ESSENTIAL DIMENSION: A SURVEY. PRELIMIANRY DRAFT, JUNE 27, 2008

ZINOVY REICHSTEIN[†]

ABSTRACT. These notes are written in connection with a five lecture mini-course to be given at a workshop on Essential and Canonical Dimension in Lens, France, June 23-27, 2008. The goal is to give a give an overview and some highlights of the theory of essential dimension. Some of the material in these notes is based on joint work with G. Berhuy, P. Brosnan, J. Buhler, Ph. Gille, A. Vistoli and B. Youssin.

CONTENTS

1. LETURE 1: DEFINITION AND FIRST PROPERTIES

In this lecture I will discuss the definition of essential dimension, and prove some lower bounds based on cohomological invariants and the Tsen-Lang theorem. Most of the results in this section come from [RY00] and [Rei99].

Let k be a base field, K/k be a field extension and q be an n-dimensional quadratic form over K. Let us assume that $\mathrm{char}(k) \neq 2$ and denote the symmetric bilinear form associated to q by b. We would like to know if q can be defined over some smaller field $k \subset K_0 \subset K$. This means that there is a K-basis $e_1, \ldots, e_n$ of K^n such that $b(e_i, e_j) \in K_0$ for every $i, j = 1, \ldots, n$. If we can find such a basis, we will say that q *descends* to K_0 or that q is defined over K_0. It is natural to ask if there is a minimal field K_{min} (with

---

respect to inclusion) to which q descends. The answer to this question is usually "no". For example, the "generic" form

(1.1) $$q(x_1, \ldots, x_n) = a_1 x_1^2 + \cdots + a_n x_n^2$$

over the field $K = k(a_1, \ldots, a_n)$, where $a_1, \ldots, a_n$ are independent variables, has no minimal field of definition; see Exercise 1.1. We will thus modify our question a bit: instead of asking for a minimal field of definition K_0 for q, we will ask for the minimal value of the transcendence degree $\operatorname{tr\,deg}_k(K_0)$ [1]

Note that neither the number we just defined and nor the line of reasoning that led to this definition is in any way particular to quadratic forms. In exactly the same way we can talk about fields of definition of any polynomial in $K[x_1, \ldots, x_n]$, of a K-algebra, of an algebraic variety defined over K, etc. In each case the minimal transcendence degree of a field of definition is an interesting numerical invariant which gives us some insight into the "complexity" of the object in question. This brings us to the following general definition.

We will write Fields_k for the category of field extensions K/k. Let $F \colon \operatorname{Fields}_k \to \operatorname{Sets}$ be a covariant functor.

Let K/k be a field extension. We will say that $a \in F(K)$ *descends* to an intermediate field $k \subseteq K_0 \subseteq K$ if a is in the image of the induced map $F(K_0) \to F(K)$.

The *essential dimension* $\operatorname{ed}(a)$ of $a \in F(K)$ is the minimum of the transcendence degrees $\operatorname{tr\,deg}_k(K_0)$ taken over all fields $k \subseteq K_0 \subseteq K$ such that a descends to K_0.

The essential dimension $\operatorname{ed} F$ of the functor F is the supremum of $\operatorname{ed}(a)$ (respectively, of $\operatorname{ed}(a; p)$) taken over all $a \in F(K)$ with K in Fields_k.

These notions are clearly relative to the base field k, we will write ed instead of ed_k, if the reference to k is clear from the context. To simplify matters, unless otherwise specified, we will assume in the sequel that k is algebraically closed of characteristic 0. Also, to streamline our terminology, the term "functor" will always refer to a functor of the above form, i.e., to a covariant functor from Fields_k to Sets (we will occasionally vary k though).

Example 1.2. Let $F(K) := H^r(K, \boldsymbol{\mu}_n)$. If $\alpha \in H^r(K, \boldsymbol{\mu}_n)$ is non-trivial then by the Serre vanishing theorem, $\operatorname{ed}(\alpha) \geq r$.

Example 1.3. Let $\mathbf{Forms}_{n,d}(K)$ be the set of homogeneous polynomials of degree d in n variables. If $\alpha \in \mathbf{Forms}_{n,d}(K)$ is anisotropic over K then by the Tsen-Lang theorem, $n \leq d^{\operatorname{ed}(\alpha)}$ or equivalently,

$$\operatorname{ed}(\alpha) \geq \log_d(n) \, .$$

On the other hand, clearly, $\operatorname{ed}(\alpha) \leq \binom{n+d-1}{d}$; in particular, $\operatorname{ed} \mathbf{Forms}_{n,d}$ is finite. The exact value of $\operatorname{ed} \mathbf{Forms}_{n,d}$ is not known in general. We will return to this question in the sequel.

---

[1] One can also ask which quadratic forms have a minimal field of definition. To the best of my knowledge, this is an open question.

Of particular interest to us will be the Galois cohomology functors, F_G given by $K \rightsquigarrow \mathrm{H}^1(K, G)$, where G is an algebraic group over k. Here, as usual, $\mathrm{H}^1(K, G)$ denotes the set of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$, in the fppf topology. The essential dimension of this functor is a numerical invariant of G, which, roughly speaking, measures the complexity of G-torsors over fields. We write $\mathrm{ed}\, G$ for $\mathrm{ed}\, F_G$. Essential dimension was originally introduced in this context; see [BuR97, Rei00, RY00]. (The above definition of essential dimension for a general functor F is due to A. Merkurjev; see [BF03].) In special cases this invariant was investigated much earlier. To the best of our knowledge, the first non-trivial result related to essential dimension appeared in in the work of Felix Klein [Kl1884]. In our terminology, Klein showed that the essential dimension of the symmetric group S_5 over $k = \mathbb{C}$, is 2. (Klein referred to this fact as Kroeneker's theorem, so it may go back even further.) The problem of computing the essential dimension of the symmetric group S_n, which remains open to this day for every $n \geq 7$ (cf. Example 2.9), is related to the algebraic form of Hilbert's 13th problem.

The groups of essential dimension zero are the so-called special groups, introduced by Serre and classified by Grothendieck (over an algebraically closed field) in the 1950s. The problem of computing the essential dimension of an algebraic group may be viewed as a natural extension of this theory.

It is easy to see that if $k \subset k'$ is a field extension then

$$(1.4) \qquad\qquad \mathrm{ed}_k(\mathcal{F}) \geq \mathrm{ed}_{k'}(\mathcal{F}) \,.$$

In particular,

$$(1.5) \qquad\qquad \mathrm{ed}_k(G) \geq \mathrm{ed}_{k'}(G)$$

for any k-group G.

Recall that an action of an algebraic group G on an algebraic k-variety X is called *generically free* if X has a dense open subset U such that $\mathrm{Stab}_G(x) = \{1\}$ for every $x \in U(k)$ and *primitive* if G permutes the irreducible components of X.

If K/k is finitely generated then elements of $H^1(K, G)$ can be interpreted as isomorphism classes of generically free primitive G-varieties. If X is a generically primitive G-variety, let us write $[X]$ for its class in $H^1(K, G)$. The essential dimension $\mathrm{ed}\,[X]$ is then the minimal value of $\mathrm{ed}(Y) - \dim(G)$, where the minimum is take over all dominant rational G-equivariant maps $X \dashrightarrow Y$.

An important feature of the functor $H^1(\,*\,, G)$ is the existence of so-called *versal objects*. We briefly recall the following definition.

Definition 1.6. a G-torsor α over a finitely generated field extension K/k is called versal if

(a) it can be represented by a G-torsor $\pi \colon X \to Y$, where Y is an irreducible k-variety and $k(Y) = K$. In other words, α is the restriction of π to the generic point of Y.

(b) Given a closed subvariety $Y_0 \subsetneq Y$ and a G-torsor $\tau \colon T \to \operatorname{Spec}(L)$, there exists an L-point $p \colon L \to Y$ such that p is not contained in Y_0 and τ is the pull-back of π via p:

$$
\begin{array}{ccc}
T & \longrightarrow & X \\
\downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \pi} \\
\operatorname{Spec}(L) & \xrightarrow{\; p \;} & Y \, .
\end{array}
$$

If $\alpha \in H^1(K, G)$ is a versal torsor then $\operatorname{ed}(\alpha) \geq \operatorname{ed}(\beta)$ for any other torsor $\beta \in H^1(L, G)$; cf. Exercise 1.4. In particular, $[V]$ is known to be a versal object for any generically free linear representation V of G. Consequently,

$$(1.7) \qquad\qquad \operatorname{ed}(G) = \operatorname{ed}([V]) \leq \dim(V) - \dim(G) \,. $$

These notes are devoted to the problem of computing $\operatorname{ed}(G)$, and, in particular, bounding this number from below. The simplest approach is to relate $H^1(K, G)$ to the functors in Examples 1.2 or 1.3, using the following simple observation.

Lemma 1.8. *Suppose a morphism of functors $\phi \colon F \to F'$ takes α to β. Then $\operatorname{ed}(\alpha) \geq \operatorname{ed}(\beta)$. In particular, if ϕ is surjective then $\operatorname{ed}(F) \geq \operatorname{ed}(F')$.*

Proof. Obvious from the definition. ♠

Example 1.9. Consider the tautological map $H^1(K, \mathbf{O}_n) \to \mathbf{Forms}_{n,2}$ taking a non-degenerate quadratic form q in n variables to itself. Taken $K = k(a_1, \ldots, a_n)$ and $q = \langle a_1, \ldots, a_n \rangle$, one easily checks that q is anisotropic. Thus $\operatorname{ed}(\mathbf{O}_n) \geq \operatorname{ed}(q) \geq \log_2(n)$.

To get a better lower bound, define $\phi \colon H^1(K, \mathbf{O}_n) \to \mathbf{Forms}_{2^n, 2}$. Let b be the bilinear form on $V = K^n$, associated to q. Then b naturally induces a non-degenerate bilinear form $\wedge^2(b)$ on $\bigwedge^2(V)$ by

$$ \wedge^2(b)(v_1 \wedge v_2, w_1 \wedge w_2) = b(v_1, w_1)b(v_2, w_2) - b(v_1, w_2)b(v_2, w_1) \,. $$

Similarly we define a symmetric bilinear form $\wedge^i(b)$ on $\bigwedge^i(V)$ for every $i = 1, \ldots, n$; adding them all up, we obtain a symmetric bilinear form $\wedge(b)$ on the 2^n-dimensional K-vector space $\bigwedge(V)$. Let $\phi(q)$ be the 2^r-dimensional quadratic form associated to $\wedge(b)$. If

$$ q = \langle a_1, \ldots, a_n \rangle $$

then one easily checks, in the obvious basis of $\bigwedge(V)$, that $\phi(q)$ is the n-fold Pfister form

$$ \phi(q) = \ll a_1, \ldots, a_n \gg \,. $$

We claim that for $K = k(a_1, \ldots, a_n)$ as above, with $a_1, \ldots, a_n$ independent variables, $\phi(q)$ is anisotropic. (We will prove his below.) Example 1.3 now tells us that $\operatorname{ed}(\mathbf{O}_n) \geq \operatorname{ed}(q) \geq n$. This inequality is, in fact, sharp, i.e.,

$$ \operatorname{ed}(\mathbf{O}_n) = n \,. $$

To show that $\mathrm{ed}(\mathbf{O}_n) \leq n$, note that every quadratic form can be diagonalized and hence, descends to a field generated by n elements.

To prove the claim, suppose

$$(1.10) \qquad \sum_{1 \leq i_1 < \cdots < i_r \leq n} a_{i_1} a_{i_2} \ldots a_{i_n} p_{i_1,\ldots,i_r}^2 (a_1, \ldots, a_n) = 0 \,,$$

for some the rational functions $p_{i_1,\ldots,i_r} \in K$. (Here r ranges from 0 to n.) Now consider the valuation $\nu \colon K(a_1, \ldots, a_n) \to \mathbb{Z}^n$ which associates to a polynomial $p(a_1, \ldots, a_n)$ the exponent of its lexicographically largest term. (This valuation extends to all of K in the obvious way: if $p, q \in k[a_1, \ldots, a_n]$ then $\nu(p/q) = \nu(p) - \nu(q)$.). The non-zero terms in the above sum all have different valuations in $\mathbb{Z}^n$, modulo 2. This means that they cannot add up to 0. We conclude that (1.10) is only possible if every $p_{i_1,\ldots,i_r} = 0$. In other words, the Pfister form $\phi(q) = \ll a_1, \ldots, a_n \gg$ is anisotropic, as claimed.

Of course, $\phi(q)$ is, essentially, the nth Stielfel-Whitney class of q. Thus the inequality $\mathrm{ed}(\mathbf{O}_n) \geq n$ can also be deduced from the following observation, due to Serre.

Lemma 1.11. *If G has a non-trivial cohomological invariant $H^1(K, G) \to H^r(K, G)$ then $\mathrm{ed}(G) \geq r$.*

Here is another example.

Example 1.12. $\mathrm{ed}(\boldsymbol{\mu}_n^r) = r$. For the lower bound use the cohomological invariant

$$H^1(K, \boldsymbol{\mu}_n^r) = K^*/(K^*)^n \times \cdots \times K^*/(K^*)^n \to H^r(K, \boldsymbol{\mu}_n)$$

given by $(a_1, \ldots, a_r) \to (a_1) \cup \cdots \cup (a_r)$. For the upper bound note that $\boldsymbol{\mu}_n^r$ has a generically free r-dimensional representation.

Remark 1.13. It is easy to see that if H is a closed subgroup of G then $\mathrm{ed}(G) \geq \mathrm{ed}(H) + \dim(H) - \dim(G)$. In particular, if a finite group contains an abelian subgroup of rank r then $\mathrm{ed}(G) \geq r$. In particular, if G if the symmetric group Sym_n and $H \simeq (\mathbb{Z}/2\mathbb{Z})^{[n/2]}$ is the subgroup generated by the commuting 2-cycles (12), (34), (56), etc. this yields $\mathrm{ed}(S_n) \geq [n/2]$; cf. [BuR97].

Example 1.14. Let $n = p^s$ be a prime power, $a_1, \ldots, a_{2s}$ be independent variables over k, $K = k(a_1, \ldots, a_{2s})$, and

$$A = (a_1, a_2)_p \otimes_K \otimes \cdots \otimes (a_{2s-1}, a_{2s})_p$$

be a tensor product of s symbol algebras of degree p. By definition A is a central simple algebra of degree $n = p^s$; hence, we can identify it with an element of $H^1(K, \mathbf{PGL}_n)$. Since $\mathrm{tr}\,\deg_k(K) = 2s$, we clearly have $\mathrm{ed}(A) \leq 2s$. We claim that, in fact, $\mathrm{ed}(A) = 2s$ and thus $\mathrm{ed}(\mathbf{PGL}_n) \geq 2s$. This is the best (and essentially the only) known lower bound on $\mathrm{ed}(\mathbf{PGL}_n)$, where $n \geq 5$ is a prime power.

To show that $\mathrm{ed}(A) \geq 2s$, consider the morphism of functors

$$\phi\colon H^1(K, \mathbf{PGL}_n) \to \mathbf{Forms}_{n^2, p}$$

given by sending a central simple algebra B to the degree p trace form $x \to \mathrm{Tr}_B(x^p)$. It is now easy to write out $\phi(A)$ explicitly and show that it is anisotropic over K. (The argument here is essentially the same as in the case of the generic Pfister form in Example 1.9.) The inequality $\mathrm{ed}(A) \geq 2s$ now follows from Lemma 1.11 and Example 1.9.

EXERCISES FOR LECTURE 1

Exercise 1.1. Let $a_1, \ldots, a_n$ are independent variables, $K = k(a_1, \ldots, a_n)$ and $q = \langle a_1, \ldots, a_n \rangle$ be as in (1.1). Show that q has no minimal field of definition. I other words, if q descends to some $k \subset K_0 \subset K$ then it also descends to a proper subfield K_1 of K_0 (with $k \subset K_1$).

Hint: Use the fact that $\mathrm{ed}(q) = n$ proved in Example 1.9.

Exercise 1.2. Prove the inequalities (1.4) and (1.5).

Exercise 1.3. Show that notion of versal torsor in Definition 1.6 depends only on α and not on the specific model $X \to Y$.

Exercise 1.4. Show that if $\alpha \in H^1(K, G)$ is versal then $\mathrm{ed}(G) = \mathrm{ed}(\alpha)$.

Exercise 1.5. Prove the inequality $\mathrm{ed}(G) \geq \mathrm{ed}(H) + \dim(H) - \dim(G)$ of Remark 1.13. Here H is a subgroup of G.

Exercise 1.6. Let A be a central simple algebra of degree n over a field K, containing k. We will view A as an element of $H^1(K, \mathbf{PGL}_n)$.

(a) Show that $\mathrm{ed}(A) \geq 2$. (Hint: Use the morphism of functors $H^1(K, \mathbf{PGL}_n) \to \mathbf{Forms}_{n^2, n}$ sending A to its reduced norm.)

(b) Show that equality holds in part (a) if A is cyclic. (The converse to this assertion is an open problem.)

Exercise 1.7. Modify the argument of Example 1.9 to show that $\mathrm{ed}(\mathbf{SO}_n) = n - 1$ for any $n \neq 2$. What happens if $n = 1$?

Hint: Recall that $H^1(K, SO_n)$ is the set of non-degenerate quadratic forms q of discriminant 1 on $V = K^n$. Show that the quadratic form

$$\wedge^0(q) \times \cdots \times \wedge^{[(n-1)/2]}(q)$$

is anisotropic Consider the cases where n is even and odd separately.

Exercise 1.8. Prove the inequality $\mathrm{ed}(\boldsymbol{\mu}_n^r) \geq r$ of example 1.12 by constructing a morphism of functors

$$H^1(K, \boldsymbol{\mu}_n^r) \to \mathbf{Forms}_{n^r, n}(K)$$

whose image contains an anisotropic form.

2. Lecture 2: Essential dimension at p

In this lecture I will introduce essential dimension at a prime p and discuss the relationship between essential dimension and essential dimension at p in a boader context. My main point is that some problems in Galois cohomology are sensitive to prime-to-p field extensions and some aren't. Loosely speaking, I will call such problems type 2 and type 1, respectively. Type 2 problems tend to be difficult; conversely, under closer examination many open problems turn out to be of type 2. I find this dichotomy quite useful in thinking about problems in Galois cohomology, including those involving essential dimension. I should warn you however, that this section is mostly "metamathematical"; there will be very few specific results here.

In the previous section we considered several examples where we showed that

$$\mathrm{ed}(\alpha) \geq d$$

for certain functors F, certain $\alpha \in F(K)$ and certain positive integers d. A closer look at these arguments reveals that they all prove a bit more. Namely, in each case there is a prime p (sometimes more than one), and our argument shows that, in fact $\mathrm{ed}(\alpha_L) \geq d$, for every finite field extension L/K whose degree is not divisible by p. (In the sequel we will refer to such L/K as prime-to-p extensions.) For instance, let us briefly return to Example 1.9, where we considered the quadratic form $q = \langle a_1, \ldots, a_n \rangle$ defined over the field $K = k(a_1, \ldots, a_n)$, (where $a_1, \ldots, a_n$ are independent variables over k) and showed that $\mathrm{ed}(q) \geq n$. We did this by exhibiting a morphism of functors

$$\phi \colon H^1(K, O_n) \to \mathbf{Forms}_{2^n, 2}(K)$$

and showing that $\phi(q)$ is anisotropic. But then $\phi(q)$ is, in fact, anisotropic over any odd degree field extension L of K. This is a general fact, due to Springer, but in this case, it follows directly from our method of proof.

(The point of sidestepping Springer's theorem here is that the same argument can be applied to the degree p trace form $x \mapsto \mathrm{Tr}_B(x^p)$ in Example 1.14. There is no analogue of Springer's theorem for forms of degree ≥ 3; however, the same argument that shows that the degree trace form is anisotropic over K also shows that it is anisotropic over any field extension L/K of degree prime to p.)

Let us now formalize these observations in the following definition.

Definition 2.1. Let F be a functor and $a \in F(K)$ for some field K/k. The essential dimension $\mathrm{ed}(a; p)$ of a at a prime integer p is defined as the minimal value of $\mathrm{ed}(a_L)$, as L ranges over all finite field extensions L/K such that p does not divide the degree $[L : K]$.

The essential dimension $\mathrm{ed}(F; p)$ is then defined as the maximal value of $\mathrm{ed}(a; p)$, as K ranges over all field extensions of k and a ranges over $F(K)$.

As usual, in the case where $F = H^1(K, G)$ for some algebraic group G defined over k, we will write $\mathrm{ed}(G; p)$ in place of $\mathrm{ed}(F; p)$.

The following lemma summarizes several basic properties of essential dimension at p.

Lemma 2.2. *(a) If $\alpha \in F(K)$ and L/K is a prime-to-p field extension the $\mathrm{ed}(\alpha_L; p) = \mathrm{ed}(\alpha; p)$.*

(b) $\mathrm{ed}(\alpha; p) = \mathrm{ed}(\alpha_{K^p})$ where K^p/K is the prime-to-p-closure of K.

(c) If Γ is a finite group then $\mathrm{ed}(\Gamma; p) = \mathrm{ed}(\Gamma_p; p)$, where Γ_p is a Sylow p-subgroup of Γ.

(d) Suppose G is a semisimple group then $\mathrm{ed}(G; p) \neq 0$ if and only if p is an exceptional prime of G.

Proof. (a), (b) and (c) follow directly from the definition. (d) is a consequence of the following theorem due to Tits: for every $\alpha \in H^1(K, G)$ is split by a finite field extension L/K such that the only prime divisors of $[L : K]$ are the exceptional primes of G; cf. [Se95]. ♠

As we noted at the beginning of this lecture, the arguments we used in Examples 1.9, 1.12 and 1.14 actually show that in fact, $\mathrm{ed}(O_n; 2) = n$, $\mathrm{ed}(\boldsymbol{\mu}_p^r; p) = r$ and $\mathrm{ed}(\mathbf{PGL}_{p^s}; p) \geq 2s$.

The same is true of almost all existing methods for computing lower bounds on $\mathrm{ed}(F)$ and, in particular, on $\mathrm{ed}(G)$. In those cases where these methods apply, and yield an inequality of the form $\mathrm{ed}(F) \geq d$, a slightly modification of the same argument usually yields $\mathrm{ed}(F; p) \geq d$ for a suitable prime p. If one is lucky, one can then explicitly show that $\mathrm{ed}(F) \leq d$ and thus $\mathrm{ed}(G; p) = \mathrm{ed}(G) = d$. If no such upper bound is available, one is usually out of luck; the "gap" between the best known lower bound on $\mathrm{ed}(F; p)$ and the best known upper bound on $\mathrm{ed}(F)$ is usually very hard to close by any existing method. The following definition will enable us to discuss this phenomenon in more formal terms.

Let $F\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a functor we want to study. By a *property* of elements of F we shall mean a collection of maps $f = \{f_K\colon F(K) \to S\}$ for a fixed set S. Note that f_K is not assumed to be functorial in K.

Our terminology is based on the case where S is the set of two elements, say $S = \{0, 1\}$ or where 1 stands for "Yes" and 0 stands for "No". In this case we think of $\alpha \in F(K)$ as having property f if and only if $f_K(\alpha) = 1$. For example, if $F(K) = H^1(K, \mathbf{PGL}_n) =$ central simple algebras of degree n over K, we can think of the properties of being a division algebra or of being cyclic or of being a crossed product in this way. For $F(K) = H^1(K, \mathbf{O}_n)$ $=$ non-degenrate quadratic forms on K^n, some of the interesting properties are: being anisotropic, being a Pfister form, being in a given power $I^d(K)$ of the fundamental ideal.

In other cases S can have more than two elements, say S could be the set $\mathbb{N}$ of non-negative integers. For such S one could, for example, define $f_K(\alpha) = \mathrm{ed}(\alpha)$.

Given a prime integer p, we will say that f is *of type* 1, relative to a prime p, if $f_K(\alpha) = f_L(\alpha_L)$ for every $\alpha \in F(K)$ and every finite field

extension L/K of degree prime to p. Informally speaking, this means that f is insensitive to prime-to-p field extensions. Sometimes, if the reference to the prime p is clear, we will not mention it explicitly and simply say that property f is of type 1.

Example 2.3. Let $F = H^1(K, \mathbf{PGL}_n)$ and $S = \{0, 1\}$, as above, and $n = p^r$ is a prime power. Then the property of being a division algebra is of type 1, relative to p.

Example 2.4. Let $F(K) = H^1(K, \mathbf{O}_n)$, $S = \mathbb{N}$, and $f_K(q) = $ Witt index of q. By a theorem of Springer, this property is of type 1, relative to the prime $p = 2$.

If we take $S = \{0, 1\}$ and take f to be the property of being a Pfister form then f is again of type 1 relative to any prime $q \neq 2$, by a theorem of Rost [Rost99].

I will refer to problems concerning type 1 properties as *type 1 problems*. If the problem we are intereted in concerns a property $f = \{f_K\}$ which is not of type 1, we can often consider the "associated" (cruder) type 1 property f^p. If S is well ordered, we define $f_K^p(\alpha)$ to be the minimal value of $f_L(\alpha_L)$ over all prime-to-p field extensions L/K. We can then replace problems of the form "Show that $f_K(\alpha) \leq d$" by the type 1 problem "Show that $f_K^p(\alpha) \leq d$" or equivalently, "Show that $f_L(\alpha_L) = d$ for some prime-to-p extension L/K". I will refer to such modified questions as the *associated type 1 problems* and to the property f^p as the *associated type 1 property*.

For example, if $f_K(\alpha) = \mathrm{ed}(\alpha)$ then $f_K^p(\alpha) = \mathrm{ed}(\alpha; p)$.

Now suppose we have a problem of the form "Show that $f_K(\alpha) = d$" for a particular $\alpha \in F(K)$ (or some α or every α). If the associated type 1 problem is solved (or assumed or trivial) for every p then I will refer to this questions as a type 2 problem and to the property f as a *type 2 property*.

Observation 2.5. *Most existing methods apply to type 1 problems only. For this reason type 2 problems tend to be hard. Many long-standing open problems in Galois cohomology and related areas are of type 2.*

This observation is a bit vague, but I have found it to be quite useful in thinking about a whole range of problems in Galois cohomology and related areas. Here are some examples.

Example 2.6. The crossed product problem. Recall that a central simple algebra A/K of degree n is a crossed product if it contains a commutative Galois subalgebra L/K of degree n. For a number of years it was not known whether every central simple algebra is a crossed product. For notational convenience, we will restrict our attention to the case where $n = p^r$ is a prime power; the general case reduces to this one by the primary decomposition theorem. In 1972 Amitsur [Am72] showed that a "generic division algebra $U(n)$ of degree n is not a crossed product. For $r = 1, 2$ the question is still open.

For $r = 1$ this is the famous *cyclicity conjecture* of Albert. This problem
is of type 2, in the sense that for every degree p algebra A/K, there exists
a field extension L/K of degree dividing $p - 1$ such that A_L is cyclic; see
Exercise 2.2.

Rowen and Saltman [RS92] showed that the same is true for $r = 2$; any
central simple algebra A of degree p^2 becomes a crossed product after a
prime-to-p extension of the center. Moreover, in the same paper they explain
that Amitsur's argument can be modified to show that, in fact, $UD(p^r)_L$ is a
non-crossed product for any prime-to-p extension L of the center of $\mathrm{UD}(p^r)$.

In summary, the remaining open cases of the crossed product problem (for
algebras of degree p and p^2) are of type 2. The associated type 1 problem
has been completely solved by Amitsur and Rowen-Saltman. (Note that the
only relevant prime is here p; the associated type 1 problem relative to any
other prime is trivial).

Example 2.7. The torsion index. Let F be a functor from Fields to the
category of marked sets. The torsion index n_α of $\alpha \in H^1(K, G)$ is defined as
the gcd of the degrees $[L : K]$, where L ranges over all finite splitting fields
L/K (i.e., α_L is split). The torsion index of F is then the least common
multiple of n_α taken over all K and all $\alpha \in F(K)$.

In the case where $F(K) = H^1(K, G)$ the torsion index was introduced by
Grothendieck and is denoted by n_G. One can show that $n_G = n_{\alpha_{versal}}$, where
$\alpha_{versal} \in H^1(K_{versal}, G)$ is a versal G-torsor. One can show, using a theorem
of Tits [Se95], that the prime divisors of n_G are precisely the exceptional
primes of G. The problem of computing n_G and more generally, of n_α for
$\alpha \in H^1(K, G)$ can thus be rephrased as follows. Given an exceptional prime
p for G, find the highest exponent d_p such that p^{d_p} divides $[L : K]$ for every
splitting extension L/K. It is easy to see that this is a type 1 problem; d does
not change if we replace α by $\alpha_{K'}$, where K'/K is a prime-to-p extension.
This problem has been solved (for every simple groups G and $\alpha = \alpha_{versal}$)
by Tits and Totaro; cf. [Ti92, To05$_1$, To05$_2$].

The related type 2 problem, of finding the possible values of $e_1, \ldots, e_r$
such that α_{versal} is split by a field extension L/K of degree $p_1^{e_1} \ldots p_r^{e_r}$, where
$p_1, \ldots, p_r$ are the exceptional primes for G, remains open. This type 2
question is particularly natural for those G with only one exceptional prime,
e.g., for $G = \mathbf{Spin}_n$.

Example 2.8. The following open question is due to Serre [Se95, §2.4].

*Suppose $\alpha \in H^1(K, G)$ is split by finite field extensions $L_1, \ldots, L_n$ of k
such that the degrees $[L_i : K]$ have no common prime factors. Prove that α
is split (or give a counterexample).*

This is a "pure type 2" question in the following sense. The associated
type 1 problem is as follows: Given a prime p, show that $\alpha_L = 1$ for some
prime-to-p extension L/K. But this is trivial, since we are assuming that
L_i/K is a prime-to-p extension for some i.

Example 2.9. One of the most interesting open problems about essential dimension is to find the exact value of $\operatorname{ed}(S_n)$ for $n \geq 7$. We know that $\operatorname{ed}(S_n) \geq [n/2]$ for all n and $\operatorname{ed}(S_n) \leq n - 3$ for $n \geq 5$; cf. Exercise 2.9 and [BuR97]. This is a type 2 problem.

The associated type 1 problem is completely solved: $\operatorname{ed}(S_n; p) = [n/p]$ for every prime integer p; cf. Exercise 2.1.

Example 2.10. Another important open problem is to compute $\operatorname{ed}(\mathbf{PGL}_p)$. This is again a type 2 problem. Indeed, as we mentioned in Example 2.6. every central simple algebra of degree p becomes cyclic after a prime-to-p extension. Hence, $\operatorname{ed}(\mathbf{PGL}_p; p) = 2$.

If one can show that $\operatorname{ed}(\mathbf{PGL}_p) > 2$, this would disprove Albert's cyclicity conjecture.

Example 2.11. Computing the canonical dimension $\operatorname{cdim}(G)$ of an algebraic group G is a largely open type 2 problem. The p-canonical dimension $\operatorname{cdim}_p(G)$ has been computed by Karpenko-Merkurjev [KM06] and Zainoulline [Zai07].

Exercises for Lecture 2

Exercise 2.1. Show that $\operatorname{ed}(\operatorname{Sym}_n; p) = [n/p]$ for every prime integer p.

Hint: For the lower bound use the argument of Remark 1.13. For the upper bound show that a Sylow p-subgroup of Sym_n has a linear representation of dimension $[n/p]$, then appeal to the inequality (1.7).

Exercise 2.2. Let A/K be a division algebra of degree n. Show that for any prime factor p of n there exists a finite field exension L/K of degree dividing $n!/p$ such that $A \otimes_K L$ is cyclic.

3. Lecture 3. Finite abelian subgroups

In this section we will discuss lower bounds on $\operatorname{ed}(G)$ related to non-toral finite abelian subgroups of G; this material is based primarily on [RY00] and [GR07].

A key role will be played by the following result from [RY00].

Theorem 3.1. *Suppose k is an algebraically closed base field and A is an abelian group such that $\operatorname{char}(k)$ does not divide $|A|$. Let $f \colon X \dashrightarrow Y$ be a rational map of A-varieties. If X has a smooth A-fixed point and Y is complete then T has an A-fixed point.*

Proof. (Kollar-Szabo [RY00]). We argue by induction on $\dim(X)$. The base case, $\dim(X) = 0$ is trivial.

For the induction step, let $X' \to X$ be the blow up of a smooth A-fixed point $x \in X$; denote the exceptional divisor by $E \simeq \mathbb{P}(T_x(X)))$, where $T_x(X)$ is the tangent space to X and x. Diagonalizing the A-action on $T_p(X)$, we see that E has A-fixed points.

We can now think of f as a rational map $X' \dashrightarrow Y$. Since X' is smooth at every point of E, E is a divisor and Y is complete, we conclude that f restricts to an A-equivariant map $E \dashrightarrow Y$. Since $\dim(E) = \dim(X) - 1$, we see that Y has an A-fixed point by our induction assumption.   ♠

In the sequel, A will be a finite abelian subgroup of a larger algebraic group G. Let us start with the "toy" case where G is finite. The following inequality is immediate from Example 1.12 but the argument below will carry over in greater generality.

Corollary 3.2. *Let G be a finite group and A be an abelian subgroup. If* $\mathrm{char}(k) = 0$ *then* $\mathrm{ed}_k(G) \geq \mathrm{rank}(A)$.

Proof. Let V is a generically free G-representation. It suffices to show that if there exists a G-compression $V \dashrightarrow X$ then $\dim(X) \geq \mathrm{rank}(A)$. We may assume without loss of generality that X is smooth and projective. By the Going Down Theorem 3.1, since V has a smooth A-fixed point (namely, the origin), so does X. Thus $\dim(X) \geq \mathrm{rank}(A)$, as claimed.   ♠

The above argument contains the germ of the proof of the following inequality conjectured by Serre and proved in [GR07]. An earlier version of this theorem appeared in [RY00] and was refined in [CS06].

Theorem 3.3. *If G is connected, A is a finite abelian subgroup of G, and* $\mathrm{char}(k)$ *does not divide $|A|$ then* $\mathrm{ed}(G) \geq \mathrm{rank}(A) - \mathrm{rank}\, C_G^0(A)$.

Here by $\mathrm{rank}(A)$ we mean the minimal integer r such that A can be written as a direct product of r cyclic groups. On the other hand, by $\mathrm{rank}\, C_G^0(A)$ we mean the dimension of the maximal torus of the connected group $C_G^0(A)$.

Note that if A is contained in a torus T then $C_G^0(A)$ contains T, and the inequality of Theorem 3.3 becomes vacuous. We will be primarily interested in so-called non-toral abelian subgroups. These have come up in many different contexts, starting with the work of Borel in the 1950s. The first indication that there is a connection with essential dimension comes in the form of the following theorem:

Theorem 3.4. *Let G be a linear algebraic group over an algebraically closed field of characteristic 0. The following conditions on a prime p are equivalent. are equivalent.*

  (a) Every finite abelian subgroup of G is toral,

  (b) G is special, i.e., $H^1(K, G) = \{1\}$ for every K/k,

  (c) $\mathrm{ed}(G) = 0$.

The equivalence of (b) and (c) is easy; see Exercise 3.1 below. The equivalence of (a) and (b) is an old result of Steinberg [St75]. Let me prove (b) $\Longrightarrow$ (a) using the Going Down Theorem 3.1.

Assume (b) holds and let A be a finite abelian subgroup of G. Suppose V is a finite-dimensional generically free linear representation of G. By (b),

the torsor defined by the G-action on a dense open subset of V is split. In other words, V is G-equivariantly birationally isomorphic to $G \times Z$ for some algebraic variety Z. Hence, there is a G-equivariant map $V \dashrightarrow G$ and thus a G-equivariant rational map $V \dashrightarrow G/B$. Since G/B is complete, the Going Down Theorem tells us that G/B has an A-fixed point. In other words, A lies in a Borel subgroup of G and hence, in a maximal torus of G, as claimed. ♠

To convey the flavor of the proof of Theorem 3.3 I will make the following additional assumptions: $\mathrm{char}(k) = 0$ and $C_G(A)$ is finite. The conclusion then simplifies to $\mathrm{ed}(G) \geq \mathrm{rank}(A)$. In this form the theorem is proved in [RY00] but I will give a much simplified argument here.

It suffices to show the following.

Proposition 3.5. *Suppose G is a connected linear algebraic group and Y is a generically free G-variety with $\mathrm{tr} \deg_k k(Y)^G = d$. Then Y has a smooth projective birational model $\overline{Y}$ with the following property: if $\overline{Y}$ has an A-fixed point, for some finite abelian subgroup $A \subset G$ satisfying $|C_G(A)| < \infty$ then $d \geq \mathrm{rank}(A)$.*

Indeed, suppose the proposition is established. Let V be a generically free G-variety, $V \dashrightarrow Y$ be a G-compression and $\mathrm{tr} \deg_k k(Y)^G = d$. Need to show that $d \geq \mathrm{rank}(A)$. Replace Y by the model whose existence is asserted by the proposition. The Going Down Theorem tells us that Y has an A-fixed point. Thus by the proposition $d \geq \mathrm{rank}(A)$, as claimed.

To prove the proposition, we use the following result of Chernousov-Gille-R.: there exists a finite subgroup $S \subset G$ such that the map $H^1(K, S) \to H^1(K, G)$ is surjective for every K/k. In other words, Y is birationally isomorphic to $G \times^S Z$, where Z is a faithful S-variety.

Now the birational model we are interested in is

$$\overline{Y} := \overline{G} \times^S \overline{Z},$$

where $\overline{Z}$ is a smooth projective model for Z (as an S-variety) and $\overline{G}$ is a so-called "wonderful" (or "regular") compactification of G.

Recall that $G \times G$ acts on G, extendind the left and right G-action on itself, that $\overline{G} \smallsetminus G$ is a normal crossing divisor $D_1 \cup \cdots \cup D_r$, where each D_i is irreducible, and the intersection of any number of D_i is the closure of a single $G \times G$-orbit in $\overline{G}$. The compactification $\overline{G}$ has many wonderful properties; the only one we will need is the following.

Fact 3.6. *For every $x \in \overline{G}$, $P = \mathrm{pr}_1(\mathrm{Stab}_{G \times G}(x))$ is a parabolic subgroup of G. Here p_1 is projection to the first factor. Moreover, $P = p_1(\mathrm{Stab}_{G \times G}(x))$ equals all of G if and only if $x \in G$; otherwise, P is a proper parabolic in G.*

For a proof, see [Br98, Proposition A1].

We will now show that $\overline{Y}$ has the property asserted in the Proposition. Here $d = \dim(Z)$, so we need to show that if $\dim(Z) \geq \mathrm{rank}(A)$. It suffices to prove that S contains a conjugate A' of A, and A' has a fixed point in $\overline{Z}$.

We know that $\overline{Y}$ has an A-fixed point in $\overline{Y}$. Denote this point by $[x, \overline{z}]$ for some $x \in \overline{G}$ and $\overline{z} \in \overline{Z}$. That is, $[ax, \overline{z}] = [x, \overline{z}]$ in $\overline{Y}$. Equivalently,

$$(3.7) \qquad \begin{cases} ax = xs^{-1} \\ sz = z \end{cases}$$

for some $s \in S$. In other words, for every $a \in A$, there exists an $s \in \mathrm{Stab}_S(z)$ such that $(a, s) \in \mathrm{Stab}_{G \times G}(x)$. Equivalently, the image of the natural projection

$$p_1 \colon \mathrm{Stab}_{G \times G}(x) \to G$$

contains A. Since we are assuming $C_G^0(A)$ is finite, A cannot be contained in any proper parabolic subgroup of G. Thus $x \in G$. Now (3.7) tells us that $x^{-1} A x \subset \mathrm{Stab}_S(z)$, as desired.   ♠

Corollary 3.8. *(a)* $\mathrm{ed}(\mathbf{SO}_n) \geq n - 1$ *for any $n \geq 3$.*

(b) $\mathrm{ed}(\mathbf{PGL}_{p^s}) \geq 2s$.

(c) $\mathrm{ed}(\mathbf{Spin}_n) \geq \begin{cases} [n/2] \text{ for any } n \geq 11, \\ [n/2] + 1 \text{ if } n \equiv -1, \, 0 \text{ or } 1 \text{ modulo } 8. \end{cases}$

(d) $\mathrm{ed}(G_2; 2) \geq 3$.

(e) $\mathrm{ed}(F_4; 2) \geq 5$.

(d) $\mathrm{ed}(F_4) \geq 5$.

(e) $\mathrm{ed}(E_6^{sc}) \geq 4$. *Here E_6^{sc} denotes the simply connected group of type E_6 over k.*

(f) $\mathrm{ed}(E_7^{sc}) \geq 7$. *Here E_7^{sc} denotes the simply connected group of type E_7 over k.*

(g) $\mathrm{ed}(E_7^{ad}) \geq 8$. *Here E_7^{ad} denotes the adjoint E_7.*

(h) $\mathrm{ed}(E_8) \geq 9$.

Each of these inequalities is proved by exhibiting a non-toral abelian subgroup $A \subset G$ whose centralizer is finite; the details are worked out in [RY00] [2].

For example, in part (a) we can take $A \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}$ to be the subgroup of diagonal matrices of the form

$$(3.9) \qquad \begin{pmatrix} \epsilon_1 & 0 & \ldots & 0 \\ 0 & \epsilon_2 & \ldots & 0 \\ \multicolumn{4}{c}{\ldots\ldots\ldots\ldots} \\ 0 & 0 & \ldots & \epsilon_n \end{pmatrix} \quad \text{where each } \epsilon_i = \pm 1 \text{ and } \epsilon_1 \cdot \ldots \cdot \epsilon_n = 1.$$

---

[2] In part (c) only the second line is worked out in [RY00]. The first line was first noticed by Chernousov and Serre [CS06] who proved it by a different method. I later noticed that it can be deduced from Theorem 3.3 as well; the finite abelian subgroups one uses here can be found in [Woo89].

Exercises for Lecture 3

Exercise 3.1. Show that conditions (a) and (b) of Therem 3.4 are equivalent.

Exercise 3.2. Consider a faithful action of a finite abelian group A on an irreducible algebraic variety X, defined over a field k. Assume $\mathrm{char}(k)$ does not divide $|A|$. If A fixes a smooth k-point in X then $\dim(X) \geq \mathrm{rank}(A)$.

Exercise 3.3. Complete the proof of Corollary 3.8(a) by showing that the subgroup A defined in (3.9) has finite centralizer in $\mathbf{SO}_n$.

Exercise 3.4. Deduce the inequality $\mathrm{ed}(\mathbf{PGL}_4) \geq 4$ from Theorem 3.3. (A similar argument proves the more general assertion of Corollary 3.8(b).)

4. Lecture 4. Essential dimension of homogeneous forms

We now return to the question posed in Example 1.3: What is the essential dimension of the functor $\mathbf{Forms}_{n,d}$? Recall that this functor associates to a field K the set of homogeneous polynomials in n variables with coefficients in K, up to equivalence. A related natural question is what is the essential dimension of the functor $\mathbf{Hypsurf}_{n,d}$ where $\mathbf{Hypsurf}_{n,d}(K)$ is the set of hypersurfaces in $\mathbb{P}_K^{n-1}$, i.e., the set of homogeneous polynomials of degree d in n variables, with coefficients in K, up to coordinate changes and scalar multiplication.

We have considered the case where $d = 2$. If we replace $\mathbf{Forms}_{n,2}$ by the subfunctor of non-singular quadratic forms, (which does not change the essential dimension), it will become isomorphic to the Galois cohomology functor $H^1(K, \mathbf{O}_n)$. Informally speaking, Galois cohomology functors F have trivial "geometric moduli spaces". In other words, $F(\overline{K})$ is a single point for any algebraically closed field $\overline{K}$, and the "complexity" of F (some aspects of which are measured by its essential dimension) is entirely "arithmetic". At the other extreme, there are "purely geometric" functors $X \colon K \mapsto X(K)$, where X is an algebraic variety. A simple but important observation due to Merkurjev [BF03] is that the essential dimension of this functor is $\dim(X)$; cf. Exercise 4.2.

For larger d, the functor $\mathbf{Forms}_{n,d}$ is in neither category, it has a non-trivial geometric moduli space (at least if one restricts to the open subset of $\mathbb{A}^N$ of smooth forms). In other words, if a rational function α of the coefficients of

$$f(x_1, \ldots, x_n) \in \mathbf{Forms}_{n,d}(K)$$

is left invariant by the action of $\mathbf{GL}_n$ then whenever f descends to a subfield $K_0 \subset K$, then $\alpha \in K_0$. For this reason,

$$\mathrm{ed}(\mathbf{Forms}_{n,d}) \geq \mathrm{tr}\deg_k k(\mathbb{A}^N)^{\mathbf{GL}_n} = N - n^2 \,,$$

where $N = \binom{n+d-1}{d}$. Here $N - n^2$ is the "geometric contribution" to essential dimension. However, the functors $\mathbf{Forms}_{n,d}$ and $\mathbf{Hypsurf}_{n,d}$ also has some

"arithmetic" complexity, which accounds for the fact that $\mathrm{ed}(\mathbf{Forms}_{n,d})$ may actually be strictly larger than $N - n^2$.

In fact, "most" functors are neither "purely arithmetic" nor "purely geometric". This phenomenon is most naturally understood in terms of fibered categories and more specifically algebraic (Artin) stacks. In these notes I will try to avoid stack-theoretic terminology; keep in mind however, that it will be "lurking in the background".

Unfortunately, I do not know what $\mathrm{ed}(\mathbf{Forms}_{n,d})$ and $\mathrm{ed}(\mathbf{Hypsurf}_{n,d})$ are in general. In order to say something interesting I need to modify them by considering only smooth forms. Denote the corresponding functors by $\mathbf{Forms}_{n,d}^{smooth}$ and $\mathbf{Hypsurf}_{n,d}^{smooth}$. I will also assume that $n \geq 2$ and $d \geq 5$ if $n = 2$, $d \geq 4$ if $n = 3$ and $d \geq 3$ in all other cases. Under these assumptions, the main theorem, based on joint work with Berhuy and Brosnan-Vistoli, is as follows.

Theorem 4.1. *Suppose* $\gcd(n, d) = p^r$ *is a prime power, and* $n = p^s m$, *where p does not divide m. Then*

(a) $\mathrm{ed}(\mathbf{Hypsurf}_{n,d}^{smooth}) = \begin{cases} \binom{n+d-1}{d} - n^2 + p^s - 1, \ \textit{if } r \geq 1, \ \textit{and} \\ \binom{n+d-1}{d} - n^2, \ \textit{if } r = 0. \end{cases}$

(b) $\mathrm{ed}(\mathbf{Forms}_{n,d}^{smooth}) = \begin{cases} \binom{n+d-1}{d} - n^2 + p^s, \ \textit{if } r \geq 1, \ \textit{and} \\ \binom{n+d-1}{d} - n^2 + 1, \ \textit{if } r = 0. \end{cases}$

Everything in the sequel will be based on the following important theorem of Karpenko [Ka00]; in particular, this theorem is ultimately responsible for the "arithmetic contribution" of $p^s - 1$ to $\mathrm{ed}(\mathbf{Hypsurf}_{n,d}^{smooth})$ in part (a).

Theorem 4.2. *Let A be a division algebra over a field K, of prime power index p^r and let $\mathrm{BS}(A)$ be its Brauer-Severi variety. Then every rational map $\mathrm{BS}(A) \dashrightarrow \mathrm{BS}(A)$ defined over K is dominant.* ♠

The rest of this lecture will be devoted to outlining a proof of Theorem 4.1. Let us start by considering a slightly more general setting. Suppose X is an irreducible G-variety defined over k. We are interested in the essential dimension of the orbit functor

$$\mathbf{Orb}_{X,G} \colon L \mapsto \{\text{the set of } G(L)\text{-orbits in } X(L)\}$$

If $X = \mathbb{A}^N =$ space of homogeneous polynomials of degree n in d variables, with the natural action of $G = \mathbf{GL}_n$, then $\mathbf{Orb}_{X,G}$ becomes $\mathbf{Forms}_{n,d}$. Similarly if we take $X = \mathbb{P}^{N-1}$ then $\mathbf{Orb}_{X,G}$ becomes $\mathbf{Hypsurf}_{n,d}$.

Let $\mathcal{F}_{X,G}$ be the functor which associates to a field L the isomorphism classes of diagrams of the form

$$(4.3) \qquad\qquad \begin{array}{ccc} T & \xrightarrow{\ \psi\ } & X \\ {\scriptstyle \pi}\big\downarrow & & \\ \mathrm{Spec}(L) & & \end{array}$$

where π is a G-torsor and ψ is a G-equivariant map. If G is special, this functor is isomorphic to $\mathbf{Orb}_{X,G}$; indeed, in this case T is split over $\mathrm{Spec}(L)$ and the image of ϕ is exactly one $G(L)$-orbit in $X(L)$; cf. Exercise 4.1.

We will also consider the subfunctor $\mathcal{F}_{X,G}^{dom}$ of $\mathcal{F}_{X,G}$, where $\mathcal{F}_{X,G}^{dom}(K)$ is the set of diagram of the form (4.3) with ψ dominant. Note that for every such diagram L contains $K = k(X)^G$. For this reason it is natural to think of K as the base field for this functor, rather than k, i.e., to think of $\mathcal{F}_{X,G}^{dom}$ as a functor $\mathrm{Fields}_K \to \mathrm{Sets}$ and to talk about $\mathrm{ed}_K \mathcal{F}_{X,G}^{dom}$.
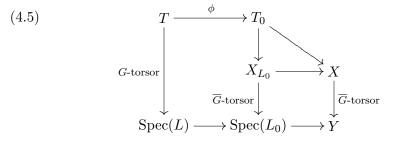
Example 4.4. Suppose $\pi \colon X \to Y$ is a G-torsor. Then $\mathrm{ed}(\mathcal{F}_{X,G}) = \dim(Y)$.

Indeed, in this case diagrams of the form (4.3) are in 1-1 correspondence with morphisms $\mathrm{Spec}(L) \to Y$ (T is then the pullback of π), i.e., the functor $\mathcal{F}_{X,G}$ is isomorphic to Y. Here we view Y as a functor $L \mapsto Y(L)$. The functor Y has essential dimension $\dim(Y)$; cf. Exercise 4.2.

The actions of $\mathbf{GL}_n$ on $X = \mathbb{A}^N$ or $\mathbb{P}^N$ are not of this form; in fact, a point in general position in $\mathbb{A}^N$ is $\boldsymbol{\mu}_d$ or $\mathbb{G}_m$, respectively. Thus we look at the following "next simplest case".

Assume that G is a central extension
$$1 \to C \to G \to \overline{G} \to 1$$
and $X \to Y$ is an $\overline{G}$-torsor but we view it as a G-variety. Let us try to compute the essential dimension of the diagram (4.3). Suppose the diagram (4.3) descends to L_0, i.e., it factors as

(4.5)

$$
\begin{array}{ccc}
T & \xrightarrow{\ \phi\ } & T_0 \\
\end{array}
$$

for some G-torsor $T_0 \to \mathrm{Spec}(L_0)$. In particular, the $\overline{G}$-torsor $X_{L_0} \to \mathrm{Spec}(L_0)$ lifts to a G-torsor. Examining the exact sequence
$$H^1(L_0, G) \to H^1(L_0, \overline{G}) \xrightarrow{\delta} H^2(K, C),$$
we see that this is equivalent to saying that L_0 splits the class of $\alpha = \delta([X]) \in H^2(K, C)$, where $K = k(Y)$.

Conversely, suppose L_0 splits α, i.e., $\overline{G}$-torsor $X_{L_0} \to \mathrm{Spec}(L_0)$ can be lifted to a G-torsor. Since liftings are in a (non-canoical) 1-1 correspondence with $H^1(L_0, C)$. (More precisely, the set of such liftings can be thought of as an "$H^1(L_0, C)$-torsor" .) In particular, if C is a torus, (as is the case for the $\mathbf{PGL}_n$-action on $X = \mathbb{P}^{N-1}$), then this lifting is essentially unique, and the existence of ϕ is guaranteed. For general C, ϕ may not exist. Once we choose an intermediate field $K \subset L_1 \subset L$ so that L_1 splits α, ϕ will

only exist if we replace L_1 by a larger intermediate extension L_0, where $K \subset L_1 \subset L_0 \subset L$ and $\operatorname{tr} \deg_{L_1}(L_0) = \operatorname{ed}(C)$.

I will mainly focus on the case where $C = \mathbb{G}_m$, corresponding to part (a) of Theorem 4.1 because it is easier to explain. In the setting of Theorem 4.1(b), $C = \boldsymbol{\mu}_d$. This why the formulas in parts (a) and (b) differ by 1.

Proposition 4.6. *Let* $1 \to C \to G \to \overline{G} \to 1$ *be a central extension of linear algebraic k-groups, and* $\pi \colon X \to Y$ *an $\overline{G}$-torsor, $K = k(Y) = k(X)^G$ and $\alpha = \delta([X]) \in H^2(K, C)$, as above. Assume that the index of α is a prime power p^s.*

Suppose $C = \mathbb{G}_m$. *Then*

(a) $\operatorname{ed}_K(\mathcal{F}_{X,G}^{dom}) = p^s - 1$ *and*

(b) $\operatorname{ed}_k(\mathcal{F}_{X,G}) = \dim(Y) + p^s - 1$.

Now suppose $C = \boldsymbol{\mu}_d$ *for some $d \geq 1$. Then*

(c) $\operatorname{ed}_K(\mathcal{F}_{X,G}^{dom}) = p^s$ *and*

(d) $\operatorname{ed}_k(\mathcal{F}_{X,G}) = \dim(Y) + p^s$.

Proof. First we note that (b) follows from (a). Indeed, for every diagram (4.3), ψ is dominant onto some G-invariant closed subvariety X' of X, where x is itself the total space of an $\overline{G}$-torsor $X' \to Y'$ over some closed subvariety $Y' \subset Y$. Thus $\operatorname{ed}_k(\mathcal{F}_{X,G}) =$

$$\max \operatorname{ed}_k(\mathcal{F}_{X',G}^{dom}) = \max\big(\operatorname{tr} \deg(K'/k) + \operatorname{ed}_K(\mathcal{F}_{X',G}^{dom})\big) = \max\big(\dim(Y') + \operatorname{ind}(\alpha') - 1\big),$$

where $K' = k(X')^G$, $\alpha' = \delta([X']) \in H^2(K', C)$, and the maximum is taken over the G-invariant subvarieties $X' \subset X$, as above. Since α' is a specialization of α, its index will divide p^s. In other words, the maximum in the above formula is $\dim(Y) + p^s - 1$; it will be attained for $X' = X$.

The same argument shows that (c) implies (d), I will now describe the proof of (a). The proof of (c) requires an additional effort; see [BRV07].

To prove (a), consider a diagram γ of the form (4.3) with ψ dominant. We will first show that $\operatorname{ed}_K(\gamma) \leq p^s - 1$. As I mentioned above, L splits α, giving rise to an L-point $p \colon \operatorname{Spec}(L) \to \operatorname{BS}(\alpha)$ of the Brauer-Severi variety of α (i.e., of the underlying division algebra of α). Moreover, the diagram (4.3) descends to L_0/K if and only if p descends on L_0. Thus

$$\operatorname{ed}(_K\gamma) \leq \operatorname{ed}(BS(\alpha)) = p^s - 1.$$

We will now construct a diagram γ whose essential dimension meets this bound. Let L be the generic point of $\operatorname{BS}(\alpha)$. Then L splits α, giving rise to a point $\operatorname{Spec}(L) \to \operatorname{BS}(\alpha)$, i.e., to a rational map $\operatorname{BS}(\alpha) \dashrightarrow \operatorname{BS}(\alpha)$ defined over K. Suppose γ descends to a subfield $K \subset L_0 \subset L$. Let Z_0 be a K-variety whose functoin field is L_0. Since L_0 splits α, we obtain the following rational maps

$$\operatorname{BS}(\alpha) \xdashrightarrow{f_1} Z_0 \xdashrightarrow{f_2} \operatorname{BS}(\alpha)$$

defined over K. Here f_1 is induced by the inclusion $L_0 \subset L = K(\mathrm{BS}(\alpha)$ and f_2 exists because L_0 splits α. After replacing Z_0 by the closure of the graph of f_2, we may assume that f_2 is regular. Applying Karpenko's theorem 4.2 to the composition

$$f_2 \circ f_1 \colon \mathrm{BS}(\alpha) \dashrightarrow \mathrm{BS}(\alpha)$$

we conclude that

$$\operatorname{tr} \deg(L_0/K) = \dim(Y) = \dim(\mathrm{BS}(\alpha)) = p^s - 1\,,$$

as claimed.   ♠

Let me now explain how to deduce Theorem 4.1 from the proposition. I will focus on part (a); the proof of part (b) is essentially the same. Our exact sequence here is

$$1 \to \mathbb{G}_m \to \mathbf{GL}_n \to \mathbf{PGL}_n \to 1$$

and $X = \mathbb{P}^{N-1}$ is the space of degree d hypersurfaces in $\mathbb{P}^{n-1}$. The first complicationis that $\overline{G} = \mathbf{PGL}_n$ does not act freely on $X = \mathbb{P}^N$; however, the proposition will apply (for suitable n and d) if we replace X by a $\mathbf{GL}_n$-invariant dense open subset. The fact that this open subset can be taken to be the subset of smooth hypersurfaces is a consequence of a deep *genericity theorem* of Vistoli [BRV07]. This is not a crucial point for us, and I will not explain this further; if you are uncomfortable with this, replace $\mathbb{A}^N_{smooth}$ and $\mathbb{P}^{N-1}_{smooth}$ by smaller $\mathbf{GL}_n$-equivariant dense open subsets, where the actions of $\mathbf{GL}_n/\boldsymbol{\mu}_d$ and $\mathbf{PGL}_n$, respectively, are free,

After replacing $\mathbb{P}^{N-1}$ by a suitable $\mathbf{GL}_n$-invariant dense open subset (which I will denote by X), we obtain a $\mathbf{PGL}_n$-torsor $X \to Y$. Here

$$\dim(Y) = \dim(X) - \dim(\mathbf{PGL}_n) = N - n^2 = \binom{n + d - 1}{d} - n^2\,.$$

This torsor gives rise to a central simple algebra A, and $\alpha = \delta([X]) \in H^2(K, \mathbb{G}_m)$ is the Brauer class of A. The index of α is thus the index of A. In order to prove Theorem 4.1(a), we need to compute the index of A.

By construction X is the quotient of a dense $\mathbf{GL}_n$-invariant open subset U of $\mathbb{A}^N$ by $\mathbb{G}_m$. We can thus think of U as the total space of a $\mathbf{GL}_n/\boldsymbol{\mu}_d$-torsor $U \to Y$. Since the $\mathbf{GL}_n/\boldsymbol{\mu}_d$-action on U comes from a generically free linear action on $\mathbb{A}^N$, this $\mathbf{GL}_n/\boldsymbol{\mu}_d$-torsor is *versal*. To sum up, $\alpha \in H^2(K, \mathbb{G}_m)$ is the image of a versal $\mathbf{GL}_n/\boldsymbol{\mu}_d$-torsor $U \to Y$ under the natural map

$$H^1(K, \mathbf{GL}_n/\boldsymbol{\mu}_d) \longrightarrow H^1(K, \mathbf{PGL}_n) \longrightarrow H^2(K, \mathbb{G}_m)$$

$$[U] \longrightarrow [X] \longrightarrow \alpha$$

Tracing through standard exact sequences in Galois cohomology one sees that the image of this map consists of the classes in $H^2(K, \mathbb{G}_m)$ of index dividing by n and exponent dividing d. or equivalently, of index dividing

by n and exponent dividing $e = \gcd(n, d) = p^r$; cf. Exercise 4.3. Since U is versal, we conclude that the index of α is maximal possible under these constraints, i.e., is $p^s =$ highest power of p dividing n. Theorem 4.1 now follows from Theorem 4.2.

EXERCISES FOR LECTURE 4

Exercise 4.1. Suppose G is a special group. Show that the functors $\mathbf{Orb}_{X,G}$ and $\mathcal{F}_{X,G}$ are isomorphic.

Exercise 4.2. Let Y be a (not necessarily integral) scheme defined over a (not necessarily algebraically closed) field k. Show that the essential dimension (over k) of the functor $K \to Y(K)$ equals $\dim_k(Y)$.

Exercise 4.3. Show that the image of the connecting homomorphism

$$\partial_K \colon H^1(K, \mathbf{GL}_n/\boldsymbol{\mu}_d) \to H^2(K, \boldsymbol{\mu}_d)$$

associated to the exact sequence

$$1 \to \mathbb{G}_m \to \mathbf{GL}_n/\boldsymbol{\mu}_d \to \mathbf{PGL}_n \to 1$$

consists of Brauer classes of index dividing n and exponent dividing d.

Exercise 4.4. (a) Find $\mathrm{ed}(\mathbf{Forms}_{n,1})$. (b) Find $\mathrm{ed}(\mathbf{Forms}_{2,3})$.

5. LECTURE 5. LOWER BOUNDS FOR CENTRAL EXTENSIONS

In this lecture we will prove the following theorem.

Theorem 5.1. *Let X be a G-variety defined over k. Then*

$$\mathrm{ed}_k(G) \geq \mathrm{ed}_K(\mathcal{F}_{X,G}^{dom}) - e \,,$$

where $K = k(X)^G$ and e is the maximal dimension of a G-orbit in X.

Before proceeding with the proof we will discuss some applications. Suppose

$$(5.2) \qquad\qquad 1 \longrightarrow C \longrightarrow G \longrightarrow \overline{G} \longrightarrow 1$$

is an exact sequence of algebraic groups over a field k, with C central. We would like to apply Theorem 5.1 to a $\overline{G}$-torsor $X \to B$, which we view as a G-variety. For every field extension K/k the sequence (5.2) induces a connecting map $\partial_K \colon \mathrm{H}^1(K, \overline{G}) \to \mathrm{H}^2(K, C)$. Combining Theorem 5.1 with the formula for $\mathrm{ed}_K \mathcal{F}_{X,G}^{dom}$ given in Proposition 4.6, we obtain the following inequality.

Corollary 5.3. *Let $1 \to C \to G \to \overline{G} \to 1$ be an exact sequence of k-groups, where G is central and $G \simeq \mathbb{G}_m$ or $\boldsymbol{\mu}_d$ for some $d \geq 1$. For each field K/k, consider the connecting map $\partial_K \colon \mathrm{H}^1(K, \overline{G}) \to \mathrm{H}^2(K, C)$. If p^s divides the index of $\partial_K(t)$ for some $t \in \mathrm{H}^1(K, \overline{G})$ then $\mathrm{ed}(G) \geq p^s - \dim(G)$.*

Proof. We may assume that K is finitely generated over k.

Moreover, after replacing K by a finite prime-to-p extension, we may also assume that the index of $\partial_K(t)$ is exactly p^s. (This follows from the primary decomposition theorem for central simple algebras; see Exercise 5.1.)

Let $\pi\colon X \to Y$ be the $\overline{G}$-torsor representing t. Here

$$K = k(Y) = k(X)^{\overline{G}} = k(X)^G;$$

to obtain t we restrict this torsor to the generic point of Y. If $C \simeq \mathbb{G}_m$ then Proposition 4.6(a) tells us that $\operatorname{ed}_K \mathcal{F}^{dom}_{X,G} = p^s - 1$. Hence, by Theorem 5.1,

$$\operatorname{ed}_k(G) \geq p^s - 1 - \dim(\overline{G}) = p^s - \dim(G)\,.$$

If $C \simeq \boldsymbol{\mu}_d$ then $\operatorname{ed}_K \mathcal{F}^{dom}_{X,G} = p^s$ by Proposition 4.6(c) and thus

$$\operatorname{ed}_k(G) \geq p^s - \dim(\overline{G}) = p^s - \dim(G)\,,$$

as claimed.   ♠

Corollary 5.4. *(a) If n is odd then* $\operatorname{ed}(\mathbf{Spin}_n) = 2^{(n-1)/2} - \dfrac{n(n-1)}{2}$.

(b) If $n \equiv 2 \pmod 4$ then $\operatorname{ed}(\mathbf{Spin}_n) = 2^{(n-2)/2} - \dfrac{n(n-1)}{2}$.

Proof. (a) We apply Corollary 5.3 to the exact sequence

$$1 \to \boldsymbol{\mu}_2 \to \mathbf{Spin}_n \to \mathbf{SO}_n \to 1\,,$$

where $\boldsymbol{\mu}_2$ is the center of $\mathbf{Spin}_n$. In this case $\delta_K\colon H^1(K,\mathbf{SO}_n) \to H^2(K,\boldsymbol{\mu}_2)$ is the Hasse-Witt invariant. If $n = 2m+1$ is odd, set $K = k(a_1, b_1, \ldots, a_m, b_m)$, where $a_1, b_1, \ldots, a_m, b_m$ are independent variables, and define q_n recursively by

$$q_3 = \langle a_1, b_1, a_1 b_1 \rangle \text{ and } q_{n+2} = \langle a_n b_n \rangle \otimes q_n \oplus \langle a_n, b_n \rangle.$$

A direct computation using basic properties of the Hasse-Witt invariant shows that $c(q_{2m+1})$ is the class of the product $(a_1, b_1)_2 \otimes_K \cdots \otimes_K (a_m, b_m)_2$ of quaternion algebras. This class has index 2^m, and Corollary 5.3 yields
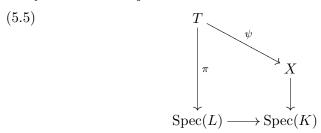
$$\operatorname{ed}(\mathbf{Spin}_n) \geq 2^{(n-1)/2} - \frac{n(n-1)}{2}\,.$$

The opposite inequality is a consequence of (1.7), applied to the spin representation of $\mathbf{Spin}_n$. The spin representation has dimension $2^{(n-1)/2}$ and is generically free (in characteristic 0) for every $n \geq 15$.

The proof of part (b) is similar, with the spin representation replaced by the half-spin representation.   ♠

We now proceed with the proof of Theorem 5.1. We will avoid stack-theoretic language, so the argument here will be different from the one in [BRV07]. Note however, that that I do not know a stack-free proof of Proposition 4.6(b), on which our applications rely.
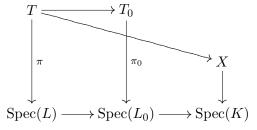
Proof. Choose an object

(5.5)

$$
\begin{array}{ccc}
T & \xrightarrow{\ \psi\ } & \\
\downarrow{\scriptstyle\pi} & \searrow & X \\
 & & \downarrow \\
\mathrm{Spec}(L) & \longrightarrow & \mathrm{Spec}(K)
\end{array}
$$

with ψ dominant, of maximal essential dimension $\mathrm{ed}_K(\mathcal{F}_{X,G})^{dom}$. Here π is a G-torsor, ϕ is a G-equivariant map, $K = k(X)^G$. Note that the maximal dimension of a G-orbit in X, denoted by e in the statement of the theorem can also be written as
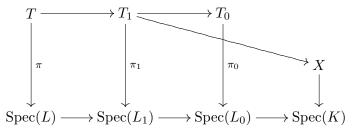
$$
e = \mathrm{tr}\deg(k(X)/K) = \dim_K(X)\,,
$$

where we view X as a K-variety (in fact, a homogeneous space), via the rational map $X \to \mathrm{Spec}(K)$ induced by inclusion $K = k(X)^G \subset k(X)$. Since $\mathrm{ed}_k(G) \geq \mathrm{ed}_K(G)$ (cf. (1.5)), it suffices to show that

(5.6) $\mathrm{ed}_K(\pi) \geq \mathrm{ed}_K(\mathcal{F}_{X,G}^{dom}) - e\,.$

Indeed, choose a subfield $K \subset L_0 \subset K$ such that π descends to L_0 and $\mathrm{tr}\deg(L_0/K) = \mathrm{ed}_K(\pi)$. (This is by definition the minimal possible value of $\mathrm{tr}\deg(L_0/K)$ for such L_0.) In other words, we have the following diagram:

$$
\begin{array}{ccccc}
T & \longrightarrow & T_0 & & \\
\downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi_0} & \searrow & X \\
 & & & & \downarrow \\
\mathrm{Spec}(L) & \longrightarrow & \mathrm{Spec}(L_0) & \longrightarrow & \mathrm{Spec}(K)
\end{array}
$$

I claim that there exists a further intermediate extension $K \subset L_0 \subset L_1 \subset L$ such that $\mathrm{tr}\deg(L_1/L_0) \leq e$ and the above diagram can be factored through a G-torsor $\pi_1\colon T_1 \to \mathrm{Spec}(L_1)$ as follows:

$$
\begin{array}{ccccccc}
T & \longrightarrow & T_1 & \longrightarrow & T_0 & & \\
\downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi_1} & & \downarrow{\scriptstyle\pi_0} & \searrow & X \\
 & & & & & & \downarrow \\
\mathrm{Spec}(L) & \longrightarrow & \mathrm{Spec}(L_1) & \longrightarrow & \mathrm{Spec}(L_0) & \longrightarrow & \mathrm{Spec}(K)
\end{array}
$$

If we can establish the claim then the original object (5.5) will descend to the field L_1 and thus

$$
\mathrm{ed}(\mathcal{F}_{X,G})^{dom} \leq \mathrm{tr}\deg(L_1/K) = \mathrm{tr}\deg(L_1/L_0) + \mathrm{tr}\deg(L_0/K) \leq e + \mathrm{ed}_K(\pi)\,,
$$

proving (5.6).

To verify the claim, let X be the scheme $S = \mathrm{Mor}_G(T_0, X_{L_0})$ defined over L_0. Over the algebraic closure $\overline{L}$ of L this scheme becomes (non-canonically) isomorphic to X. Indeed, over $\overline{L}$, T_0 (or equivalently, T) can be (non-canonically) identified with G, and specifying a morphism $T \to X$ is equivalent to specifying which point of X is the image of the identity element of G. We know that there exists a G-equivariant map $T \to X$; this is equivalent to the existence of an L-point $p\colon \mathrm{Spec}(L) \to S$. Hence, p descends to a subfield L_1 such that $\mathrm{tr\,deg}(L_1/L_0) \le \dim_{L_0}(S) = \dim_K(X) = e$. That is, S has an L_1-point or equivalently, there exists a map from T_1 to X.   ♠

Exercises for Lecture 5

Exercise 5.1. Let A/K be a central simple algebra of index $n = p^s m$, where m is not divisible by p. Show that there exists a prime-to-p extension L/K, so that the index of $A \otimes_K L$ is exactly p^s

Exercise 5.2. Let K/k be a field extension and $\partial_K\colon \mathrm{H}^1(K, \overline{G}) \to \mathrm{H}^2(K, C)$. be the connecting homomorphism associated to the central extension

$$1 \longrightarrow C \longrightarrow G \longrightarrow \overline{G} \longrightarrow 1\,,$$

as in 5.2. $\partial_K\colon \mathrm{H}^1(K, \overline{G}) \to \mathrm{H}^2(K, C)$. Show that for every $t \in H^1(K, \overline{G})$ there exists a finitely generated field extension K_0/k and an element $t_0 \in H^1(K_0, \overline{G})$ such that $\mathrm{ind}(\alpha)$ divides $\mathrm{ind}_p(\alpha_0)$.

References

[Am72]   S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), 408–420.

[BF03]   Grégory Berhuy and Giordano Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330 (electronic).

[BerR05]   G. Berhuy, Z. Reichstein, *On the notion of canonical dimension for algebraic groups*, Adv. Math. **198** (2005), no. 1, 128–171.

[Br98]   M. Brion, *The behaviour at infinity of the Bruhat decomposition*, Comment. Math. Helv. **73** (1998), no. 1, 137–174.

[Bro07]   Patrick Brosnan, *The essential dimension of a g-dimensional complex abelian variety is 2g*, Transform. Groups **12** (2007), no. 3, 437–441.

[BRV07]   Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli, *Essential dimension and algebraic stacks*, 2007, `arXiv:math/0701903v1 [math.AG]`.

[BuR97]   J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159–179.

[CS06]   Vladimir Chernousov and Jean-Pierre Serre, *Lower bounds for essential dimensions via orthogonal representations*, J. Algebra **305** (2006), no. 2, 1055–1070.

[GMS03]   Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003.

[GR07]   Ph. Gille, Z. Reichstein, *A lower bound on the essential dimension of a connected linear group*, Commentarii Math Helvitici, to appear.

[Ka00]   N. A. Karpenko, *On anisotropy of orthogonal involutions*, J. Ramanujan Math. Soc. **15** (2000), no. 1, 1–22.

[KM06]   Nikita A. Karpenko, and Alexander S. Merkurjev, *Canonical p-dimension of algebraic groups*, Adv. Math. **205** (2006), no. 2, 410–433.

[KM07]   N. A. Karpenko and A. S. Merkurjev, *Essential dimension of finite groups*, to appear in Inventiones Math., **172**, no. 3, June, 2008.

[Kl1884]   F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom 5ten Grade*, 1884.

[PV94]   V. L. Popov, E. B. Vinberg, Invariant theory, in Algebraic geometry. IV. A translation of Algebraic geometry. **4** (Russian), Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989. Encyclopaedia of Mathematical Sciences, **55**, Springer-Verlag, Berlin, 1994.

[Rei99]   Z. Reichstein, *On a theorem of Hermite and Joubert*, Can. J. Math. **51**, No.1, 69-95 (1999).

[Rei00]   Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304.

[RY00]   Zinovy Reichstein and Boris Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056, With an appendix by János Kollár and Endre Szabó.

[RS92]   L. H. Rowen, D. J. Saltman, *Prime-to-p extensions of division algebras*, Israel J. Math. **78** (1992), no. 2-3, 197–207.

[Rost99]   M. Rost, *A descent property for Pfister forms*, J. Ramanujan Math. Soc. **14** (1999), no. 1, 55–63.

[Se95]   J.-P. Serre, *Cohomologie galoisienne: progre's et proble'mes*, Se'minaire Bourbaki, Vol. 1993/94. Aste'risque **227** (1995), Exp. No. 783, 4, 229–257.

[St75]   R. Steinberg, *Torsion in reductive groups*, Advances in Math. **15** (1975), 63–92.

[Ti92]   J. Tits, *Sur les degrés des extensions de corps déployant les groupes algébriques simples*, C. R. Acad. Sci. Paris, t. 315, Série I (1992), 1131–1138.

[To05₁]   B. Totaro, *The torsion index of the spin groups*, Duke Math. J. **129** (2005), no. 2, 249–290.

[To05₂]   B. Totaro, *The torsion index of E_8 and other groups*, Duke Math. J. **129** (2005), no. 2, 219–248.

[Woo89]   Jay A. Wood, *Spinor groups and algebraic coding theory*, J. Combin. Theory Ser. A **51** (1989), no. 2, 277–313.

[Zai07]   K. Zainoulline, *Canonical p-dimensions of algebraic groups and degrees of basic polynomial invariants*, Bull. Lond. Math. Soc. **39** (2007), no. 2, 301–304.

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF BRITISH COLUMBIA, 1984 MATHEMATICS ROAD, VANCOUVER, B.C., CANADA V6T 1Z2

E-mail address, Reichstein: `reichst@math.ubc.ca`