorem 3.4.5. Since X is not the trivial torsor, the corresponding degree p algebra D is non-split and is therefore division and of Schur index p.

Recall that for any field extension K/k, $X(K) \neq \varnothing$ if and only if $D \otimes_E (E \otimes_k K)$ is split. By Lemma 6.1.4, there exist degree M_i field extensions L_i/k for sufficiently large M_i and degree p field extensions F_i/L_i such that the algebras $D \otimes_E (E \otimes_k F_i)$ are split.

So each $X(F_i) \neq \varnothing$. Since we can choose the M_i to be arbitrarily large, we can also choose M_1 and M_2 to be coprime. Then $\gcd\{[F_1 : k], [F_2 : k]\} = \gcd\{pM_1, pM_2\} = p$, hence X admits a zero-cycle of degree p. So $\operatorname{ind}(X) = 1$ or $\operatorname{ind}(X) = p$.

If $\operatorname{ind}(X) = 1$, then X has a closed point of some prime-to-p degree m. Then $D \otimes_E (E \otimes_k K)$ is split for some degree m field extension K/k. So $E \otimes_k K \cong \prod_{i=1}^{r} K_i$ for some field extensions $K_1, \ldots, K_q/E$ such that $\sum_{i=1}^{q} [K_i : E] = [K : k] = m$, meaning that $D \otimes_E K_i$ is split for each i. Since $p \nmid m$, $p \nmid [K_{i^*} : E]$ for some i^*. But $D \otimes_E K_{i^*}$ being split contradicts that D has Schur index p. So $\operatorname{ind}(X) = p$.

Now, if K/k is a degree p field extension, then $E \otimes_k K \cong \prod_{i=1}^{r} E_i$ for some field extensions $E_1, \ldots, E_r/E$ such that $\sum_{i=1}^{q} [E_i : E] = [K : k] = p$. Since $K \subseteq E$ by the choice of E, each $[E_i : E] \leq p-1$, else $q = 1$ and $E \otimes_k K$ is a field extension of E. Just as before, each $D \otimes_E E_i$ is division since D has Schur index p. Then $D \otimes_k K$ is not split, hence $X(K) = \varnothing$. So X has no closed points of degree p. $\square$

For an illustrative example, let $k = \mathbb{Q}_2$ and $E = k(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Then $[E : k] = 8$, and E contains every quadratic extension of k. Let $G = R_{E/k}(\mathrm{PGL}_2)$, which evidently has rank 8. By Theorem 6.1.5, every non-trivial G-torsor has index 2 but has no closed point of degree 2. In fact, there is only one non-trivial G-torsor over k: the class of $R_{E/k}(C)$ for the conic $C : (ax^2 + by^2 = z^2) \subseteq \mathbb{P}^2_E$ where $Q = (a, b)_E$ is the unique quaternion division algebra over E by local class field theory. The conic is birational to the variety $N : (N_{E(\sqrt{a})/E}(x + y\sqrt{a}) = b) \subseteq \mathbb{P}^1_E$, a $R^{(1)}_{E(\sqrt{a})/E}(\mathbb{G}_m)$-torsor over E. Let $T = R_{E/k}(R^{(1)}_{E(\sqrt{a})/E}(\mathbb{G}_m))$. Then T is a rank 8 torus birational to G, and so $R_{E/k}(N)$ is a non-trivial T-torsor of index 2 with no closed points of degrees 2.

Corollary 6.1.6. *There exist a semisimple linear algebraic group G (and a torus T) of rank 8 over $\mathbb{Q}$ and a non-trivial G-torsor (and T-torsor) that has index 2 but has no closed points of degree 2.*

Proof. Let $k = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $E_2 = \mathbb{Q}_2(\sqrt{2}, \sqrt{3}, \sqrt{5})$, and $G = R_{E/k}(\mathrm{PGL}_2)$.

Observe that $E \otimes_k \mathbb{Q}_2 \cong E_2$ is a field, and so there is only one valuation ν_2 on E extending the dyadic valuation on k. Fix a real place ν_∞ on E. As in the previous example, there is a unique quaternion division algebra Q_2 over E_2, and furthermore, there is a unique quaternion division algebra Q_∞ over $\mathbb{R} = E_\infty$.

From the Brauer exact sequence ([Pie82, Theorem 18.5])

$$0 \to \operatorname{Br}(E) \to \bigoplus_{\nu \in \Omega} \operatorname{Br}(E_\nu) \to \mathbb{Q}/\mathbb{Z} \to 0$$

where Ω is the set of places of E, we obtain a quaternion division algebra Q over E such that $Q \otimes_E E_2 \cong Q_2$, $Q \otimes_E E_\infty \cong Q_\infty$, and $Q \otimes_E E_\nu$ is split for all $\nu \in \Omega - \{\nu_2, \nu_\infty\}$. If Q were split by any quadratic field extension of k, then Q_2 would be split by a field extension of $\mathbb{Q}_2$ of degree at most 2, which is impossible by Theorem 6.1.5 as Q_2 identifies a non-trivial $R_{E_2/\mathbb{Q}_2}(\mathrm{PGL}_2)$-torsor. So the non-trivial G-torsor X corresponding to Q has no closed points of degree at most 2.

Now, we show that X admits a zero-cycle of degree 2. By Lemma 6.1.4, for sufficiently large M, there is a degree M field extension $L_2/\mathbb{Q}_2$ and an $a \in L_2^\times - (L_2^\times)^2$ such that $Q_2 \otimes_{E_2} (E_2 \otimes_{\mathbb{Q}_2} L_2(\sqrt{a}))$ is split. Then by Krasner's lemma–see [Lan94, p. 44, Section II.2, Corollary]–there is a degree M field extension $L/\mathbb{Q}$ such that $L_2 \cong L \otimes_k \mathbb{Q}_2$. Let $\hat{\nu}_2$ and $\hat{\nu}_\infty$ denote valuations on L extending the dyadic and real valuations on k, respectively. Then L_∞, the completion of L with respect to $\hat{\nu}_\infty$, is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, hence $E_\infty \otimes_{\mathbb{R}} L_\infty \cong \mathbb{R}$ or $\mathbb{C}$.

Now, choose an $\alpha \in L^\times \setminus (L^\times)^2$ that approximates a at $\hat{\nu}_2$ and -1 at $\hat{\nu}_\infty$. Since $Q_2 \otimes_{E_2} (E_2 \otimes_{\mathbb{Q}_2} L_2(\sqrt{a}))$ and $Q_\infty \otimes_{E_\infty} (E_\infty \otimes_{\mathbb{R}} L_\infty(\sqrt{-1}))$ are both split, the Brauer exact sequence yields that $Q \otimes_E (E \otimes_k L(\sqrt{\alpha}))$ is split. So the field extension $L(\sqrt{\alpha})/k$ yields a closed point of degree $2M$ on X. Since M can be taken to be arbitrarily large, X admits a zero-cycle of degree 2. So $\operatorname{ind}(X) = 1$ or $\operatorname{ind}(X) = 2$.

If $\operatorname{ind}(X) = 1$, then X has a closed point of some odd degree m. Then $Q \otimes_E (E \otimes_k$

K) is split for some degree m field extension K/k. Since $[E : k] = 8$, $E \otimes_k K \cong EK$ is a field, and so $[EK : E] = [K : k] = m$. But Q is a quaternion division algebra over E, and $Q \otimes_E EK$ being split contradicts that Q has Schur index 2. So $\mathrm{ind}(X) = 2$. Arguing exactly as in the previous example yields a rank 8 torus T over $\mathbb{Q}$ birational to G and a T-torsor satisfying the desired properties, completing the proof. □

Remark (Colliot-Thélène). If G is a smooth connected linear algebraic group of rank r over a field k and X is a non-trivial G-torsor exhibiting a negative answer to Totaro's question, then for any $n \geq 0$, $X \times_k \mathbb{G}_m^n$ and $X \times_k \mathrm{SL}_2^n$ are non-trivial torsors under $G \times_k \mathbb{G}_m^n$ and $G \times_k (SL_2)^n$, respectively, exhibiting negative answers to Totaro's question. In particular, Corollary 6.1.6 then says that for every $r \geq 8$, there is a semisimple linear algebraic group G (and a torus T) of rank r over $\mathbb{Q}$ such that every non-trivial G-torsor (and T-torsor) has index 2 but has no closed points of degree 2.

6.2. Examples over Other Discrete Valuation Fields

To produce the second class of examples, we exploit an arithmetic feature of "higher-dimensional" fields: the existence of biquaternion division algebras. We begin by constructing quaternion algebras whose corestrictions along some field extensions of odd prime degree are Brauer equivalent to biquaternion division algebras.

Lemma 6.2.1. *Let k be a global field of characteristic $\neq 2$, and let p an odd prime. Let ℓ/k be a separable field extension of degree p. Then there exist a quaternion division algebra Q over k and a $\lambda \in \ell^\times$ such that*

1. *$Q \otimes_k \ell(\sqrt{\lambda})$ is split,*
2. *$N_{\ell/k}(\lambda) \notin (k^\times)^2$, and*
3. *$Q \otimes_k k(\sqrt{N_{\ell/k}(\lambda)})$ is division.*

Proof. Let Ω denote the set of places of k. As a consequence of the Chebotarev Density Theorem–see [Neu99, Theorem VII.13.4]–there are distinct places $\nu, \nu' \in \Omega$

with respective parameters $\pi, \pi' \in k$ that split completely in ℓ into places $\nu_1, \ldots, \nu_p$ and $\nu'_1, \ldots, \nu'_p$. Choose $\theta, \theta' \in k^\times - (k^\times)^2$ such that $\theta \notin (k_\nu^\times)^2$ and $\theta' \notin (k_{\nu'}^\times)^2$. Furthermore, let $\nu'' \in \Omega$ such that $\ell \otimes_k k_{\nu''}$ is a field, and let $\tilde{\nu}''$ be the unique place of ℓ extending ν''. Then $\ell_{\tilde{\nu}''} \cong \ell \otimes_k k_{\nu''}$. Since $[\ell : k]$ is odd, there exists some $\theta'' \in \ell_{\tilde{\nu}''}^\times$ such that $N_{\ell_{\tilde{\nu}''}/k_{\tilde{\nu}''}}(\theta'') \notin (k_{\nu''}^\times)^2$. By approximation, we can choose a $\lambda \in \ell^\times$ that is

(a) close to π (resp. π') at ν_1 (resp. ν'_1),

(b) close to θ (resp. θ') at $\nu_2, \ldots, \nu_{p-1}$ (resp. $\nu'_2, \ldots, \nu'_{p-1}$),

(c) close to $\pi^{-1}\theta^{-(p-2)}$ (resp. $\pi'^{-1}\theta'^{-(p-2)}$) at ν_p (resp. ν'_p), and

(d) close to θ'' at $\tilde{\nu}''$.

By the Brauer exact sequence, there is a quaternion division algebra Q over k such that $Q \otimes_k k_\nu$ and $Q \otimes_k k_{\nu'}$ are division but $Q \otimes_k k_\omega$ is split for every $\omega \in \Omega - \{\nu, \nu'\}$. By (a), (b), and (c), λ is not a square at any ν_i or ν'_j, which means that each $\ell_{\nu_i}(\sqrt{\lambda})/\ell_{\nu_i}$ and each $\ell_{\nu'_j}(\sqrt{\lambda})/\ell_{\nu'_j}$ is a quadratic field extension. Then by [CF67, Corollary VI.1.1], each $Q \otimes_k \ell_{\nu_i}(\sqrt{\lambda})$ and each $Q \otimes_k \ell_{\nu'_j}(\sqrt{\lambda})$ is split.

Now, since $Q \otimes_k k_\omega$ is split for every $\omega \in \Omega - \{\nu, \nu'\}$, $Q \otimes_k \ell(\sqrt{\lambda})$ is split at every place of $\ell(\sqrt{\lambda})$ and is therefore split by the Brauer exact sequence, yielding the first condition. As $N_{\ell_{\tilde{\nu}''}/k_{\tilde{\nu}''}}(\theta'') \notin (k_{\nu''}^\times)^2$, $N_{\ell_{\tilde{\nu}''}/k_{\nu''}}(\lambda) \notin (k_{\nu''}^\times)^2$ by (d). So $N_{\ell/k}(\lambda) \notin (k^\times)^2$, hence the second condition. By (a), (b), and (c), $N_{\ell/k}(\lambda)$ is close to 1 at ν, hence $\sqrt{N_{\ell/k}(\lambda)} \in k_\nu$. Then $Q \otimes_k k_\nu(\sqrt{N_{\ell/k}(\lambda)}) \cong Q \otimes_k k_\nu$ is division, hence so is $Q \otimes_k k(\sqrt{N_{\ell/k}(\lambda)})$, yielding the third condition and completing the proof. □

Proposition 6.2.2. *Let k be a global field of characteristic not equal to 2, let p be an odd prime, let ℓ/k be a separable field extension of degree p, let K be a complete discrete valuation field with residue field k, and let L/K be the unique unramified field extension of degree p with residue field ℓ. Then there exists a quaternion division algebra D over L such that* $\mathrm{ind}_{\mathrm{Sch}}(\mathrm{cor}_{L/K}(D)) = 4$.

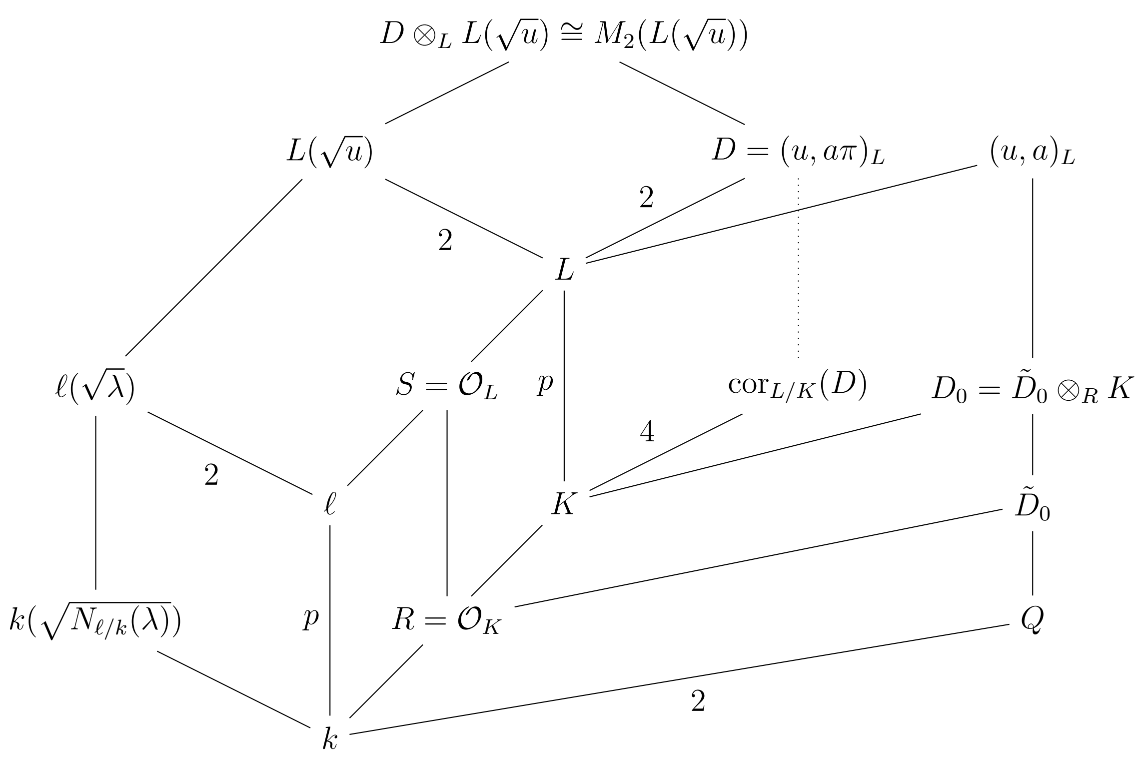
Proof. Let $R \subseteq K$ and $S \subseteq L$ be the rings of integers, let $\pi \in R$ be a parameter, and let Q be a quaternion division algebra over k and $\lambda \in \ell^\times$ as in Lemma 6.2.1. Since

$\mathrm{Br}(k) \cong \mathrm{Br}(R)$–see [Cip77, p. 257, Corollary]–there is a quaternion algebra $\tilde{D}_0$ over R such that $\tilde{D}_0 \otimes_R R/(\pi) \cong Q$. Let $D_0 = \tilde{D}_0 \otimes_R K$. If $u \in S^\times$ is a lift of $\lambda \in \ell^\times$, then since $Q \otimes_k \ell(\sqrt{\lambda})$ is split, so is $D_0 \otimes_K L(\sqrt{u})$. Then $D_0 \otimes_K L = (u, a)_L$ for some $a \in L^\times$ by [GS06, Proposition 1.2.3].

Let $D = (u, a\pi)_L$. Then $[D] = [(u, a\pi)_L] = [(u, a)_L] + [(u, \pi)_L]$ by [GS06, Lemma 1.5.2]. Note that $\mathrm{cor}_{L/K}([D_0 \otimes_K L]) = \mathrm{cor}_{L/K} \circ \mathrm{res}_{L/K}([D_0]) = p[D_0]$ by Lemma 3.3.3. Since p is odd and $\mathrm{cor}_{L/K}([(u, \pi)_L]) = [(N_{L/K}(u), \pi)_K]$ by [CF67, Proposition IV.7.9.(iv)], $\mathrm{cor}_{L/K}([D]) = [D_0] + [(N_{L/K}(u), \pi)_K]$. Noting that D_0 is unramified over R, $N_{L/K}(u) \in R^\times$, and $D_0 \otimes_K K(\sqrt{N_{L/K}(u)})$ is a quaternion division algebra, [FS95, Proposition 1.(3)] yields

$$\begin{aligned}
\mathrm{ind}_{\mathrm{Sch}}(\mathrm{cor}_{L/K}(D)) &= \mathrm{ind}_{\mathrm{Sch}}(D_0 \otimes_K (N_{L/K}(u), \pi)_K) \\
&= [k(\sqrt{N_{\ell/k}(\lambda)}) : k] \cdot \mathrm{ind}_{\mathrm{Sch}}(Q \otimes_k k(\sqrt{N_{\ell/k}(\lambda)})) \\
&= 4,
\end{aligned}$$

as desired. □



Proposition 6.2.3. *Let K be a field, L/K be a separable field extension of prime degree p, and let A be a central simple algebra over L such that $p \nmid \mathrm{ind}_{\mathrm{Sch}}(A)$. Then there exists a field extension F/K such that $p \nmid [F:k]$ and $A \otimes_L (L \otimes_K F)$ is split.*

Proof. Since A is a central simple algebra over L, by Theorem 2.1.2.(c), there exists a finite separable extension E/L such that $A \otimes_L E$ is split . Replacing E by its Galois closure over K, we can assume that E/K is Galois. Let S_p be the p-Sylow subgroup of the Galois group of E/K, and let $F = E^{S_p}$ be the fixed field of S_p. Then $p \nmid [F:K]$ and $[E:F]$ is a power of p. As $[L:K] = p$, $F \subseteq L \otimes_K F \cong LF \subseteq E$. Then $p \nmid [LF:L]$ and $[E:LF]$ is a power of p. Since $A \otimes_L E$ is split and $p \nmid \mathrm{ind}_{\mathrm{Sch}}(A)$, $A \otimes_L LF \cong A \otimes_L (L \otimes_K F)$ is split by Theorem 2.1.2.(a). □

Theorem 6.2.4. *Let k be a global field of characteristic not equal to 2, let ℓ/k be a separable field extension of odd prime degree p, let K be a complete discrete valuation field with residue field k, let L/K be the unramified field extension of degree p with residue field ℓ, and let $G = R_{L/K}(\mathrm{PGL}_2)$. Then there exists a non-trivial G-torsor X such that X has index 2 but has no closed points of degree 2.*

Proof. Let Q be a quaternion division algebra over L as in Proposition 6.2.2. By Theorems 3.4.7 and 3.4.5, $H^1(K, G) \leftrightarrow H^1(L, \mathrm{PGL}_2)$ classifies quaternion algebras over L up to isomorphism. Let X be the non-trivial G-torsor over K given by Q. Then $X(K) = \varnothing$. Let E/K be a quadratic field extension, and suppose that $X(E) \neq \varnothing$. Then $Q \otimes_L (L \otimes_K E)$ is split. In particular, $\mathrm{cor}_{L/K}(Q) \otimes_K E$ is split. Since $[E:K] = 2$, $\mathrm{ind}_{\mathrm{Sch}}(\mathrm{cor}_{L/K}(Q))$ is at most 2 by Theorem 2.1.2, contradicting the choice of Q by Lemma 6.2.1. So X has no closed points of degree 2.

Now, since Q is split over a quadratic field extension of L and $[L:K] = p$ is odd, X has a closed point of degree $2p$. By Proposition 6.2.3, there exists a field extension F/K such that $p \nmid [F:K]$ and $Q \otimes_L (L \otimes_K F)$ is split. Then $X(F) \neq \varnothing$. Since $\mathrm{cor}_{L/K}(Q) \otimes_K F = \mathrm{cor}_{LF/F}(Q \otimes_L LF)$ is split and $\mathrm{ind}_{\mathrm{Sch}}(\mathrm{cor}_{L/K}(Q)) = 4$, $4 \mid [F:K]$

by Theorem 2.1.2.(a). As $p \nmid [F : K]$, X admits a zero-cycle of degree 2. Then arguing as in the proof of Theorem 6.1.5, $\mathrm{ind}(X) = 2$. □

Corollary 6.2.5. *Let k be a global field of characteristic not equal to 2, let ℓ/k be a separable field extension of odd prime degree p, and let K be a complete discrete valuation field with residue field k. Then there exist a torus T of rank p over K and a non-trivial T-torsor X that has index 2 but has no closed points of degree 2.*

Proof. Let $Q = (a, b)_L$ be a quaternion division algebra over L as in Proposition 6.2.2. Then arguing as in the example from Section 6.1, the non-trivial $R_{L/K}(\mathrm{PGL}_2)$-torsor obtained in Theorem 6.2.4 is birational to a non-trivial $R_{L/K}(R^{(1)}_{L(\sqrt{a})/L}(\mathbb{G}_m))$-torsor, which necessarily has index 2 but has no closed points of degree 2. □

Remark. $\mathbb{Q}(t)$ (resp. $\mathbb{Q}_p(t)$) has a discrete valuation ν with residue field a global field of characteristic not equal to 2. Arguing as in Corollary 6.1.6, the constructions of Theorem 6.2.4 and Corollary 6.2.5 over the completion of $\mathbb{Q}(t)$ (resp. $\mathbb{Q}_p(t)$) at ν descend to $\mathbb{Q}(t)$ (resp. $\mathbb{Q}(t)$). So there exist smooth connected linear algebraic groups over $\mathbb{Q}(t)$ and $\mathbb{Q}_p(t)$ for which Totaro's question has a negative answer.

Remark (Colliot-Thélène). If we take $p = 3$ throughout this section, then Theorem 6.2.4 and Corollary 6.2.5 yield semisimple linear algebraic groups and tori, respectively, of rank 3 for which Totaro's question has a negative answer. Arguing as before, we then produce failures of Totaro's question in all ranks at least 3.

Bibliography

[Alb61] A. A. Albert. *Structure of algebras*. Revised printing. American Mathematical Society Colloquium Publications, Vol. XXIV. American Mathematical Society, Providence, R.I., 1961.

[Alb72] A. A. Albert. Tensor products of quaternion algebras. *Proc. Amer. Math. Soc.*, 35:65–66, 1972.

[BFL90] E. Bayer-Fluckiger and H. W. Lenstra, Jr. Forms in odd degree extensions and self-dual normal bases. *Amer. J. Math.*, 112(3):359–373, 1990.

[Bha16] N. Bhaskhar. *R-equivalence and norm principles in algebraic groups*. ProQuest LLC, Ann Arbor, MI, 2016. Thesis (Ph.D.)–Emory University.

[Blu10] M. Blunk. Del Pezzo surfaces of degree 6 over an arbitrary field. *J. Algebra*, 323(1):42–58, 2010.

[BP14] J. Black and R. Parimala. Totaro's question for simply connected groups of low rank. *Pacific J. Math.*, 269(2):257–267, 2014.

[CF67] *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

[Cip77] M. Cipolla. Remarks on the lifting of algebras over Henselian pairs. *Math. Z.*, 152(3):253–257, 1977.

[CTC79] J.-L. Colliot-Thélène and D. Coray. L'équivalence rationnelle sur les points fermés des surfaces rationnelles fibrées en coniques. *Compositio Math.*, 39(3):301–332, 1979.

[EKM08] R. Elman, N. Karpenko, and A. Merkurjev. *The algebraic and geometric theory of quadratic forms*, volume 56 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2008.

[Flo04] M. Florence. Zéro-cycles de degré un sur les espaces homogènes. *Int. Math. Res. Not.*, (54):2897–2914, 2004.

[FS95] B. Fein and M. Schacher. $\mathbf{Q}(t)$ and $\mathbf{Q}((t))$-admissibility of groups of odd order. *Proc. Amer. Math. Soc.*, 123(6):1639–1645, 1995.

[GH06] S. Garibaldi and D. W. Hoffmann. Totaro's question on zero-cycles on G_2, F_4 and E_6 torsors. *J. London Math. Soc. (2)*, 73(2):325–338, 2006.

[GLL13] O. Gabber, Q. Liu, and D. Lorenzini. The index of an algebraic variety. *Invent. Math.*, 192(3):567–626, 2013.

[GSa] R. L. Gordon-Sarney. Totaro's question for adjoint groups of types A_1 and A_{2n}. *to appear in Proc. Amer. Math. Soc.*

[GSb] R. L. Gordon-Sarney. Totaro's question for tori of low rank. *to appear in Trans. Amer. Math. Soc.*

[GS06] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[Jac96] N. Jacobson. *Finite-dimensional division algebras over fields*. Springer-Verlag, Berlin, 1996.

[KMRT98] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits.

[Lan94] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Man72] Yu. I. Manin. *Kubicheskie formy: algebra, geometriya, arifmetika*. Izdat. "Nauka", Moscow, 1972.

[Man86] Yu. I. Manin. *Cubic forms*, volume 4 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, second edition, 1986. Algebra, geometry, arithmetic, Translated from the Russian by M. Hazewinkel.

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Par05] R. Parimala. Homogeneous varieties—zero-cycles of degree one versus rational points. *Asian J. Math.*, 9(2):251–256, 2005.

[Pie82] R. S. Pierce. *Associative algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982. Studies in the History of Modern Science, 9.

[Sch75] W. Scharlau. Zur Existenz von Involutionen auf einfachen Algebren. *Math. Z.*, 145(1):29–32, 1975.

[Sch85] W. Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[Ser] J.-P. Serre. *Galois cohomology*. Springer-Verlag, Berlin. Translated from the French by Patrick Ion and revised by the author.

[Ser62] J.-P. Serre. Cohomologie galoisienne des groupes algébriques linéaires. In *Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962)*, pages 53–68. Librairie Universitaire, Louvain; Gauthier-Villars, Paris, 1962.

[Ser95] J.-P. Serre. Cohomologie galoisienne: progrès et problèmes. *Astérisque*, (227):Exp. No. 783, 4, 229–257, 1995. Séminaire Bourbaki, Vol. 1993/94.

[Spr52] T. A. Springer. Sur les formes quadratiques d'indice zéro. *C. R. Acad. Sci. Paris*, 234:1517–1519, 1952.

[Tot04] B. Totaro. Splitting fields for E_8-torsors. *Duke Math. J.*, 121(3):425–455, 2004.

[Veĭ69] B. Ju. Veĭsfeĭler. Certain properties of singular semisimple algebraic groups over non-closed fields. *Trudy Moskov. Mat. Obšč.*, 20:111–136, 1969.

[Vos65] V. E. Voskresenskiĭ. On two-dimensional algebraic tori. *Izv. Akad. Nauk SSSR Ser. Mat.*, 29:239–244, 1965.

[Vos98] V. E. Voskresenskiĭ. *Algebraic groups and their birational invariants*, volume 179 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1998. Translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ].