# Essential dimension

Zinovy Reichstein

Department of Mathematics
University of British Columbia
, Vancouver, Canada

Spring School on Torsors, Motives and Cohomological Invariants
May 2013
Fields Institute, Toronto

# Introduction

Informally speaking, the essential dimension of an algebraic object is the minimal number of independent parameters one needs to define it. In the past 15 years this numerical invariant has been extensively studied by a variety of algebraic, geometrc and cohomological techniques. The goal of these lectures is to survey some of this research.

Most of the material here is based on the expository paper I have written for the 2010 ICM and the November 2012 issue of the AMS Notices. See also a 2003 Documenta Math. article by G. Berhuy and G. Favi, and a recent survey by A. Merkurjev (to appear in the journal of Transformation Groups).

# Introduction

Informally speaking, the essential dimension of an algebraic object is the minimal number of independent parameters one needs to define it. In the past 15 years this numerical invariant has been extensively studied by a variety of algebraic, geometrc and cohomological techniques. The goal of these lectures is to survey some of this research.

Most of the material here is based on the expository paper I have written for the 2010 ICM and the November 2012 issue of the AMS Notices. See also a 2003 Documenta Math. article by G. Berhuy and G. Favi, and a recent survey by A. Merkurjev (to appear in the journal of Transformation Groups).

# First examples

To motivate the notion of essential dimension, I will start with three simple examples.

In each example $k$ will denote a field and $K/k$ will be a field extension. The objects of interest to us will always be defined over $K$. In considering quadratic forms, I will always assume that $\operatorname{char}(k) \neq 2$, and in considering elliptic curves, I will assume that $\operatorname{char}(k) \neq 2$ or 3.

# First examples

To motivate the notion of essential dimension, I will start with three simple examples.

In each example $k$ will denote a field and $K/k$ will be a field extension. The objects of interest to us will always be defined over $K$. In considering quadratic forms, I will always assume that $\text{char}(k) \neq 2$, and in considering elliptic curves, I will assume that $\text{char}(k) \neq 2$ or 3.

# Example 1: The essential dimension of a quadratic form

Let $q$ be a non-degenerate quadratic form on $K^d$.

Denote the symmetric bilinear form associated to $q$ by $b$. We would like to know if $q$ can be *defined over* (or equivalently, *descends to*) some smaller field $k \subset K_0 \subset K$.

This means that there is a $K$-basis $e_1, \ldots, e_d$ of $K^d$ such that

$$b_{ij} := b(e_i, e_j) \in K_0$$

for every $i, j = 1, \ldots, d$.

Equivalently, in this basis $q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} b_{ij} x_i x_j$ has all of its coefficients in $K_0$.

# Example 1: The essential dimension of a quadratic form

Let $q$ be a non-degenerate quadratic form on $K^d$.

Denote the symmetric bilinear form associated to $q$ by $b$. We would like to know if $q$ can be *defined over* (or equivalently, *descends to*) some smaller field $k \subset K_0 \subset K$.

This means that there is a $K$-basis $e_1, \ldots, e_d$ of $K^d$ such that

$$b_{ij} := b(e_i, e_j) \in K_0$$

for every $i, j = 1, \ldots, d$.

Equivalently, in this basis $q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} b_{ij} x_i x_j$ has all of its coefficients in $K_0$.

# Example 1: The essential dimension of a quadratic form

Let $q$ be a non-degenerate quadratic form on $K^d$.

Denote the symmetric bilinear form associated to $q$ by $b$. We would like to know if $q$ can be *defined over* (or equivalently, *descends to*) some smaller field $k \subset K_0 \subset K$.

This means that there is a $K$-basis $e_1, \ldots, e_d$ of $K^d$ such that

$$b_{ij} := b(e_i, e_j) \in K_0$$

for every $i, j = 1, \ldots, d$.

Equivalently, in this basis $q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} b_{ij} x_i x_j$ has all of its coefficients in $K_0$.

# Example 1: The essential dimension of a quadratic form

Let $q$ be a non-degenerate quadratic form on $K^d$.

Denote the symmetric bilinear form associated to $q$ by $b$. We would like to know if $q$ can be *defined over* (or equivalently, *descends to*) some smaller field $k \subset K_0 \subset K$.

This means that there is a $K$-basis $e_1, \ldots, e_d$ of $K^d$ such that

$$b_{ij} := b(e_i, e_j) \in K_0$$

for every $i, j = 1, \ldots, d$.

Equivalently, in this basis $q(x_1, \ldots, x_n) = \sum_{i,j=1}^n b_{ij} x_i x_j$ has all of its coefficients in $K_0$.

# Example 1 continued: the essential dimension of a quadratic form

It is natural to ask if there is a minimal field $K_0$ (with respect to inclusion) to which $q$ descends. The answer is usually "no".

So, we modify the question: instead of asking for a minimal field of definition $K_0$ for $q$, we ask for a field of definition $K_0$ of minimal transcendence degree.

The smallest possible value of $\mathrm{trdeg}_k(K_0)$ is called the *essential dimension* of $q$ and is denoted by $\mathrm{ed}(q)$ or $\mathrm{ed}_k(q)$.

# Example 1 continued: the essential dimension of a quadratic form

It is natural to ask if there is a minimal field $K_0$ (with respect to inclusion) to which $q$ descends. The answer is usually "no".

So, we modify the question: instead of asking for a minimal field of definition $K_0$ for $q$, we ask for a field of definition $K_0$ of minimal transcendence degree.

The smallest possible value of $\mathrm{trdeg}_k(K_0)$ is called the *essential dimension* of $q$ and is denoted by $\mathrm{ed}(q)$ or $\mathrm{ed}_k(q)$.

# Example 1 continued: the essential dimension of a quadratic form

It is natural to ask if there is a minimal field $K_0$ (with respect to inclusion) to which $q$ descends. The answer is usually "no".

So, we modify the question: instead of asking for a minimal field of definition $K_0$ for $q$, we ask for a field of definition $K_0$ of minimal transcendence degree.

The smallest possible value of $\mathrm{trdeg}_k(K_0)$ is called the *essential dimension* of $q$ and is denoted by $\mathrm{ed}(q)$ or $\mathrm{ed}_k(q)$.

# Example 1 continued: the essential dimension of a quadratic form

It is natural to ask if there is a minimal field $K_0$ (with respect to inclusion) to which $q$ descends. The answer is usually "no".

So, we modify the question: instead of asking for a minimal field of definition $K_0$ for $q$, we ask for a field of definition $K_0$ of minimal transcendence degree.

The smallest possible value of $\mathrm{trdeg}_k(K_0)$ is called the *essential dimension* of $q$ and is denoted by $\mathrm{ed}(q)$ or $\mathrm{ed}_k(q)$.

# Example 2: The essential dimension of a linear transformation

Once again, let $k$ be an arbitrary field, and $K/k$ be a field extension. Consider a linear transformation $T\colon K^n \to K^n$. Here, as usual, $K$-linear transformations are considered equivalent if their matrices are conjugate over $K$. If $T$ is represented by an $n \times n$ matrix $(a_{ij})$ then $T$ descends to $K_0 = k(a_{ij} \mid i,j = 1,\dots,n)$.

Once again, the smallest possible value of $\mathrm{trdeg}_k(K_0)$ is called the *essential dimension* of $T$ and is denoted by $\mathrm{ed}(T)$ or $\mathrm{ed}_k(T)$. A priori $\mathrm{ed}(T) \leqslant n^2$.

# Example 2: The essential dimension of a linear transformation

Once again, let $k$ be an arbitrary field, and $K/k$ be a field extension. Consider a linear transformation $T\colon K^n \to K^n$. Here, as usual, $K$-linear transformations are considered equivalent if their matrices are conjugate over $K$. If $T$ is represented by an $n \times n$ matrix $(a_{ij})$ then $T$ descends to $K_0 = k(a_{ij} \mid i, j = 1, \dots, n)$.

Once again, the smallest possible value of $\mathrm{trdeg}_k(K_0)$ is called the *essential dimension* of $T$ and is denoted by $\mathrm{ed}(T)$ or $\mathrm{ed}_k(T)$. A priori $\mathrm{ed}(T) \leqslant n^2$.

# Example 2 continued

However, the obvious bound $\mathrm{ed}(T) \leqslant n^2$. is not optimal. We can specify $T$ more economically by its rational canonical form $R$. Recall that $R$ is a block-diagonal matrix $\mathrm{diag}(R_1, \ldots, R_m)$, where each $R_i$ is a companion matrix. If $m = 1$ and

$R = R_1 = \begin{pmatrix} 0 & \ldots & 0 & c_1 \\ 1 & \ldots & 0 & c_2 \\ & \ddots & & \vdots \\ 0 & \ldots & 1 & c_n \end{pmatrix}$, then $T$ descends to $k(c_1, \ldots, c_n)$ and thus $\mathrm{ed}(T) \leqslant n$.

A similar argument shows that $\mathrm{ed}(T) \leqslant n$ for any $m$.

# Example 2 continued

However, the obvious bound $\mathrm{ed}(T) \leqslant n^2$. is not optimal. We can specify $T$ more economically by its rational canonical form $R$. Recall that $R$ is a block-diagonal matrix $\mathrm{diag}(R_1, \ldots, R_m)$, where each $R_i$ is a companion matrix. If $m = 1$ and $R = R_1 = \begin{pmatrix} 0 & \ldots & 0 & c_1 \\ 1 & \ldots & 0 & c_2 \\ & \ddots & & \vdots \\ 0 & \ldots & 1 & c_n \end{pmatrix}$, then $T$ descends to $k(c_1, \ldots, c_n)$ and thus $\mathrm{ed}(T) \leqslant n$.

A similar argument shows that $\mathrm{ed}(T) \leqslant n$ for any $m$.

# Example 3: The essential dimension of an elliptic curve

Let $X$ be an elliptic curve curves defined over $K$. We say that $X$ descends to $K_0 \subset K$, if $X = X \times_K K_0$ for some elliptic curve $X_0$ defined over $K_0$. The essential dimension $\mathrm{ed}(X)$ is defined as the minimal value of $\mathrm{trdeg}_k(K_0)$, where $X$ descends to $K_0$.

Every elliptic curve $X$ over $K$ is isomorphic to the plane curve cut out by a Weierstrass equation $y^2 = x^3 + ax + b$, for some $a, b \in K$. Hence, $X$ descends to $K_0 = k(a, b)$ and $\mathrm{ed}(X) \leqslant 2$.

# Example 3: The essential dimension of an elliptic curve

Let $X$ be an elliptic curve curves defined over $K$. We say that $X$ descends to $K_0 \subset K$, if $X = X \times_K K_0$ for some elliptic curve $X_0$ defined over $K_0$. The essential dimension $\mathrm{ed}(X)$ is defined as the minimal value of $\mathrm{trdeg}_k(K_0)$, where $X$ descends to $K_0$.

Every elliptic curve $X$ over $K$ is isomorphic to the plane curve cut out by a Weierstrass equation $y^2 = x^3 + ax + b$, for some $a, b \in K$. Hence, $X$ descends to $K_0 = k(a, b)$ and $\mathrm{ed}(X) \leqslant 2$.

# Towards a more general definition

In a similar manner one can consider fields of definition of any polynomial in $K[x_1, \ldots, x_n]$, any finite-dimensional $K$-algebra, any 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.

We will now state this more formally.

# Towards a more general definition

In a similar manner one can consider fields of definition of any polynomial in $K[x_1, \ldots, x_n]$, any finite-dimensional $K$-algebra, any 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.

We will now state this more formally.

# Towards a more general definition

In a similar manner one can consider fields of definition of any polynomial in $K[x_1, \ldots, x_n]$, any finite-dimensional $K$-algebra, any 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.

We will now state this more formally.

# Covariant functors

Let $k$ be a base field, $\mathsf{Fields}_k$ be the category of field extensions $K/k$, Sets be the category of sets, and

$$\mathcal{F}\colon\ \mathsf{Fields}_k \to \mathsf{Sets}$$

be a covariant functor.

In Example 1, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of non-degenerate quadratic forms on $K^n$,

In Example 2, $\mathcal{F}(K)$ is the set of equivalence classes of linear transformations $K^n \to K^n$.

In Example 3, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of elliptic curves defined over $K$.

In general we think of $\mathcal{F}$ as specifying the type of algebraic object we want to work with, and elements of $\mathcal{F}(K)$ as algebraic objects of this type defined over $K$.

# Covariant functors

Let $k$ be a base field, $\mathsf{Fields}_k$ be the category of field extensions $K/k$, Sets be the category of sets, and

$$\mathcal{F}\colon \mathsf{Fields}_k \to \mathsf{Sets}$$

be a covariant functor.

In Example 1, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of non-degenerate quadratic forms on $K^n$,

In Example 2, $\mathcal{F}(K)$ is the set of equivalence classes of linear transformations $K^n \to K^n$.

In Example 3, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of elliptic curves defined over $K$.

In general we think of $\mathcal{F}$ as specifying the type of algebraic object we want to work with, and elements of $\mathcal{F}(K)$ as algebraic objects of this type defined over $K$.

# Covariant functors

Let $k$ be a base field, $\text{Fields}_k$ be the category of field extensions $K/k$, Sets be the category of sets, and

$$\mathcal{F}\colon\ \text{Fields}_k \to \text{Sets}$$

be a covariant functor.

In Example 1, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of non-degenerate quadratic forms on $K^n$,

In Example 2, $\mathcal{F}(K)$ is the set of equivalence classes of linear transformations $K^n \to K^n$.

In Example 3, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of elliptic curves defined over $K$.

In general we think of $\mathcal{F}$ as specifying the type of algebraic object we want to work with, and elements of $\mathcal{F}(K)$ as algebraic objects of this type defined over $K$.

# Covariant functors

Let $k$ be a base field, $\mathrm{Fields}_k$ be the category of field extensions $K/k$, Sets be the category of sets, and

$$\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}$$

be a covariant functor.

In Example 1, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of non-degenerate quadratic forms on $K^n$,

In Example 2, $\mathcal{F}(K)$ is the set of equivalence classes of linear transformations $K^n \to K^n$.

In Example 3, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of elliptic curves defined over $K$.

In general we think of $\mathcal{F}$ as specifying the type of algebraic object we want to work with, and elements of $\mathcal{F}(K)$ as algebraic objects of this type defined over $K$.

# Covariant functors

Let $k$ be a base field, $\mathsf{Fields}_k$ be the category of field extensions $K/k$, $\mathsf{Sets}$ be the category of sets, and

$$\mathcal{F}\colon \mathsf{Fields}_k \to \mathsf{Sets}$$

be a covariant functor.

In Example 1, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of non-degenerate quadratic forms on $K^n$,

In Example 2, $\mathcal{F}(K)$ is the set of equivalence classes of linear transformations $K^n \to K^n$.

In Example 3, $\mathcal{F}(K)$ is the set of $K$-isomorphism classes of elliptic curves defined over $K$.

In general we think of $\mathcal{F}$ as specifying the type of algebraic object we want to work with, and elements of $\mathcal{F}(K)$ as algebraic objects of this type defined over $K$.

# The essential dimension of an object

Given a field extension $K/k$, we will say that an object $\alpha \in \mathcal{F}(K)$ *descends* to an intermediate field $k \subseteq K_0 \subseteq K$ if $\alpha$ is in the image of the induced map $\mathcal{F}(K_0) \to \mathcal{F}(K)$:

$$\begin{tikzcd}
\alpha_0 \arrow[r] \arrow[d, dash] & \alpha \arrow[d, dash] \\
K_0 \arrow[r] & K\,.
\end{tikzcd}$$

The *essential dimension* $\mathrm{ed}(\alpha)$ of $\alpha \in \mathcal{F}(K)$ is the minimum of the transcendence degrees $\mathrm{trdeg}_k(K_0)$ taken over all fields

$$k \subseteq K_0 \subseteq K$$

such that $\alpha$ descends to $K_0$.

# The essential dimension of an object

Given a field extension $K/k$, we will say that an object $\alpha \in \mathcal{F}(K)$ *descends* to an intermediate field $k \subseteq K_0 \subseteq K$ if $\alpha$ is in the image of the induced map $\mathcal{F}(K_0) \to \mathcal{F}(K)$:

$$\begin{tikzcd} \alpha_0 \arrow[r] \arrow[d, dash] & \alpha \arrow[d, dash] \\ K_0 \arrow[r] & K . \end{tikzcd}$$

The *essential dimension* $\mathrm{ed}(\alpha)$ of $\alpha \in \mathcal{F}(K)$ is the minimum of the transcendence degrees $\mathrm{trdeg}_k(K_0)$ taken over all fields

$$k \subseteq K_0 \subseteq K$$

such that $\alpha$ descends to $K_0$.

# The essential dimension of a functor

In many instances one is interested in the "worst case scenario", i.e., in the number of independent parameters which may be required to describe the "most complicated" objects of its kind. With this in mind, we define the essential dimension $\mathrm{ed}(\mathcal{F})$ of the functor $\mathcal{F}$ as the supremum of $\mathrm{ed}(\alpha)$ taken over all $\alpha \in \mathcal{F}(K)$ and all $K$. We have shown that $\mathrm{ed}(\mathcal{F}) \leqslant n$ in Examples 1 and 2, and $\mathrm{ed}(\mathcal{F}) \leqslant 2$ in Example 3.

We will later see that, in fact,

$\mathrm{ed}(\mathcal{F}) = n$ in Example 1 (quadratic forms).

One can also show that

$\mathrm{ed}(\mathcal{F}) = n$ in Example 2 (linear transformations) and

$\mathrm{ed}(\mathcal{F}) = 2$ in Example 3 (elliptic curves).

# The essential dimension of a functor

In many instances one is interested in the "worst case scenario", i.e., in the number of independent parameters which may be required to describe the "most complicated" objects of its kind. With this in mind, we define the essential dimension $\mathrm{ed}(\mathcal{F})$ of the functor $\mathcal{F}$ as the supremum of $\mathrm{ed}(\alpha)$ taken over all $\alpha \in \mathcal{F}(K)$ and all $K$. We have shown that $\mathrm{ed}(\mathcal{F}) \leqslant n$ in Examples 1 and 2, and $\mathrm{ed}(\mathcal{F}) \leqslant 2$ in Example 3.

We will later see that, in fact,

$\mathrm{ed}(\mathcal{F}) = n$ in Example 1 (quadratic forms).

One can also show that

$\mathrm{ed}(\mathcal{F}) = n$ in Example 2 (linear transformations) and

$\mathrm{ed}(\mathcal{F}) = 2$ in Example 3 (elliptic curves).

# The essential dimension of a functor

In many instances one is interested in the "worst case scenario", i.e., in the number of independent parameters which may be required to describe the "most complicated" objects of its kind. With this in mind, we define the essential dimension $\mathrm{ed}(\mathcal{F})$ of the functor $\mathcal{F}$ as the supremum of $\mathrm{ed}(\alpha)$ taken over all $\alpha \in \mathcal{F}(K)$ and all $K$. We have shown that $\mathrm{ed}(\mathcal{F}) \leqslant n$ in Examples 1 and 2, and $\mathrm{ed}(\mathcal{F}) \leqslant 2$ in Example 3.

We will later see that, in fact,

$\mathrm{ed}(\mathcal{F}) = n$ in Example 1 (quadratic forms).

One can also show that

$\mathrm{ed}(\mathcal{F}) = n$ in Example 2 (linear transformations) and

$\mathrm{ed}(\mathcal{F}) = 2$ in Example 3 (elliptic curves).

# The essential dimension of a group

An important class of examples are the Galois cohomology functors $\mathcal{F}_G = H^1(*, G)$ sending a field $K/k$ to the set $H^1(K, G_K)$ of isomorphism classes of $G$-torsors over $\mathrm{Spec}(K)$. Here $G$ is an algebraic group defined over $k$.

$\mathrm{ed}(\mathcal{F}_\mathcal{G})$ is a numerical invariant of $G$. Informally speaking, it is a measure of complexity of $G$-torsors over fields. This number is usually denoted by $\mathrm{ed}(G)$.

The notion of essential dimension was originally introduced in this context; the more general definition for a covariant functor is due to A. S. Merkurjev.

# The essential dimension of a group

An important class of examples are the Galois cohomology functors $\mathcal{F}_G = H^1(*, G)$ sending a field $K/k$ to the set $H^1(K, G_K)$ of isomorphism classes of $G$-torsors over $\mathrm{Spec}(K)$. Here $G$ is an algebraic group defined over $k$.

$\mathrm{ed}(\mathcal{F}_\mathcal{G})$ is a numerical invariant of $G$. Informally speaking, it is a measure of complexity of $G$-torsors over fields. This number is usually denoted by $\mathrm{ed}(G)$.

The notion of essential dimension was originally introduced in this context; the more general definition for a covariant functor is due to A. S. Merkurjev.

# The essential dimension of a group

An important class of examples are the Galois cohomology functors $\mathcal{F}_G = H^1(*, G)$ sending a field $K/k$ to the set $H^1(K, G_K)$ of isomorphism classes of $G$-torsors over $\mathrm{Spec}(K)$. Here $G$ is an algebraic group defined over $k$.

$\mathrm{ed}(\mathcal{F}_{\mathcal{G}})$ is a numerical invariant of $G$. Informally speaking, it is a measure of complexity of $G$-torsors over fields. This number is usually denoted by $\mathrm{ed}(G)$.

The notion of essential dimension was originally introduced in this context; the more general definition for a covariant functor is due to A. S. Merkurjev.

# Classical examples

- F. Klein, 1885: $\mathrm{ed}(\mathrm{S}_5) = 2$. ("Kroneker's theorem"?)

- J.-P. Serre, A. Grothendieck, 1958: Classified "special groups" over an algebraically closed field. Recall that $k$-group $G$ is called *special* if

$$H^1(K, G_K) = \{pt\}$$

for every field $K/k$. $G$ is special if and only if $\mathrm{ed}(G) = 0$.

- C. Procesi, 1967: $\mathrm{ed}(\mathrm{PGL}_n) \leq n^2$.

# Classical examples

- F. Klein, 1885: $\mathrm{ed}(\mathrm{S}_5) = 2$. ("Kroneker's theorem"?)

- J.-P. Serre, A. Grothendieck, 1958: Classified "special groups" over an algebraically closed field. Recall that $k$-group $G$ is called *special* if
$$H^1(K, G_K) = \{pt\}$$
for every field $K/k$. $G$ is special if and only if $\mathrm{ed}(G) = 0$.

- C. Procesi, 1967: $\mathrm{ed}(\mathrm{PGL}_n) \leq n^2$.

# Classical examples

- F. Klein, 1885: $\mathrm{ed}(\mathrm{S}_5) = 2$. ("Kroneker's theorem"?)

- J.-P. Serre, A. Grothendieck, 1958: Classified "special groups" over an algebraically closed field. Recall that $k$-group $G$ is called *special* if
$$H^1(K, G_K) = \{pt\}$$
for every field $K/k$. $G$ is special if and only if $\mathrm{ed}(G) = 0$.

- C. Procesi, 1967: $\mathrm{ed}(\mathrm{PGL}_n) \leq n^2$.

# Classical examples

- F. Klein, 1885: $\mathrm{ed}(\mathrm{S}_5) = 2$. ("Kroneker's theorem"?)

- J.-P. Serre, A. Grothendieck, 1958: Classified "special groups" over an algebraically closed field. Recall that $k$-group $G$ is called *special* if
$$H^1(K, G_K) = \{pt\}$$
for every field $K/k$. $G$ is special if and only if $\mathrm{ed}(G) = 0$.

- C. Procesi, 1967: $\mathrm{ed}(\mathrm{PGL}_n) \leq n^2$.

# Techniques for proving lower bounds on ed($G$)

- Bounds related to cohomological invariants of $G$.
- Bounds related to non-toral abelian subgroups of $G$.
- Bounds related to Brauer classes induced by a central extension

$$1 \to C \to G \to \overline{G} \to 1\,.$$

# Techniques for proving lower bounds on $\mathrm{ed}(G)$

- Bounds related to cohomological invariants of $G$.
- Bounds related to non-toral abelian subgroups of $G$.
- Bounds related to Brauer classes induced by a central extension

$$1 \to C \to G \to \overline{G} \to 1 .$$

# Techniques for proving lower bounds on ed($G$)

- Bounds related to cohomological invariants of $G$.
- Bounds related to non-toral abelian subgroups of $G$.
- Bounds related to Brauer classes induced by a central extension

$$1 \to C \to G \to \overline{G} \to 1\,.$$

# Cohomological invariants

A morphism of functors $\mathcal{F} \to H^d(\ast, \mu_n)$ is called a *cohomological invariant* of degree $d$; it is said to be nontrivial if $\mathcal{F}(K)$ contains a non-zero element of $H^d(K, \mu_n)$ for some $K/k$.

Observation (J.-P. Serre) Suppose $k$ is algebraically closed. If there exists a non-trivial cohomological invariant $\mathcal{F} \to H^d(\ast, \mu_n)$ then $\mathrm{ed}(\mathcal{F}) \geq d$.

Proof:

$$\begin{tikzcd}
\mathcal{F}(K) \arrow[r] & H^d(K, \mu_n) \\
\mathcal{F}(K_0) \arrow[r] \arrow[u] & H^d(K_0, \mu_n) \arrow[u]
\end{tikzcd}$$

If $\mathrm{trdeg}_k(K_0) < d$ then by the Serre Vanishing Theorem $H^d(K_0, \mu_n) = (0)$.

$\square$

# Cohomological invariants

A morphism of functors $\mathcal{F} \to H^d(\,*\,,\mu_n)$ is called a *cohomological invariant* of degree $d$; it is said to be nontrivial if $\mathcal{F}(K)$ contains a non-zero element of $H^d(K,\mu_n)$ for some $K/k$.

Observation (J.-P. Serre) Suppose $k$ is algebraically closed. If there exists a non-trivial cohomological invariant $\mathcal{F} \to H^d(\,*\,,\mu_n)$ then $\mathrm{ed}(\mathcal{F}) \geq d$.

Proof:

$$\begin{tikzcd} \mathcal{F}(K) \arrow[r] & H^d(K,\mu_n) \\ \mathcal{F}(K_0) \arrow[r] \arrow[u] & H^d(K_0,\mu_n)\,. \arrow[u] \end{tikzcd}$$

If $\mathrm{trdeg}_k(K_0) < d$ then by the Serre Vanishing Theorem $H^d(K_0,\mu_n) = (0)$. $\square$

# Cohomological invariants

A morphism of functors $\mathcal{F} \to H^d(\,*\,, \mu_n)$ is called a *cohomological invariant* of degree $d$; it is said to be nontrivial if $\mathcal{F}(K)$ contains a non-zero element of $H^d(K, \mu_n)$ for some $K/k$.

Observation (J.-P. Serre) Suppose $k$ is algebraically closed. If there exists a non-trivial cohomological invariant $\mathcal{F} \to H^d(\,*\,, \mu_n)$ then $\mathrm{ed}(\mathcal{F}) \geq d$.

Proof:

$$\begin{tikzcd}
\mathcal{F}(K) \arrow[r] & H^d(K, \mu_n) \\
\mathcal{F}(K_0) \arrow[r] \arrow[u] & H^d(K_0, \mu_n) \arrow[u]
\end{tikzcd}$$

If $\mathrm{trdeg}_k(K_0) < d$ then by the Serre Vanishing Theorem $H^d(K_0, \mu_n) = (0)$.

# Cohomological invariants

A morphism of functors $\mathcal{F} \to H^d(\,*\,, \mu_n)$ is called a *cohomological invariant* of degree $d$; it is said to be nontrivial if $\mathcal{F}(K)$ contains a non-zero element of $H^d(K, \mu_n)$ for some $K/k$.

Observation (J.-P. Serre) Suppose $k$ is algebraically closed. If there exists a non-trivial cohomological invariant $\mathcal{F} \to H^d(\,*\,, \mu_n)$ then $\mathrm{ed}(\mathcal{F}) \geq d$.

Proof:

$$\begin{tikzcd} \mathcal{F}(K) \arrow[r] & H^d(K, \mu_n) \\ \mathcal{F}(K_0) \arrow[r] \arrow[u] & H^d(K_0, \mu_n)\,. \arrow[u] \end{tikzcd}$$

If $\mathrm{trdeg}_k(K_0) < d$ then by the Serre Vanishing Theorem $H^d(K_0, \mu_n) = (0)$.

# Examples of cohomological invariants

- $\mathrm{ed}(\mathrm{O}_n) = n$. Cohomological invariant $H^1(K, \mathrm{O}_n) \to H^n(K, \mu_2)$: $n$th Stiefel-Whitney class of a quadratic form.

- $\mathrm{ed}(\mu_p^r) = r$. Cohomological invariant $H^1(K, \mu_p^r) \to H^r(K, \mu_p)$: cup product.

- $\mathrm{ed}(\mathrm{S}_n) \geq [n/2]$. Cohomological invariant $H^1(K, \mathrm{S}_n) \to H^{[n/2]}(K, \mu_2)$: $[n/2]$th Stiefel-Whitney class of the trace form of an étale algebra. Alternatively, (c) can be deduced from (b).

# Examples of cohomological invariants

- $\mathrm{ed}(\mathrm{O}_n) = n$. Cohomological invariant $H^1(K, \mathrm{O}_n) \to H^n(K, \mu_2)$: $n$th Stiefel-Whitney class of a quadratic form.
- $\mathrm{ed}(\mu_p^r) = r$. Cohomological invariant $H^1(K, \mu_p^r) \to H^r(K, \mu_p)$: cup product.
- $\mathrm{ed}(\mathrm{S}_n) \geq [n/2]$. Cohomological invariant $H^1(K, \mathrm{S}_n) \to H^{[n/2]}(K, \mu_2)$: $[n/2]$th Stiefel-Whitney class of the trace form of an étale algebra. Alternatively, (c) can be deduced from (b).

# Examples of cohomological invariants

- $\mathrm{ed}(\mathrm{O}_n) = n$. Cohomological invariant $H^1(K, \mathrm{O}_n) \to H^n(K, \mu_2)$: $n$th Stiefel-Whitney class of a quadratic form.

- $\mathrm{ed}(\mu_p^r) = r$. Cohomological invariant $H^1(K, \mu_p^r) \to H^r(K, \mu_p)$: cup product.

- $\mathrm{ed}(\mathrm{S}_n) \geq [n/2]$. Cohomological invariant $H^1(K, \mathrm{S}_n) \to H^{[n/2]}(K, \mu_2)$: $[n/2]$th Stiefel-Whitney class of the trace form of an étale algebra. Alternatively, (c) can be deduced from (b).

# Examples continued

- $\mathrm{ed}(\mathrm{PGL}_{p^r}) \geq 2r$. Cohomological invariant: $H^1(K, \mathrm{PGL}_n) \xrightarrow{\partial} H^2(K, \mu_{p^r}) \xrightarrow{p_r} H^{2r}(K, \mu_{p^r})$, where $p_r$ is the divided $r$th power map.
- $\mathrm{ed}(F_4) \geq 5$. Cohomological invariant: $H^1(K, F_4) \to H^5(K, \mu_2)$, first defined by Serre.

# Examples continued

- $\mathrm{ed}(\mathrm{PGL}_{p^r}) \geq 2r$. Cohomological invariant: $H^1(K, \mathrm{PGL}_n) \xrightarrow{\partial} H^2(K, \mu_{p^r}) \xrightarrow{p_r} H^{2r}(K, \mu_{p^r})$, where $p_r$ is the divided $r$th power map.

- $\mathrm{ed}(F_4) \geq 5$. Cohomological invariant: $H^1(K, F_4) \to H^5(K, \mu_2)$, first defined by Serre.

# Non-toral abelian subgroups

Theorem: (R.-Youssin, 2000; R.-Gille, 2007) If $G$ is connected, $A$ is a finite abelian subgroup of $G$ and char$(k)$ does not divide $|A|$, then

$$\mathrm{ed}_k(G) \geq \mathrm{rank}(A) - \mathrm{rank}\ C_G^0(A)\,.$$

Remarks:

- May pass to the algebraic closure $\overline{k}$.
- If $A$ lies in a torus of $G$ then the above inequality is vacuous.
- Most interesting case: $C_G^0(A)$ is finite. This happens iff $A$ is not contained in any proper parabolic subgroup of $G$.
- The shortest known proof relies on resolution of singularities. If $A$ is a $p$-group, Gabber's theorem on alterations can be used as a substitute.

# Non-toral abelian subgroups

Theorem: (R.-Youssin, 2000; R.-Gille, 2007) If $G$ is connected, $A$ is a finite abelian subgroup of $G$ and char($k$) does not divide $|A|$, then

$$\mathrm{ed}_k(G) \geq \mathrm{rank}(A) - \mathrm{rank}\ C_G^0(A)\,.$$

Remarks:

- May pass to the algebraic closure $\overline{k}$.
- If $A$ lies in a torus of $G$ then the above inequality is vacuous.
- Most interesting case: $C_G^0(A)$ is finite. This happens iff $A$ is not contained in any proper parabolic subgroup of $G$.
- The shortest known proof relies on resolution of singularities. If $A$ is a $p$-group, Gabber's theorem on alterations can be used as a substitute.

# Non-toral abelian subgroups

Theorem: (R.-Youssin, 2000; R.-Gille, 2007) If $G$ is connected, $A$ is a finite abelian subgroup of $G$ and $\mathrm{char}(k)$ does not divide $|A|$, then

$$\mathrm{ed}_k(G) \geq \mathrm{rank}(A) - \mathrm{rank}\ C_G^0(A)\,.$$

Remarks:

- May pass to the algebraic closure $\overline{k}$.
- If $A$ lies in a torus of $G$ then the above inequality is vacuous.
- Most interesting case: $C_G^0(A)$ is finite. This happens iff $A$ is not contained in any proper parabolic subgroup of $G$.
- The shortest known proof relies on resolution of singularities. If $A$ is a $p$-group, Gabber's theorem on alterations can be used as a substitute.

# Non-toral abelian subgroups

Theorem: (R.-Youssin, 2000; R.-Gille, 2007) If $G$ is connected, $A$ is a finite abelian subgroup of $G$ and $\mathrm{char}(k)$ does not divide $|A|$, then

$$\mathrm{ed}_k(G) \geq \mathrm{rank}(A) - \mathrm{rank}\ C_G^0(A)\,.$$

Remarks:

- May pass to the algebraic closure $\overline{k}$.
- If $A$ lies in a torus of $G$ then the above inequality is vacuous.
- Most interesting case: $C_G^0(A)$ is finite. This happens iff $A$ is not contained in any proper parabolic subgroup of $G$.
- The shortest known proof relies on resolution of singularities. If $A$ is a $p$-group, Gabber's theorem on alterations can be used as a substitute.

# Non-toral abelian subgroups

Theorem: (R.-Youssin, 2000; R.-Gille, 2007) If $G$ is connected, $A$ is a finite abelian subgroup of $G$ and $\mathrm{char}(k)$ does not divide $|A|$, then

$$\mathrm{ed}_k(G) \geq \mathrm{rank}(A) - \mathrm{rank}\ C_G^0(A)\,.$$

Remarks:

- May pass to the algebraic closure $\overline{k}$.
- If $A$ lies in a torus of $G$ then the above inequality is vacuous.
- Most interesting case: $C_G^0(A)$ is finite. This happens iff $A$ is not contained in any proper parabolic subgroup of $G$.
- The shortest known proof relies on resolution of singularities. If $A$ is a $p$-group, Gabber's theorem on alterations can be used as a substitute.

# Examples

- $\mathrm{ed}(\mathrm{SO}_n) \geq n-1$ for any $n \geq 3$,
- $\mathrm{ed}(\mathrm{PGL}_{p^s}) \geq 2s$
- $\mathrm{ed}(\mathrm{Spin}_n) \geq [n/2]$ for any $n \geq 11$.
- $\mathrm{ed}(\mathrm{G}_2) \geq 3$
- $\mathrm{ed}(\mathrm{F}_4) \geq 5$
- $\mathrm{ed}(\mathrm{E}_6^{sc}) \geq 4$
- $\mathrm{ed}(\mathrm{E}_7^{sc}) \geq 7$
- $\mathrm{ed}(\mathrm{E}_8) \geq 9$

Minor restrictions on $\mathrm{char}(k)$ apply.

Each inequality is proved by exhibiting a non-toral abelian subgroup $A \subset G$ whose centralizer is finite. For example, in part (a) we assume $\mathrm{char}(k) \neq 2$ and take $A \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}$ to be the subgroup of diagonal matrices in $\mathrm{SO}_n$.

# Examples

- $\mathrm{ed}(\mathrm{SO}_n) \geq n-1$ for any $n \geq 3$,
- $\mathrm{ed}(\mathrm{PGL}_{p^s}) \geq 2s$
- $\mathrm{ed}(\mathrm{Spin}_n) \geq [n/2]$ for any $n \geq 11$.
- $\mathrm{ed}(\mathrm{G}_2) \geq 3$
- $\mathrm{ed}(\mathrm{F}_4) \geq 5$
- $\mathrm{ed}(\mathrm{E}_6^{sc}) \geq 4$
- $\mathrm{ed}(\mathrm{E}_7^{sc}) \geq 7$
- $\mathrm{ed}(\mathrm{E}_8) \geq 9$

Minor restrictions on $\mathrm{char}(k)$ apply.

Each inequality is proved by exhibiting a non-toral abelian subgroup $A \subset G$ whose centralizer is finite. For example, in part (a) we assume $\mathrm{char}(k) \neq 2$ and take $A \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}$ to be the subgroup of diagonal matrices in $\mathrm{SO}_n$.

# Examples

- $\mathrm{ed}(\mathrm{SO}_n) \geq n - 1$ for any $n \geq 3$,
- $\mathrm{ed}(\mathrm{PGL}_{p^s}) \geq 2s$
- $\mathrm{ed}(\mathrm{Spin}_n) \geq [n/2]$ for any $n \geq 11$.
- $\mathrm{ed}(\mathrm{G}_2) \geq 3$
- $\mathrm{ed}(\mathrm{F}_4) \geq 5$
- $\mathrm{ed}(\mathrm{E}_6^{sc}) \geq 4$
- $\mathrm{ed}(\mathrm{E}_7^{sc}) \geq 7$
- $\mathrm{ed}(\mathrm{E}_8) \geq 9$

Minor restrictions on $\mathrm{char}(k)$ apply.

Each inequality is proved by exhibiting a non-toral abelian subgroup $A \subset G$ whose centralizer is finite. For example, in part (a) we assume $\mathrm{char}(k) \neq 2$ and take $A \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}$ to be the subgroup of diagonal matrices in $\mathrm{SO}_n$.

# Central extensions

**Theorem:** (Brosnan–R.–Vistoli, Karpenko—Merkurjev)
Suppose $1 \to C \to G \to \overline{G} \to 1$ is a central exact sequence of $k$-groups, with $C \simeq_k \mu_p$.
Assume that $k$ is a field of characteristic $\neq p$ containing a primitive $p$th root of unity. Then

$$\mathrm{ed}_k(G) \geq \gcd\{\dim(\rho)\} - \dim G\,,$$

where $\rho$ ranges over all $k$-representations of $G$ whose restriction to $C$ is faithful.

Karpenko and Merkurjev have extended this bound to the case where $C \simeq_k \mu_p^r$ for some $r \geq 1$.

# Central extensions

**Theorem:** (Brosnan–R.–Vistoli, Karpenko—Merkurjev)
Suppose $1 \to C \to G \to \overline{G} \to 1$ is a central exact sequence of $k$-groups, with $C \simeq_k \mu_p$.
Assume that $k$ is a field of characteristic $\neq p$ containing a primitive $p$th root of unity. Then

$$\mathrm{ed}_k(G) \geq \gcd\{\dim(\rho)\} - \dim G \,,$$

where $\rho$ ranges over all $k$-representations of $G$ whose restriction to $C$ is faithful.

Karpenko and Merkurjev have extended this bound to the case where $C \simeq_k \mu_p^r$ for some $r \geq 1$.

# Central extensions

**Theorem:** (Brosnan–R.–Vistoli, Karpenko—Merkurjev)
Suppose $1 \to C \to G \to \overline{G} \to 1$ is a central exact sequence of $k$-groups, with $C \simeq_k \mu_p$.
Assume that $k$ is a field of characteristic $\neq p$ containing a primitive $p$th root of unity. Then

$$\mathrm{ed}_k(G) \geq \gcd\{\dim(\rho)\} - \dim G\,,$$

where $\rho$ ranges over all $k$-representations of $G$ whose restriction to $C$ is faithful.

Karpenko and Merkurjev have extended this bound to the case where $C \simeq_k \mu_p^r$ for some $r \geq 1$.

# Applications

Brosnan–R.–Vistoli: $\mathrm{ed}(\mathrm{Spin}_n)$ increases exponentially with $n$.

An exponential lower bound can be obtained by applying the theorem to the central sequence

$$1 \to \mu_2 \to \mathrm{Spin}_n \to \mathrm{SO}_n \to 1\,.$$

(Karpenko – Merkurjev): Let $G$ be a finite $p$-group and $k$ be a field containing a primitive $p$th root of unity. Then

$$\mathrm{ed}_k(G) = \min \dim(\phi)\,, \tag{1}$$

where the minimum is taken over all faithful $k$-representations $\phi$ of $G$.

# Applications

Brosnan–R.–Vistoli: $\mathrm{ed}(\mathrm{Spin}_n)$ increases exponentially with $n$.

An exponential lower bound can be obtained by applying the theorem to the central sequence

$$1 \to \mu_2 \to \mathrm{Spin}_n \to \mathrm{SO}_n \to 1\,.$$

(Karpenko – Merkurjev): Let $G$ be a finite $p$-group and $k$ be a field containing a primitive $p$th root of unity. Then

$$\mathrm{ed}_k(G) = \min \dim(\phi)\,, \tag{1}$$

where the minimum is taken over all faithful $k$-representations $\phi$ of $G$.

# Applications

Brosnan–R.–Vistoli: $\mathrm{ed}(\mathrm{Spin}_n)$ increases exponentially with $n$.

An exponential lower bound can be obtained by applying the theorem to the central sequence

$$1 \to \mu_2 \to \mathrm{Spin}_n \to \mathrm{SO}_n \to 1\,.$$

(Karpenko – Merkurjev): Let $G$ be a finite $p$-group and $k$ be a field containing a primitive $p$th root of unity. Then

$$\mathrm{ed}_k(G) = \min \dim(\phi)\,, \tag{1}$$

where the minimum is taken over all faithful $k$-representations $\phi$ of $G$.

# Two types of problems

Suppose we are given a functor

$$\mathcal{F}\colon \mathsf{Fields}_k \to \mathsf{Sets}$$

and we would like to show that some (or every) $\alpha \in \mathcal{F}(K)$ has a certain property.

It is often useful to approach this problem in two steps. For the first step we choose a prime $p$ and ask whether or not $\alpha_L$ has the desired property for some prime-to-$p$ extension $L/K$. This is what I call a *Type 1 problem*.

If the answer is "no" for some $p$ then we are done.

If the answer is "yes" for every prime $p$, then the remaining problem is to determine whether or not $\alpha$ itself has the desired property. I refer to problems of this type as *Type 2 problems*.

# Two types of problems

Suppose we are given a functor

$$\mathcal{F}\colon \text{Fields}_k \to \text{Sets}$$

and we would like to show that some (or every) $\alpha \in \mathcal{F}(K)$ has a certain property.

It is often useful to approach this problem in two steps. For the first step we choose a prime $p$ and ask whether or not $\alpha_L$ has the desired property for some prime-to-$p$ extension $L/K$. This is what I call a *Type 1 problem*.

If the answer is "no" for some $p$ then we are done.

If the answer is "yes" for every prime $p$, then the remaining problem is to determine whether or not $\alpha$ itself has the desired property. I refer to problems of this type as *Type 2 problems*.

# Two types of problems

Suppose we are given a functor

$$\mathcal{F}\colon \text{Fields}_k \to \text{Sets}$$

and we would like to show that some (or every) $\alpha \in \mathcal{F}(K)$ has a certain property.

It is often useful to approach this problem in two steps. For the first step we choose a prime $p$ and ask whether or not $\alpha_L$ has the desired property for some prime-to-$p$ extension $L/K$. This is what I call a *Type 1 problem*.

If the answer is "no" for some $p$ then we are done.

If the answer is "yes" for every prime $p$, then the remaining problem is to determine whether or not $\alpha$ itself has the desired property. I refer to problems of this type as *Type 2 problems*.

# Two types of problems

Suppose we are given a functor

$$\mathcal{F}\colon \mathsf{Fields}_k \to \mathsf{Sets}$$

and we would like to show that some (or every) $\alpha \in \mathcal{F}(K)$ has a certain property.

It is often useful to approach this problem in two steps. For the first step we choose a prime $p$ and ask whether or not $\alpha_L$ has the desired property for some prime-to-$p$ extension $L/K$. This is what I call a *Type 1 problem*.

If the answer is "no" for some $p$ then we are done.

If the answer is "yes" for every prime $p$, then the remaining problem is to determine whether or not $\alpha$ itself has the desired property. I refer to problems of this type as *Type 2 problems*.

# Two types of problems

Suppose we are given a functor

$$\mathcal{F}\colon \text{Fields}_k \to \text{Sets}$$

and we would like to show that some (or every) $\alpha \in \mathcal{F}(K)$ has a certain property.

It is often useful to approach this problem in two steps. For the first step we choose a prime $p$ and ask whether or not $\alpha_L$ has the desired property for some prime-to-$p$ extension $L/K$. This is what I call a *Type 1 problem*.

If the answer is "no" for some $p$ then we are done.

If the answer is "yes" for every prime $p$, then the remaining problem is to determine whether or not $\alpha$ itself has the desired property. I refer to problems of this type as *Type 2 problems*.

# Essential dimension at $p$

Let $\mathcal{F}\colon \text{Fields}_k \to \text{Sets}$ be a functor and $\alpha \in \mathcal{F}(K)$ for some field $K/k$.

The essential dimension $\mathrm{ed}(\alpha; p)$ of $\alpha$ at a prime integer $p$ is defined as the minimal value of $\mathrm{ed}(\alpha_L)$, as $L$ ranges over all finite field extensions $L/K$ such that $p$ does not divide $[L : K]$.

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

# Essential dimension at $p$

Let $\mathcal{F}\colon \text{Fields}_k \to \text{Sets}$ be a functor and $\alpha \in \mathcal{F}(K)$ for some field $K/k$.

The essential dimension $\text{ed}(\alpha; p)$ of $\alpha$ at a prime integer $p$ is defined as the minimal value of $\text{ed}(\alpha_L)$, as $L$ ranges over all finite field extensions $L/K$ such that $p$ does not divide $[L:K]$.

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

# Essential dimension at $p$

Let $\mathcal{F}\colon$ Fields$_k \to$ Sets be a functor and $\alpha \in \mathcal{F}(K)$ for some field $K/k$.

The essential dimension $\mathrm{ed}(\alpha; p)$ of $\alpha$ at a prime integer $p$ is defined as the minimal value of $\mathrm{ed}(\alpha_L)$, as $L$ ranges over all finite field extensions $L/K$ such that $p$ does not divide $[L : K]$.

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

# Essential dimension at $p$, continued

In the case where $\mathcal{F}(K) = H^1(K, G)$ for some algebraic group $G$ defined over $k$, we will write $\mathrm{ed}(G; p)$ in place of $\mathrm{ed}(\mathcal{F}; p)$. Clearly, $\mathrm{ed}(\alpha; p) \le \mathrm{ed}(\alpha)$, $\mathrm{ed}(\mathcal{F}; p) \le \mathrm{ed}(\mathcal{F})$, and $\mathrm{ed}(G; p) \le \mathrm{ed}(G)$ for every prime $p$.

In the context of essential dimension:

Type 1 problem. Find $\mathrm{ed}(\alpha; p)$ or $\mathrm{ed}(\mathcal{F}; p)$ or $\mathrm{ed}(G; p)$ for some (or every) prime $p$.

Type 2 problem. Assuming $\mathrm{ed}(\alpha; p)$, $\mathrm{ed}(\mathcal{F}; p)$, or $\mathrm{ed}(G; p)$ is known for every prime $p$, find the "absolute" essential dimension $\mathrm{ed}(\alpha)$, $\mathrm{ed}(\mathcal{F})$, or $\mathrm{ed}(G)$.

# Essential dimension at $p$, continued

In the case where $\mathcal{F}(K) = H^1(K, G)$ for some algebraic group $G$ defined over $k$, we will write $\mathrm{ed}(G; p)$ in place of $\mathrm{ed}(\mathcal{F}; p)$. Clearly, $\mathrm{ed}(\alpha; p) \leq \mathrm{ed}(\alpha)$, $\mathrm{ed}(\mathcal{F}; p) \leq \mathrm{ed}(\mathcal{F})$, and $\mathrm{ed}(G; p) \leq \mathrm{ed}(G)$ for every prime $p$.

In the context of essential dimension:

Type 1 problem. Find $\mathrm{ed}(\alpha; p)$ or $\mathrm{ed}(\mathcal{F}; p)$ or $\mathrm{ed}(G; p)$ for some (or every) prime $p$.

Type 2 problem. Assuming $\mathrm{ed}(\alpha; p)$, $\mathrm{ed}(\mathcal{F}; p)$, or $\mathrm{ed}(G; p)$ is known for every prime $p$, find the "absolute" essential dimension $\mathrm{ed}(\alpha)$, $\mathrm{ed}(\mathcal{F})$, or $\mathrm{ed}(G)$.

# Essential dimension at $p$, continued

In the case where $\mathcal{F}(K) = H^1(K, G)$ for some algebraic group $G$ defined over $k$, we will write $\mathrm{ed}(G; p)$ in place of $\mathrm{ed}(\mathcal{F}; p)$. Clearly, $\mathrm{ed}(\alpha; p) \le \mathrm{ed}(\alpha)$, $\mathrm{ed}(\mathcal{F}; p) \le \mathrm{ed}(\mathcal{F})$, and $\mathrm{ed}(G; p) \le \mathrm{ed}(G)$ for every prime $p$.

In the context of essential dimension:

Type 1 problem. Find $\mathrm{ed}(\alpha; p)$ or $\mathrm{ed}(\mathcal{F}; p)$ or $\mathrm{ed}(G; p)$ for some (or every) prime $p$.

Type 2 problem. Assuming $\mathrm{ed}(\alpha; p)$, $\mathrm{ed}(\mathcal{F}; p)$, or $\mathrm{ed}(G; p)$ is known for every prime $p$, find the "absolute" essential dimension $\mathrm{ed}(\alpha)$, $\mathrm{ed}(\mathcal{F})$, or $\mathrm{ed}(G)$.

# $\mathrm{ed}(G)$ versus $\mathrm{ed}(G; p)$

A closer look at the three techniques we discussed of proving lower bounds of the form $\mathrm{ed}(G) \geq d$ reveals that in every case the argument can be modified to show that in fact $\mathrm{ed}(G; p) \geq d$ for some (naturally chosen) prime $p$. In other words, these techniques are well suited to Type 1 problems only.

This is a special case of the following more general but admittedly vague phenomenon.

**Observation:** Most existing methods in Galois cohomology and related areas apply to Type 1 problems only. On the other hand, many long-standing open problems are of Type 2.

# $\mathrm{ed}(G)$ versus $\mathrm{ed}(G; p)$

A closer look at the three techniques we discussed of proving lower bounds of the form $\mathrm{ed}(G) \geq d$ reveals that in every case the argument can be modified to show that in fact $\mathrm{ed}(G; p) \geq d$ for some (naturally chosen) prime $p$. In other words, these techniques are well suited to Type 1 problems only.

This is a special case of the following more general but admittedly vague phenomenon.

**Observation:** Most existing methods in Galois cohomology and related areas apply to Type 1 problems only. On the other hand, many long-standing open problems are of Type 2.

# ed($G$) versus ed($G; p$)

A closer look at the three techniques we discussed of proving lower bounds of the form $\text{ed}(G) \geq d$ reveals that in every case the argument can be modified to show that in fact $\text{ed}(G; p) \geq d$ for some (naturally chosen) prime $p$. In other words, these techniques are well suited to Type 1 problems only.

This is a special case of the following more general but admittedly vague phenomenon.

**Observation:** Most existing methods in Galois cohomology and related areas apply to Type 1 problems only. On the other hand, many long-standing open problems are of Type 2.

# Examples of Type 2 problems

- The cyclicity problem and the cross product problem for central simple algebras
- The torsion index problem (for simply connected or adjoint groups)
- The problem of computing the canonical dimension of a simple group
- Serre's conjecture on the splitting of a torsor
- The conjecture of Cassels and Swinnerton-Dyer on cubic hypersurfaces

## Examples of Type 2 problems

- The cyclicity problem and the cross product problem for central simple algebras
- The torsion index problem (for simply connected or adjoint groups)
- The problem of computing the canonical dimension of a simple group
- Serre's conjecture on the splitting of a torsor
- The conjecture of Cassels and Swinnerton-Dyer on cubic hypersurfaces

# Examples of Type 2 problems

- The cyclicity problem and the cross product problem for central simple algebras
- The torsion index problem (for simply connected or adjoint groups)
- The problem of computing the canonical dimension of a simple group
- Serre's conjecture on the splitting of a torsor
- The conjecture of Cassels and Swinnerton-Dyer on cubic hypersurfaces

# Examples of Type 2 problems

- The cyclicity problem and the cross product problem for central simple algebras
- The torsion index problem (for simply connected or adjoint groups)
- The problem of computing the canonical dimension of a simple group
- Serre's conjecture on the splitting of a torsor
- The conjecture of Cassels and Swinnerton-Dyer on cubic hypersurfaces

# Examples of Type 2 problems

- The cyclicity problem and the cross product problem for central simple algebras
- The torsion index problem (for simply connected or adjoint groups)
- The problem of computing the canonical dimension of a simple group
- Serre's conjecture on the splitting of a torsor
- The conjecture of Cassels and Swinnerton-Dyer on cubic hypersurfaces

# Examples of Type 2 problems

- The cyclicity problem and the cross product problem for central simple algebras
- The torsion index problem (for simply connected or adjoint groups)
- The problem of computing the canonical dimension of a simple group
- Serre's conjecture on the splitting of a torsor
- The conjecture of Cassels and Swinnerton-Dyer on cubic hypersurfaces

# Another Type 2 problem

In the context of essential dimension, while we know that for some finite groups $G$,

$$\mathrm{ed}(G) > \mathrm{ed}(G;p)$$

for every prime $p$, the only natural examples where we can prove this are in low dimensions, with $\mathrm{ed}(G) \leq 3$ or (with greater effort) 4.

# Open problem 1: What is $\mathrm{ed}(\mathrm{S}_n)$?

This is a classical question, loosely related to the algebraic form of Hilbert's 13th problem.

In classical language, $\mathrm{ed}(\mathrm{S}_n)$ is a measure of how much the general polynomials,

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \,,$$

where $a_1, \ldots, a_n$ are independent variables, can be reduced by a Tschirnhaus transformation. That is, $\mathrm{ed}(\mathrm{S}_n)$ is the minimal possible number of algebraically independent elements among the coefficients $b_1, \ldots, b_n$ of a polynomial

$$g(y) = y^n + b_1 y^{n-1} + \cdots + b_n$$

such that $f(x)$ can be reduced to $g(y)$ by a Tschirnhaus transformation.

# Open problem 1: What is $\mathrm{ed}(\mathrm{S}_n)$?

This is a classical question, loosely related to the algebraic form of Hilbert's 13th problem.

In classical language, $\mathrm{ed}(\mathrm{S}_n)$ is a measure of how much the general polynomials,

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \,,$$

where $a_1, \ldots, a_n$ are independent variables, can be reduced by a Tschirnhaus transformation. That is, $\mathrm{ed}(\mathrm{S}_n)$ is the minimal possible number of algebraically independent elements among the coefficients $b_1, \ldots, b_n$ of a polynomial

$$g(y) = y^n + b_1 y^{n-1} + \cdots + b_n$$

such that $f(x)$ can be reduced to $g(y)$ by a Tschirnhaus transformation.

# More on $\mathrm{ed}(\mathrm{S}_n)$

The problem of computing $\mathrm{ed}(\mathrm{S}_n)$ turns out to be of Type 2. For simplicity, let us assume that $\mathrm{char}(k) = 0$. Then $\mathrm{ed}(\mathrm{S}_n; p) = [n/p]$, is known for every prime $p$. For the "absolute" essential dimension, we only know that

$$[n/2] \leq \mathrm{ed}(\mathrm{S}_n) \leq n - 3$$

for every $n \geq 5$.

In particular, $\mathrm{ed}(\mathrm{S}_5) = 2$ and $\mathrm{ed}(\mathrm{S}_6) = 3$. It is also easy to see that $\mathrm{ed}(\mathrm{S}_2) = \mathrm{ed}(\mathrm{S}_3) = 1$ and $\mathrm{ed}(\mathrm{S}_4) = 2$.

Theorem (A. Duncan, 2010): $\mathrm{ed}(\mathrm{S}_7) = 4$.

The proof relies on recent work in Mori theory, due to Yu. Prokhorov.

# More on $\mathrm{ed}(\mathrm{S}_n)$

The problem of computing $\mathrm{ed}(\mathrm{S}_n)$ turns out to be of Type 2. For simplicity, let us assume that $\mathrm{char}(k) = 0$. Then $\mathrm{ed}(\mathrm{S}_n; p) = [n/p]$, is known for every prime $p$. For the "absolute" essential dimension, we only know that

$$[n/2] \leq \mathrm{ed}(\mathrm{S}_n) \leq n - 3$$

for every $n \geq 5$.
In particular, $\mathrm{ed}(\mathrm{S}_5) = 2$ and $\mathrm{ed}(\mathrm{S}_6) = 3$. It is also easy to see that $\mathrm{ed}(\mathrm{S}_2) = \mathrm{ed}(\mathrm{S}_3) = 1$ and $\mathrm{ed}(\mathrm{S}_4) = 2$.

Theorem (A. Duncan, 2010): $\mathrm{ed}(\mathrm{S}_7) = 4$.

The proof relies on recent work in Mori theory, due to Yu. Prokhorov.

# More on $\mathrm{ed}(\mathrm{S}_n)$

The problem of computing $\mathrm{ed}(\mathrm{S}_n)$ turns out to be of Type 2.
For simplicity, let us assume that $\mathrm{char}(k) = 0$. Then
$\mathrm{ed}(\mathrm{S}_n; p) = [n/p]$, is known for every prime $p$. For the "absolute" essential dimension, we only know that

$$[n/2] \leq \mathrm{ed}(\mathrm{S}_n) \leq n - 3$$

for every $n \geq 5$.
In particular, $\mathrm{ed}(\mathrm{S}_5) = 2$ and $\mathrm{ed}(\mathrm{S}_6) = 3$. It is also easy to see that $\mathrm{ed}(\mathrm{S}_2) = \mathrm{ed}(\mathrm{S}_3) = 1$ and $\mathrm{ed}(\mathrm{S}_4) = 2$.

Theorem (A. Duncan, 2010): $\mathrm{ed}(\mathrm{S}_7) = 4$.

The proof relies on recent work in Mori theory, due to Yu. Prokhorov.

# More on $\mathrm{ed}(\mathsf{S}_n)$

The problem of computing $\mathrm{ed}(\mathsf{S}_n)$ turns out to be of Type 2. For simplicity, let us assume that $\mathrm{char}(k) = 0$. Then $\mathrm{ed}(\mathsf{S}_n; p) = [n/p]$, is known for every prime $p$. For the "absolute" essential dimension, we only know that

$$[n/2] \leq \mathrm{ed}(\mathsf{S}_n) \leq n - 3$$

for every $n \geq 5$.
In particular, $\mathrm{ed}(\mathsf{S}_5) = 2$ and $\mathrm{ed}(\mathsf{S}_6) = 3$. It is also easy to see that $\mathrm{ed}(\mathsf{S}_2) = \mathrm{ed}(\mathsf{S}_3) = 1$ and $\mathrm{ed}(\mathsf{S}_4) = 2$.

Theorem (A. Duncan, 2010): $\mathrm{ed}(\mathsf{S}_7) = 4$.

The proof relies on recent work in Mori theory, due to Yu. Prokhorov.

# Open problem 2: What is $\mathrm{ed}(\mathrm{PGL}_n)$?

This appears to be out of reach for now, except for a few small values of $n$. On the other hand, there has been recent progress on computing $\mathrm{ed}(\mathrm{PGL}_n; p)$?
May assume that $n = p^r$. It is easy to see that $\mathrm{ed}(\mathrm{PGL}_p; p) = 2$.

**Theorem:** For $r \geq 2$,

$$(r-1)p^r + 1 \leq \mathrm{ed}(\mathrm{PGL}_{p^r}; p) \leq p^{2r-2} + 1\,.$$

The lower bound is due to Merkurjev and the upper bound is due to his student A. Ruozzi. In particular,

$$\mathrm{ed}(\mathrm{PGL}_{p^2}; p) = p^2 + 1 \text{ and } \mathrm{ed}(\mathrm{PGL}_8; 2) = 17.$$

Of course, in general there is still a wide gap between $(r-1)p^r + 1$ and $p^{2r-2} + 1$.

# Open problem 2: What is $\mathrm{ed}(\mathrm{PGL}_n)$?

This appears to be out of reach for now, except for a few small values of $n$. On the other hand, there has been recent progress on computing $\mathrm{ed}(\mathrm{PGL}_n; p)$?

May assume that $n = p^r$. It is easy to see that $\mathrm{ed}(\mathrm{PGL}_p; p) = 2$.

**Theorem:** For $r \geq 2$,

$$(r-1)p^r + 1 \leq \mathrm{ed}(\mathrm{PGL}_{p^r}; p) \leq p^{2r-2} + 1\,.$$

The lower bound is due to Merkurjev and the upper bound is due to his student A. Ruozzi. In particular,

$$\mathrm{ed}(\mathrm{PGL}_{p^2}; p) = p^2 + 1 \text{ and } \mathrm{ed}(\mathrm{PGL}_8; 2) = 17.$$

Of course, in general there is still a wide gap between $(r-1)p^r + 1$ and $p^{2r-2} + 1$.

# Open problem 2: What is $\mathrm{ed}(\mathrm{PGL}_n)$?

This appears to be out of reach for now, except for a few small values of $n$. On the other hand, there has been recent progress on computing $\mathrm{ed}(\mathrm{PGL}_n; p)$?
May assume that $n = p^r$. It is easy to see that $\mathrm{ed}(\mathrm{PGL}_p; p) = 2$.

**Theorem:** For $r \geq 2$,

$$(r-1)p^r + 1 \leq \mathrm{ed}(\mathrm{PGL}_{p^r}; p) \leq p^{2r-2} + 1\,.$$

The lower bound is due to Merkurjev and the upper bound is due to his student A. Ruozzi. In particular,

$$\mathrm{ed}(\mathrm{PGL}_{p^2}; p) = p^2 + 1 \text{ and } \mathrm{ed}(\mathrm{PGL}_8; 2) = 17.$$

Of course, in general there is still a wide gap between $(r-1)p^r + 1$ and $p^{2r-2} + 1$.

# Open problem 2: What is $\mathrm{ed}(\mathrm{PGL}_n)$?

This appears to be out of reach for now, except for a few small values of $n$. On the other hand, there has been recent progress on computing $\mathrm{ed}(\mathrm{PGL}_n; p)$?
May assume that $n = p^r$. It is easy to see that $\mathrm{ed}(\mathrm{PGL}_p; p) = 2$.

**Theorem:** For $r \geq 2$,

$$(r-1)p^r + 1 \leq \mathrm{ed}(\mathrm{PGL}_{p^r}; p) \leq p^{2r-2} + 1\,.$$

The lower bound is due to Merkurjev and the upper bound is due to his student A. Ruozzi. In particular,

$$\mathrm{ed}(\mathrm{PGL}_{p^2}; p) = p^2 + 1 \text{ and } \mathrm{ed}(\mathrm{PGL}_8; 2) = 17.$$

Of course, in general there is still a wide gap between $(r-1)p^r + 1$ and $p^{2r-2} + 1$.

# Open problem 2: What is $\mathrm{ed}(\mathrm{PGL}_n)$?

This appears to be out of reach for now, except for a few small values of $n$. On the other hand, there has been recent progress on computing $\mathrm{ed}(\mathrm{PGL}_n; p)$?
May assume that $n = p^r$. It is easy to see that $\mathrm{ed}(\mathrm{PGL}_p; p) = 2$.

**Theorem:** For $r \geq 2$,

$$(r-1)p^r + 1 \leq \mathrm{ed}(\mathrm{PGL}_{p^r}; p) \leq p^{2r-2} + 1\,.$$

The lower bound is due to Merkurjev and the upper bound is due to his student A. Ruozzi. In particular,

$$\mathrm{ed}(\mathrm{PGL}_{p^2}; p) = p^2 + 1 \text{ and } \mathrm{ed}(\mathrm{PGL}_8; 2) = 17.$$

Of course, in general there is still a wide gap between $(r-1)p^r + 1$ and $p^{2r-2} + 1$.

# Open problem 2: What is $\mathrm{ed}(\mathrm{PGL}_n)$?

This appears to be out of reach for now, except for a few small values of $n$. On the other hand, there has been recent progress on computing $\mathrm{ed}(\mathrm{PGL}_n; p)$?
May assume that $n = p^r$. It is easy to see that $\mathrm{ed}(\mathrm{PGL}_p; p) = 2$.

**Theorem:** For $r \geq 2$,

$$(r-1)p^r + 1 \leq \mathrm{ed}(\mathrm{PGL}_{p^r}; p) \leq p^{2r-2} + 1 .$$

The lower bound is due to Merkurjev and the upper bound is due to his student A. Ruozzi. In particular,

$$\mathrm{ed}(\mathrm{PGL}_{p^2}; p) = p^2 + 1 \text{ and } \mathrm{ed}(\mathrm{PGL}_8; 2) = 17.$$

Of course, in general there is still a wide gap between $(r-1)p^r + 1$ and $p^{2r-2} + 1$.

# Open problem 3: New cohomological invariants?

Some of the lower bounds on $\mathrm{ed}(G;p) \geq d$ obtain by the fixed point method can be reproduced by considering cohomological invariants

$$H^1(*, G) \to H^d(*, \mu_p)\,.$$

In other cases, this cannot be done using any known cohomological invariants. This suggests where one might look for new cohomological invariants (but does not prove that they have to exist!).

In particular, is there

(a) a cohomological invariant of $\mathrm{PGL}_{p^r}$ of degree $2r$ with coefficients in $\mu_p$?

(b) a cohomological invariant of the (split) simply connected $E_7$ of degree 7 with coefficients in $\mu_2$?

(c) a cohomological invariant of the (split) $E_8$ of degree 9 with coefficients in $E_8$?

# Open problem 3: New cohomological invariants?

Some of the lower bounds on $\mathrm{ed}(G;p) \geq d$ obtain by the fixed point method can be reproduced by considering cohomological invariants

$$H^1(*, G) \to H^d(*, \mu_p)\,.$$

In other cases, this cannot be done using any known cohomological invariants. This suggests where one might look for new cohomological invariants (but does not prove that they have to exist!).

In particular, is there

(a) a cohomological invariant of $\mathrm{PGL}_{p^r}$ of degree $2r$ with coefficients in $\mu_p$?

(b) a cohomological invariant of the (split) simply connected $E_7$ of degree 7 with coefficients in $\mu_2$?

(c) a cohomological invariant of the (split) $E_8$ of degree 9 with coefficients in $E_8$?