Hilbert's 13th Problem for algebraic groups

Zinovy Reichstein

Department of Mathematics
University of British Columbia

June 2021
Banff

Solving polynomials

Classical problem: Solve a polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

of degree n in one variable. Here $a_1, \ldots, a_n$ are elements of some given field K. We fix a base field $k \subset K$. Often $K = k(a_1, \ldots, a_n)$.

Solving polynomials

Classical problem: Solve a polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

of degree n in one variable. Here $a_1, \ldots, a_n$ are elements of some given field K. We fix a base field $k \subset K$. Often $K = k(a_1, \ldots, a_n)$.
Here by "solving" I mean finding a procedure or a formula which produces a solution (or even better, every solution) x for a given set of coefficients $a_1, \ldots, a_n$.

Solving polynomials

Classical problem: Solve a polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

of degree n in one variable. Here $a_1, \ldots, a_n$ are elements of some given field K. We fix a base field $k \subset K$. Often $K = k(a_1, \ldots, a_n)$.
Here by "solving" I mean finding a procedure or a formula which produces a solution (or even better, every solution) x for a given set of coefficients $a_1, \ldots, a_n$. The terms "procedure" and "formula" are ambiguous.

Solving polynomials

Classical problem: Solve a polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

of degree n in one variable. Here $a_1, \ldots, a_n$ are elements of some given field K. We fix a base field $k \subset K$. Often $K = k(a_1, \ldots, a_n)$.
Here by "solving" I mean finding a procedure or a formula which produces a solution (or even better, every solution) x for a given set of coefficients $a_1, \ldots, a_n$. The terms "procedure" and "formula" are ambiguous. To get a well-posed problem, we need to specify what kinds of operations we are allowed to perform.

Solving polynomials

Classical problem: Solve a polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

of degree n in one variable. Here $a_1, \ldots, a_n$ are elements of some given field K. We fix a base field $k \subset K$. Often $K = k(a_1, \ldots, a_n)$.
Here by "solving" I mean finding a procedure or a formula which produces a solution (or even better, every solution) x for a given set of coefficients $a_1, \ldots, a_n$. The terms "procedure" and "formula" are ambiguous. To get a well-posed problem, we need to specify what kinds of operations we are allowed to perform. Elements of the base field k and the coefficients $a_1, \ldots, a_n$ of f are assumed to be given; we want to obtain each root of f by performing these operations in a finite number of steps.

Solving polynomials II

In the simplest setting we are only allowed to perform the four arithmetic operations: addition, subtraction, multiplication and division.

Solving polynomials II

In the simplest setting we are only allowed to perform the four arithmetic operations: addition, subtraction, multiplication and division.

In other words, we are asking if roots of $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$ can be expressed as a rational function of $a_1, \ldots, a_n$.

Solving polynomials II

In the simplest setting we are only allowed to perform the four arithmetic operations: addition, subtraction, multiplication and division.

In other words, we are asking if roots of $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ can be expressed as a rational function of $a_1, \ldots, a_n$.

For a general polynomial of degree $n \geqslant 2$, the answer is clearly "no".

Solving polynomials in radicals

A more interesting problem is "solving polynomials in radicals".

Solving polynomials in radicals

A more interesting problem is "solving polynomials in radicals".

Here one is allowed to use the four arithmetic operations and radicals of any degree, where the mth radical (or root) of t is a solution to

$$x^m - t = 0.$$

Solving polynomials in radicals

A more interesting problem is "solving polynomials in radicals".

Here one is allowed to use the four arithmetic operations and radicals of any degree, where the mth radical (or root) of t is a solution to

$$x^m - t = 0.$$

Once again, we want to obtain the roots of

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

in a finite number of steps, using these operations.

Solving polynomials in radicals

A more interesting problem is "solving polynomials in radicals".

Here one is allowed to use the four arithmetic operations and radicals of any degree, where the mth radical (or root) of t is a solution to

$$x^m - t = 0.$$

Once again, we want to obtain the roots of

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

in a finite number of steps, using these operations.

The answer is "yes" is $n \leqslant 4$ and "no" if $n \geqslant 5$ (Ruffini, Abel, Galois).

From polynomials to torsors

If the polynomial

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

is separable over a field K, we can think of the problem of finding its roots in geometric terms as follows.

From polynomials to torsors

If the polynomial

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

is separable over a field K, we can think of the problem of finding its roots in geometric terms as follows.

Consider the n-dimensional étale algebra E/K, where $E = K[x]/(f(x))$.

From polynomials to torsors

If the polynomial

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

is separable over a field K, we can think of the problem of finding its roots in geometric terms as follows.

Consider the n-dimensional étale algebra E/K, where $E = K[x]/(f(x))$. The class of this algebra in $H^1(K, \mathrm{S}_n)$ is represented by the S_n-torsor

$$\tau\colon T \to \mathrm{Spec}(K)\,,$$

where $T = \mathrm{Spec}(E)$.

From polynomials to torsors

If the polynomial

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

is separable over a field K, we can think of the problem of finding its roots in geometric terms as follows.

Consider the n-dimensional étale algebra E/K, where $E = K[x]/(f(x))$. The class of this algebra in $H^1(K, \mathrm{S}_n)$ is represented by the S_n-torsor

$$\tau \colon T \to \mathrm{Spec}(K)\,,$$

where $T = \mathrm{Spec}(E)$. The two questions we have asked now become:

From polynomials to torsors

If the polynomial

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

is separable over a field K, we can think of the problem of finding its roots in geometric terms as follows.

Consider the n-dimensional étale algebra E/K, where $E = K[x]/(f(x))$. The class of this algebra in $H^1(K, \mathrm{S}_n)$ is represented by the S_n-torsor

$$\tau \colon T \to \mathrm{Spec}(K)\,,$$

where $T = \mathrm{Spec}(E)$. The two questions we have asked now become:

(1) Is every S_n-torsor $\tau \colon T \to \mathrm{Spec}(K)$ split? (No, if $n \geqslant 2$.)

From polynomials to torsors

If the polynomial

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

is separable over a field K, we can think of the problem of finding its roots in geometric terms as follows.

Consider the n-dimensional étale algebra E/K, where $E = K[x]/(f(x))$. The class of this algebra in $H^1(K, \mathrm{S}_n)$ is represented by the S_n-torsor

$$\tau\colon\ T \to \mathrm{Spec}(K)\,,$$

where $T = \mathrm{Spec}(E)$. The two questions we have asked now become:

(1) Is every S_n-torsor $\tau\colon\ T \to \mathrm{Spec}(K)$ split? (No, if $n \geqslant 2$.)

(2) Can every S_n-torsor $\tau\colon\ T \to \mathrm{Spec}(K)$ be split by a solvable field extension L/K? (No, if $n \geqslant 5$.)

From S_n to an arbitrary algebraic group

The same questions can be asked if we replace S_n by an arbitrary algebraic group G defined over a field k.

From S_n to an arbitrary algebraic group

The same questions can be asked if we replace S_n by an arbitrary algebraic group G defined over a field k.

(1) Is every G-torsor $T \to \mathrm{Spec}(K)$ split? Here K is a field containing k.

From S_n to an arbitrary algebraic group

The same questions can be asked if we replace S_n by an arbitrary algebraic group G defined over a field k.

(1) Is every G-torsor $T \to \mathrm{Spec}(K)$ split? Here K is a field containing k.

(2) Can every G-torsor $T \to \mathrm{Spec}(K)$ be split by a solvable field extension L/K?

From S_n to an arbitrary algebraic group

The same questions can be asked if we replace S_n by an arbitrary algebraic group G defined over a field k.

(1) Is every G-torsor $T \to \mathrm{Spec}(K)$ split? Here K is a field containing k.

(2) Can every G-torsor $T \to \mathrm{Spec}(K)$ be split by a solvable field extension L/K?

If G is a (discrete) finite group, the answers are the same as before:

From S_n to an arbitrary algebraic group

The same questions can be asked if we replace S_n by an arbitrary algebraic group G defined over a field k.

(1) Is every G-torsor $T \to \mathrm{Spec}(K)$ split? Here K is a field containing k.

(2) Can every G-torsor $T \to \mathrm{Spec}(K)$ be split by a solvable field extension L/K?

If G is a (discrete) finite group, the answers are the same as before:
(1) "No", unless $G = 1$, and

From S_n to an arbitrary algebraic group

The same questions can be asked if we replace S_n by an arbitrary algebraic group G defined over a field k.

(1) Is every G-torsor $T \to \mathrm{Spec}(K)$ split? Here K is a field containing k.

(2) Can every G-torsor $T \to \mathrm{Spec}(K)$ be split by a solvable field extension L/K?

If G is a (discrete) finite group, the answers are the same as before:
(1) "No", unless $G = 1$, and (2) "No", unless G is solvable.

In general, groups satisfying (1) are called "special". These groups have been studies and classified since the 1950s.

From S_n to an arbitrary algebraic group

The same questions can be asked if we replace S_n by an arbitrary algebraic group G defined over a field k.

(1) Is every G-torsor $T \to \mathrm{Spec}(K)$ split? Here K is a field containing k.

(2) Can every G-torsor $T \to \mathrm{Spec}(K)$ be split by a solvable field extension L/K?

If G is a (discrete) finite group, the answers are the same as before: (1) "No", unless $G = 1$, and (2) "No", unless G is solvable.

In general, groups satisfying (1) are called "special". These groups have been studies and classified since the 1950s. In particular, Serre showed that a special group is linear and connected (1958).

From S_n to an arbitrary algebraic group

The same questions can be asked if we replace S_n by an arbitrary algebraic group G defined over a field k.

(1) Is every G-torsor $T \to \text{Spec}(K)$ split? Here K is a field containing k.

(2) Can every G-torsor $T \to \text{Spec}(K)$ be split by a solvable field extension L/K?

If G is a (discrete) finite group, the answers are the same as before: (1) "No", unless $G = 1$, and (2) "No", unless G is solvable.

In general, groups satisfying (1) are called "special". These groups have been studies and classified since the 1950s. In particular, Serre showed that a special group is linear and connected (1958).

If G is connected, then (2) has a positive answer in many cases but is an open problem in general.

From S_n to an arbitrary algebraic group

The same questions can be asked if we replace S_n by an arbitrary algebraic group G defined over a field k.

(1) Is every G-torsor $T \to \text{Spec}(K)$ split? Here K is a field containing k.

(2) Can every G-torsor $T \to \text{Spec}(K)$ be split by a solvable field extension L/K?

If G is a (discrete) finite group, the answers are the same as before: (1) "No", unless $G = 1$, and (2) "No", unless G is solvable.

In general, groups satisfying (1) are called "special". These groups have been studies and classified since the 1950s. In particular, Serre showed that a special group is linear and connected (1958).

If G is connected, then (2) has a positive answer in many cases but is an open problem in general. For example, for $G = \text{PGL}_n$, the answer is "yes" by the Merkurjev-Suslin Theorem.

A Theorem of Tits

More generally, we have the following.

A Theorem of Tits

More generally, we have the following.

Theorem (Tits, 1990): Let G be an (almost) simple linear algebraic group over a field K of any type, other than E_8.

A Theorem of Tits

More generally, we have the following.

Theorem (Tits, 1990): Let G be an (almost) simple linear algebraic group over a field K of any type, other than E_8. Then every G-torsor $T \to \mathrm{Spec}(K)$ can be split by a root extension L/K.

A Theorem of Tits

More generally, we have the following.

Theorem (Tits, 1990): Let G be an (almost) simple linear algebraic group over a field K of any type, other than E_8. Then every G-torsor $T \to \mathrm{Spec}(K)$ can be split by a root extension L/K.

Note that in characteristic 0 a root extension is the same thing as a solvable extension.

A Theorem of Tits

More generally, we have the following.

Theorem (Tits, 1990): Let G be an (almost) simple linear algebraic group over a field K of any type, other than E_8. Then every G-torsor $T \to \mathrm{Spec}(K)$ can be split by a root extension L/K.

Note that in characteristic 0 a root extension is the same thing as a solvable extension.

Question 1 (Tits): Is this true if G is of type E_8?

A Theorem of Tits

More generally, we have the following.

Theorem (Tits, 1990): Let G be an (almost) simple linear algebraic group over a field K of any type, other than E_8. Then every G-torsor $T \to \mathrm{Spec}(K)$ can be split by a root extension L/K.

Note that in characteristic 0 a root extension is the same thing as a solvable extension.

Question 1 (Tits): Is this true if G is of type E_8?

The answer is not known.

A Theorem of Tits

More generally, we have the following.

Theorem (Tits, 1990): Let G be an (almost) simple linear algebraic group over a field K of any type, other than E_8. Then every G-torsor $T \to \mathrm{Spec}(K)$ can be split by a root extension L/K.

Note that in characteristic 0 a root extension is the same thing as a solvable extension.

Question 1 (Tits): Is this true if G is of type E_8?

The answer is not known. The following slightly easier question is also wide open.

A Theorem of Tits

More generally, we have the following.

Theorem (Tits, 1990): Let G be an (almost) simple linear algebraic group over a field K of any type, other than E_8. Then every G-torsor $T \to \mathrm{Spec}(K)$ can be split by a root extension L/K.

Note that in characteristic 0 a root extension is the same thing as a solvable extension.

Question 1 (Tits): Is this true if G is of type E_8?

The answer is not known. The following slightly easier question is also wide open. Let us say that a finite group is almost solvable if its composition factors are either cyclic or A_5.

A Theorem of Tits

More generally, we have the following.

Theorem (Tits, 1990): Let G be an (almost) simple linear algebraic group over a field K of any type, other than E_8. Then every G-torsor $T \to \mathrm{Spec}(K)$ can be split by a root extension L/K.

Note that in characteristic 0 a root extension is the same thing as a solvable extension.

Question 1 (Tits): Is this true if G is of type E_8?

The answer is not known. The following slightly easier question is also wide open. Let us say that a finite group is almost solvable if its composition factors are either cyclic or A_5.

Question 2 (also Tits?) Is it true that every E_8-torsor $T \to \mathrm{Spec}(K)$ is split by a Galois field extension L/K with almost solvable Galois group $\mathrm{Gal}(L/K)$?

Beyond solvable extensions

Since Questions 1 and 2 are out of reach at the moment, I will consider a different but related problem by allowing a broader class of splitting extensions.

Beyond solvable extensions

Since Questions 1 and 2 are out of reach at the moment, I will consider a different but related problem by allowing a broader class of splitting extensions. Specifically, we will ask if every G-torsor can be split by finite field extensions of level 1 or more generally, of level $\leqslant d$ for a given positive integer d.

Beyond solvable extensions

Since Questions 1 and 2 are out of reach at the moment, I will consider a different but related problem by allowing a broader class of splitting extensions. Specifically, we will ask if every G-torsor can be split by finite field extensions of level 1 or more generally, of level $\leqslant d$ for a given positive integer d. I will define the level of a finite field extension in a few minutes.

Beyond solvable extensions

Since Questions 1 and 2 are out of reach at the moment, I will consider a different but related problem by allowing a broader class of splitting extensions. Specifically, we will ask if every G-torsor can be split by finite field extensions of level 1 or more generally, of level $\leqslant d$ for a given positive integer d. I will define the level of a finite field extension in a few minutes. All solvable extensions are of level 1.

Beyond solvable extensions

Since Questions 1 and 2 are out of reach at the moment, I will consider a different but related problem by allowing a broader class of splitting extensions. Specifically, we will ask if every G-torsor can be split by finite field extensions of level 1 or more generally, of level $\leqslant d$ for a given positive integer d. I will define the level of a finite field extension in a few minutes. All solvable extensions are of level 1.

This new problem is related to (the algebraic form of) Hilbert's 13th Problem and has deep classical roots.

Beyond solvable extensions

Since Questions 1 and 2 are out of reach at the moment, I will consider a different but related problem by allowing a broader class of splitting extensions. Specifically, we will ask if every G-torsor can be split by finite field extensions of level 1 or more generally, of level $\leqslant d$ for a given positive integer d. I will define the level of a finite field extension in a few minutes. All solvable extensions are of level 1.

This new problem is related to (the algebraic form of) Hilbert's 13th Problem and has deep classical roots.

For a finite group this new problem is harder than the problem of solving polynomials in radicals; there are no results analogous to the theorem of Abel, Ruffini and Galois in this setting.

Beyond solvable extensions

Since Questions 1 and 2 are out of reach at the moment, I will consider a different but related problem by allowing a broader class of splitting extensions. Specifically, we will ask if every G-torsor can be split by finite field extensions of level 1 or more generally, of level $\leqslant d$ for a given positive integer d. I will define the level of a finite field extension in a few minutes. All solvable extensions are of level 1.

This new problem is related to (the algebraic form of) Hilbert's 13th Problem and has deep classical roots.

For a finite group this new problem is harder than the problem of solving polynomials in radicals; there are no results analogous to the theorem of Abel, Ruffini and Galois in this setting.

However, for a connected group (and specifically for E_8) this problem turns out to be more accessible.

Polynomials of degree 5

Theorem (Bring, 1786): Let $f(x) = x^5 + a_1 x^4 + \ldots + a_5$ be a polynomial of degree 5 over a solvably closed field K.

Polynomials of degree 5

Theorem (Bring, 1786): Let $f(x) = x^5 + a_1x^4 + \ldots + a_5$ be a polynomial of degree 5 over a solvably closed field K. Then every root of $f(x)$ lies in the extension L/K obtained by adjoining a root of a polynomial of the form $x^5 + tx + t$, for some $t \in K$.

Polynomials of degree 5

Theorem (Bring, 1786): Let $f(x) = x^5 + a_1 x^4 + \ldots + a_5$ be a polynomial of degree 5 over a solvably closed field K. Then every root of $f(x)$ lies in the extension L/K obtained by adjoining a root of a polynomial of the form $x^5 + tx + t$, for some $t \in K$.

In other words, we can obtain every root of $f(x)$ from $a_1, \ldots, a_5$ and elements of the base field k, if we are allowed to apply the four arithmetic operations, extract roots and adjoin roots of polynomials of the form $x^5 + tx + t$.

Polynomials of degree 5

Theorem (Bring, 1786): Let $f(x) = x^5 + a_1 x^4 + \ldots + a_5$ be a polynomial of degree 5 over a solvably closed field K. Then every root of $f(x)$ lies in the extension L/K obtained by adjoining a root of a polynomial of the form $x^5 + tx + t$, for some $t \in K$.

In other words, we can obtain every root of $f(x)$ from $a_1, \ldots, a_5$ and elements of the base field k, if we are allowed to apply the four arithmetic operations, extract roots and adjoin roots of polynomials of the form $x^5 + tx + t$. The last operation is akin to extracting the 5th root of t. In both cases only one parameter is involved (namely t).

Polynomials of degree 5

Theorem (Bring, 1786): Let $f(x) = x^5 + a_1x^4 + \ldots + a_5$ be a polynomial of degree 5 over a solvably closed field K. Then every root of $f(x)$ lies in the extension L/K obtained by adjoining a root of a polynomial of the form $x^5 + tx + t$, for some $t \in K$.

In other words, we can obtain every root of $f(x)$ from $a_1, \ldots, a_5$ and elements of the base field k, if we are allowed to apply the four arithmetic operations, extract roots and adjoin roots of polynomials of the form $x^5 + tx + t$. The last operation is akin to extracting the 5th root of t. In both cases only one parameter is involved (namely t). In classical language, every root of $x^5 + t + t$ is an algebraic (multi-valued) functions of one variable, and so is every root of $x^5 - t$.

Polynomials of degree 5

Theorem (Bring, 1786): Let $f(x) = x^5 + a_1x^4 + \ldots + a_5$ be a polynomial of degree 5 over a solvably closed field K. Then every root of $f(x)$ lies in the extension L/K obtained by adjoining a root of a polynomial of the form $x^5 + tx + t$, for some $t \in K$.

In other words, we can obtain every root of $f(x)$ from $a_1, \ldots, a_5$ and elements of the base field k, if we are allowed to apply the four arithmetic operations, extract roots and adjoin roots of polynomials of the form $x^5 + tx + t$. The last operation is akin to extracting the 5th root of t. In both cases only one parameter is involved (namely t). In classical language, every root of $x^5 + t + t$ is an algebraic (multi-valued) functions of one variable, and so is every root of $x^5 - t$.

Informally speaking, a field extension L/K is of level $\leqslant 1$ if it can be obtained by adjoining algebraic functions of $\leqslant 1$ variables.

Polynomials of degree 5

Theorem (Bring, 1786): Let $f(x) = x^5 + a_1x^4 + \ldots + a_5$ be a polynomial of degree 5 over a solvably closed field K. Then every root of $f(x)$ lies in the extension L/K obtained by adjoining a root of a polynomial of the form $x^5 + tx + t$, for some $t \in K$.

In other words, we can obtain every root of $f(x)$ from $a_1, \ldots, a_5$ and elements of the base field k, if we are allowed to apply the four arithmetic operations, extract roots and adjoin roots of polynomials of the form $x^5 + tx + t$. The last operation is akin to extracting the 5th root of t. In both cases only one parameter is involved (namely t). In classical language, every root of $x^5 + t + t$ is an algebraic (multi-valued) functions of one variable, and so is every root of $x^5 - t$.

Informally speaking, a field extension L/K is of level $\leqslant 1$ if it can be obtained by adjoining algebraic functions of $\leqslant 1$ variables. In particular, every field extension L/K of degree $\leqslant 5$ is of level $\leqslant 1$.

Essential dimension of a field extension

Let us now define the notion of an algebraic function in $\leqslant d$ variables more formally.

Essential dimension of a field extension

Let us now define the notion of an algebraic function in $\leqslant d$ variables more formally.

Let K be a field containing a base field k, and L/K be a finite extension. We say that the essential dimension $\mathrm{ed}_k(L/K)$ is $\leqslant d$, if there exists an intermediate field $k \subset K_0 \subset K$ and a field extension L_0/K_0 such that $L = L_0 \otimes_{K_0} K$ and $\mathrm{trdeg}_k(K_0) \leqslant d$.

Essential dimension of a field extension

Let us now define the notion of an algebraic function in $\leqslant d$ variables more formally.

Let K be a field containing a base field k, and L/K be a finite extension. We say that the essential dimension $\mathrm{ed}_k(L/K)$ is $\leqslant d$, if there exists an intermediate field $k \subset K_0 \subset K$ and a field extension L_0/K_0 such that $L = L_0 \otimes_{K_0} K$ and $\mathrm{trdeg}_k(K_0) \leqslant d$.

The exact value of $\mathrm{ed}_k(L/K)$ is then the smallest integer d such that $\mathrm{ed}_k(L/K) \leqslant d$.

Essential dimension of a field extension

Let us now define the notion of an algebraic function in $\leqslant d$ variables more formally.

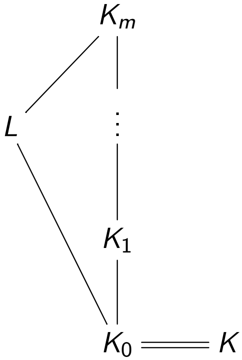
Let K be a field containing a base field k, and L/K be a finite extension. We say that the essential dimension $\mathrm{ed}_k(L/K)$ is $\leqslant d$, if there exists an intermediate field $k \subset K_0 \subset K$ and a field extension L_0/K_0 such that $L = L_0 \otimes_{K_0} K$ and $\mathrm{trdeg}_k(K_0) \leqslant d$.

The exact value of $\mathrm{ed}_k(L/K)$ is then the smallest integer d such that $\mathrm{ed}_k(L/K) \leqslant d$.

If L/K is separable, then the inequality $\mathrm{ed}_k(L/K) \leqslant d$ is equivalent to saying that L is generated over K by a single algebraic function in $\leqslant d$ variables.

The level of a finite field extension

We will say that the level $\mathrm{lev}_k(L/K)$ of L/K is $\leqslant d$ if there exists a tower



such that $[K_i : K_{i-1}] < \infty$ and $\mathrm{ed}_k(K_i/K_{i-1}) \leqslant d$ for every $i = 1, \ldots, m$.
The level of L/K is the smallest such d; I will denote it by $\mathrm{lev}_k(L/K)$.

Warning!

It is not known whether or not there exists a finite field extension L/K such that $k \subset K$ and $\text{lev}_k(L/K) > 1$, for any base field k.

The resolvent degree

Let G be an algebraic group over a field k, K/k a field extension and $T \to \mathrm{Spec}(K)$ a G-torsor.

The resolvent degree

Let G be an algebraic group over a field k, K/k a field extension and $T \to \mathrm{Spec}(K)$ a G-torsor.

The resolvent degree $\mathrm{rd}_k(T)$ is the minimal level $\mathrm{lev}_k(T)$ of a finite extension L/K which splits $T \to Spec(K)$.

The resolvent degree

Let G be an algebraic group over a field k, K/k a field extension and $T \to \mathrm{Spec}(K)$ a G-torsor.

The resolvent degree $\mathrm{rd}_k(T)$ is the minimal level $\mathrm{lev}_k(T)$ of a finite extension L/K which splits $T \to Spec(K)$.

The resolvent degree $\mathrm{rd}_k(G)$ of G is the maximal value of $\mathrm{rd}_k(T)$ as K ranges over field extensions K/k and T ranges over G-torsors $T \to \mathrm{Spec}(K)$.

Hilbert's 13th Problem

If G is a finite group, then $\mathrm{rd}_k(G)$ is the maximal value of $\mathrm{lev}_k(L/K)$, where L/K is a separable extension with Galois group G. In this case $\mathrm{rd}_k(G)$ was defined by Farb and Wolfson, who refer to $\mathrm{lev}_k(L/K)$ as the "resolvent degree of L/K".

Hilbert's 13th Problem

If G is a finite group, then $\mathrm{rd}_k(G)$ is the maximal value of $\mathrm{lev}_k(L/K)$, where L/K is a separable extension with Galois group G. In this case $\mathrm{rd}_k(G)$ was defined by Farb and Wolfson, who refer to $\mathrm{lev}_k(L/K)$ as the "resolvent degree of L/K". (The term "level" is taken from an earlier paper of Dixmier.)

Hilbert's 13th Problem

If G is a finite group, then $\mathrm{rd}_k(G)$ is the maximal value of $\mathrm{lev}_k(L/K)$, where L/K is a separable extension with Galois group G. In this case $\mathrm{rd}_k(G)$ was defined by Farb and Wolfson, who refer to $\mathrm{lev}_k(L/K)$ as the "resolvent degree of L/K". (The term "level" is taken from an earlier paper of Dixmier.)

Hilbert's 13th Problem (the algebraic version): Find $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n)$ for every positive integer n.

Hilbert's 13th Problem

If G is a finite group, then $\mathrm{rd}_k(G)$ is the maximal value of $\mathrm{lev}_k(L/K)$, where L/K is a separable extension with Galois group G. In this case $\mathrm{rd}_k(G)$ was defined by Farb and Wolfson, who refer to $\mathrm{lev}_k(L/K)$ as the "resolvent degree of L/K". (The term "level" is taken from an earlier paper of Dixmier.)

Hilbert's 13th Problem (the algebraic version): Find $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n)$ for every positive integer n.

It is known that $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) = 1$ for $n \leqslant 5$.

Hilbert's 13th Problem

If G is a finite group, then $\mathrm{rd}_k(G)$ is the maximal value of $\mathrm{lev}_k(L/K)$, where L/K is a separable extension with Galois group G. In this case $\mathrm{rd}_k(G)$ was defined by Farb and Wolfson, who refer to $\mathrm{lev}_k(L/K)$ as the "resolvent degree of L/K". (The term "level" is taken from an earlier paper of Dixmier.)

Hilbert's 13th Problem (the algebraic version): Find $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n)$ for every positive integer n.

It is known that $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) = 1$ for $n \leqslant 5$. It is not known whether $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) \longrightarrow \infty$ as $n \to \infty$

Hilbert's 13th Problem

If G is a finite group, then $\mathrm{rd}_k(G)$ is the maximal value of $\mathrm{lev}_k(L/K)$, where L/K is a separable extension with Galois group G. In this case $\mathrm{rd}_k(G)$ was defined by Farb and Wolfson, who refer to $\mathrm{lev}_k(L/K)$ as the "resolvent degree of L/K". (The term "level" is taken from an earlier paper of Dixmier.)

Hilbert's 13th Problem (the algebraic version): Find $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n)$ for every positive integer n.

It is known that $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) = 1$ for $n \leqslant 5$. It is not known whether $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) \longrightarrow \infty$ as $n \to \infty$ or even if $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) > 1$ for any n.

Hilbert's 13th Problem

If G is a finite group, then $\mathrm{rd}_k(G)$ is the maximal value of $\mathrm{lev}_k(L/K)$, where L/K is a separable extension with Galois group G. In this case $\mathrm{rd}_k(G)$ was defined by Farb and Wolfson, who refer to $\mathrm{lev}_k(L/K)$ as the "resolvent degree of L/K". (The term "level" is taken from an earlier paper of Dixmier.)

Hilbert's 13th Problem (the algebraic version): Find $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n)$ for every positive integer n.

It is known that $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) = 1$ for $n \leqslant 5$. It is not known whether $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) \longrightarrow \infty$ as $n \to \infty$ or even if $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) > 1$ for any n.

All known upper bounds are of the form $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n) \leqslant n - \epsilon(n)$, where $\epsilon(n)$ is an unbounded but very slowly increasing function of n. The latest/strongest are due to Wolfson (2020), Sutherland and Heberle-Sutherland.

New results: dependence on the base field

Theorem 1: Let G be an algebraic group over k, not necessarily smooth or linear or connected.

New results: dependence on the base field

Theorem 1: Let G be an algebraic group over k, not necessarily smooth or linear or connected. Then $\mathrm{rd}_k(G) = \mathrm{rd}_{k'}(G_{k'})$ for any field k' containing k.

New results: dependence on the base field

Theorem 1: Let G be an algebraic group over k, not necessarily smooth or linear or connected. Then $\mathrm{rd}_k(G) = \mathrm{rd}_{k'}(G_{k'})$ for any field k' containing k.

Note that the case, where k' is algebraic over k is easy and was known to the classics (e.g., Felix Klein).

New results: dependence on the base field

Theorem 1: Let G be an algebraic group over k, not necessarily smooth or linear or connected. Then $\mathrm{rd}_k(G) = \mathrm{rd}_{k'}(G_{k'})$ for any field k' containing k.

Note that the case, where k' is algebraic over k is easy and was known to the classics (e.g., Felix Klein). What is new here is that k' can be arbitrary. For example, $\mathrm{rd}_{\mathbb{Q}}(\mathsf{S}_n) = \mathrm{rd}_{\mathbb{C}}(\mathsf{S}_n)$.

New results: dependence on the base field

Theorem 1: Let G be an algebraic group over k, not necessarily smooth or linear or connected. Then $\mathrm{rd}_k(G) = \mathrm{rd}_{k'}(G_{k'})$ for any field k' containing k.

Note that the case, where k' is algebraic over k is easy and was known to the classics (e.g., Felix Klein). What is new here is that k' can be arbitrary. For example, $\mathrm{rd}_{\mathbb{Q}}(\mathrm{S}_n) = \mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n)$.

Theorem 2: Let G be a smooth affine group scheme over $\mathbb{Z}$. Assume that the connected component G^0 is split reductive and the component group G/G^0 is finite over $\mathbb{Z}$.

New results: dependence on the base field

Theorem 1: Let G be an algebraic group over k, not necessarily smooth or linear or connected. Then $\mathrm{rd}_k(G) = \mathrm{rd}_{k'}(G_{k'})$ for any field k' containing k.

Note that the case, where k' is algebraic over k is easy and was known to the classics (e.g., Felix Klein). What is new here is that k' can be arbitrary. For example, $\mathrm{rd}_{\mathbb{Q}}(\mathrm{S}_n) = \mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n)$.

Theorem 2: Let G be a smooth affine group scheme over $\mathbb{Z}$. Assume that the connected component G^0 is split reductive and the component group G/G^0 is finite over $\mathbb{Z}$. Let k be a field of characteristic 0. Then $\mathrm{rd}_k(G_k) \geqslant rd_{k'}(G_{k'})$ for any other field k'.

New results: dependence on the base field

Theorem 1: Let G be an algebraic group over k, not necessarily smooth or linear or connected. Then $\mathrm{rd}_k(G) = \mathrm{rd}_{k'}(G_{k'})$ for any field k' containing k.

Note that the case, where k' is algebraic over k is easy and was known to the classics (e.g., Felix Klein). What is new here is that k' can be arbitrary. For example, $\mathrm{rd}_{\mathbb{Q}}(\mathrm{S}_n) = \mathrm{rd}_{\mathbb{C}}(\mathrm{S}_n)$.

Theorem 2: Let G be a smooth affine group scheme over $\mathbb{Z}$. Assume that the connected component G^0 is split reductive and the component group G/G^0 is finite over $\mathbb{Z}$. Let k be a field of characteristic 0. Then $\mathrm{rd}_k(G_k) \geqslant rd_{k'}(G_{k'})$ for any other field k'.

Theorem 2 is primarily of interest in mixed characteristic, where $\mathrm{char}(k) = 0$ but $\mathrm{char}(k') > 0$.

New results: dependence on the base field

Theorem 1: Let G be an algebraic group over k, not necessarily smooth or linear or connected. Then $\mathrm{rd}_k(G) = \mathrm{rd}_{k'}(G_{k'})$ for any field k' containing k.

Note that the case, where k' is algebraic over k is easy and was known to the classics (e.g., Felix Klein). What is new here is that k' can be arbitrary. For example, $\mathrm{rd}_{\mathbb{Q}}(\mathsf{S}_n) = \mathrm{rd}_{\mathbb{C}}(\mathsf{S}_n)$.

Theorem 2: Let G be a smooth affine group scheme over $\mathbb{Z}$. Assume that the connected component G^0 is split reductive and the component group G/G^0 is finite over $\mathbb{Z}$. Let k be a field of characteristic 0. Then $\mathrm{rd}_k(G_k) \geqslant rd_{k'}(G_{k'})$ for any other field k'.

Theorem 2 is primarily of interest in mixed characteristic, where $\mathrm{char}(k) = 0$ but $\mathrm{char}(k') > 0$. If $\mathrm{char}(k') = \mathrm{char}(k')$, then $\mathrm{rd}_k(G_k) = \mathrm{rd}_F(G_F) = rd_{k'}(G_{k'})$ by Theorem 1, where F is a prime field.

New results: the resolvent degree of a connected group

Theorem 3: Let G be a connected algebraic group over a field k,

New results: the resolvent degree of a connected group

Theorem 3: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 5$.

The proof proceeds in several steps.

New results: the resolvent degree of a connected group

Theorem 3: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 5$.

The proof proceeds in several steps.

1. Use Theorem 1 to reduce to the case, where k is algebraically closed.

New results: the resolvent degree of a connected group

Theorem 3: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 5$.

The proof proceeds in several steps.

1. Use Theorem 1 to reduce to the case, where k is algebraically closed.
2. Reduce to the case, where G is smooth. $1 \to G_{\mathrm{red}} \to G$.

New results: the resolvent degree of a connected group

Theorem 3: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 5$.

The proof proceeds in several steps.

1. Use Theorem 1 to reduce to the case, where k is algebraically closed.
2. Reduce to the case, where G is smooth. $1 \to G_{\mathrm{red}} \to G$.
2. Show that $\mathrm{rd}_k(A) \leqslant 1$ for any abelian variety A. $1 \to A[d] \to A$.

New results: the resolvent degree of a connected group

Theorem 3: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 5$.

The proof proceeds in several steps.

1. Use Theorem 1 to reduce to the case, where k is algebraically closed.

2. Reduce to the case, where G is smooth. $1 \to G_{\mathrm{red}} \to G$.

2. Show that $\mathrm{rd}_k(A) \leqslant 1$ for any abelian variety A. $1 \to A[d] \to A$.

3. Use Chevalley's Structure Theorem to reduce to the case, where G is affine. $1 \to G_{\mathrm{aff}} \to G \to A \to 1$.

New results: the resolvent degree of a connected group

Theorem 3: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 5$.

The proof proceeds in several steps.

1. Use Theorem 1 to reduce to the case, where k is algebraically closed.

2. Reduce to the case, where G is smooth. $1 \to G_{\mathrm{red}} \to G$.

2. Show that $\mathrm{rd}_k(A) \leqslant 1$ for any abelian variety A. $1 \to A[d] \to A$.

3. Use Chevalley's Structure Theorem to reduce to the case, where G is affine. $1 \to G_{\mathrm{aff}} \to G \to A \to 1$.

4. Reduce to the case, where G is semisimple.
$1 \to Rad(G) \to G \to G/Rad(G) \to 1$.

New results: the resolvent degree of a connected group

Theorem 3: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 5$.

The proof proceeds in several steps.

1. Use Theorem 1 to reduce to the case, where k is algebraically closed.

2. Reduce to the case, where G is smooth. $1 \to G_{\mathrm{red}} \to G$.

2. Show that $\mathrm{rd}_k(A) \leqslant 1$ for any abelian variety A. $1 \to A[d] \to A$.

3. Use Chevalley's Structure Theorem to reduce to the case, where G is affine. $1 \to G_{\mathrm{aff}} \to G \to A \to 1$.

4. Reduce to the case, where G is semisimple.
$1 \to Rad(G) \to G \to G/Rad(G) \to 1$.

5. Reduce to the case, where G is simple. $1 \to \mu \to \prod G_i \to G \to 1$, G_i minimal connected normal subgroups.

New results: the resolvent degree of a connected group

Theorem 3: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 5$.

The proof proceeds in several steps.

1. Use Theorem 1 to reduce to the case, where k is algebraically closed.

2. Reduce to the case, where G is smooth. $1 \to G_{\mathrm{red}} \to G$.

2. Show that $\mathrm{rd}_k(A) \leqslant 1$ for any abelian variety A. $1 \to A[d] \to A$.

3. Use Chevalley's Structure Theorem to reduce to the case, where G is affine. $1 \to G_{\mathrm{aff}} \to G \to A \to 1$.

4. Reduce to the case, where G is semisimple.
$1 \to Rad(G) \to G \to G/Rad(G) \to 1$.

5. Reduce to the case, where G is simple. $1 \to \mu \to \prod G_i \to G \to 1$, G_i minimal connected normal subgroups.

6. Show that $\mathrm{rd}_k(E_8) \leqslant 5$.

A conjectural strengthening of Theorem 3

Conjecture 4: Let G be a connected algebraic group over a field k,

A conjectural strengthening of Theorem 3

Conjecture 4: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 1$.

A conjectural strengthening of Theorem 3

Conjecture 4: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 1$.

Remarks: (a) It suffices to prove this conjecture in the special case where $k = \mathbb{C}$ and G is a simple group of type E_8.

A conjectural strengthening of Theorem 3

Conjecture 4: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 1$.

Remarks: (a) It suffices to prove this conjecture in the special case where $k = \mathbb{C}$ and G is a simple group of type E_8. The proof of Theorem 4 covers the rest.

A conjectural strengthening of Theorem 3

Conjecture 4: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 1$.

Remarks: (a) It suffices to prove this conjecture in the special case where $k = \mathbb{C}$ and G is a simple group of type E_8. The proof of Theorem 4 covers the rest.

(b) Theorem 3 and Conjecture 4 are in the same spirit (but weaker) than the questions of Tits we considered earlier. Recall

A conjectural strengthening of Theorem 3

Conjecture 4: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 1$.

Remarks: (a) It suffices to prove this conjecture in the special case where $k = \mathbb{C}$ and G is a simple group of type E_8. The proof of Theorem 4 covers the rest.

(b) Theorem 3 and Conjecture 4 are in the same spirit (but weaker) than the questions of Tits we considered earlier. Recall

Question (Tits): Is it true that every E_8-torsor $T \to \mathrm{Spec}(K)$ is split by a Galois field extension L/K with solvable (or almost solvable) Galois group $\mathrm{Gal}(L/K)$?

A conjectural strengthening of Theorem 3

Conjecture 4: Let G be a connected algebraic group over a field k, not necessarily smooth or linear. Then $\mathrm{rd}_k(G) \leqslant 1$.

Remarks: (a) It suffices to prove this conjecture in the special case where $k = \mathbb{C}$ and G is a simple group of type E_8. The proof of Theorem 4 covers the rest.

(b) Theorem 3 and Conjecture 4 are in the same spirit (but weaker) than the questions of Tits we considered earlier. Recall

Question (Tits): Is it true that every E_8-torsor $T \to \mathrm{Spec}(K)$ is split by a Galois field extension L/K with solvable (or almost solvable) Galois group $\mathrm{Gal}(L/K)$?

Positive answer to Tits' question $\Longrightarrow$ Conjecture 4 $\Longrightarrow$ Theorem 3.

Some evidence for Conjecture 4

Conjecture (Serre, 1995): Let K be a field, G be a smooth algebraic group over K, and $T \to \mathrm{Spec}(K)$ be a G-torsor.

Some evidence for Conjecture 4

Conjecture (Serre, 1995): Let K be a field, G be a smooth algebraic group over K, and $T \to \mathrm{Spec}(K)$ be a G-torsor. If K_i/K are finite extensions of K of relatively prime degrees, i.e., $\gcd([K_i : K]) = 1$, and each K_i splits T, then T is split over K.

Some evidence for Conjecture 4

Conjecture (Serre, 1995): Let K be a field, G be a smooth algebraic group over K, and $T \to \mathrm{Spec}(K)$ be a G-torsor. If K_i/K are finite extensions of K of relatively prime degrees, i.e., $\gcd([K_i : K]) = 1$, and each K_i splits T, then T is split over K.

Proposition: Let G be the simple algebraic group of type E_8 over $\mathbb{C}$. If Serre's conjecture holds for G_K, for every field K containing $\mathbb{C}$, then Conjecture 4 holds.

Some evidence for Conjecture 4

Conjecture (Serre, 1995): Let K be a field, G be a smooth algebraic group over K, and $T \to \mathrm{Spec}(K)$ be a G-torsor. If K_i/K are finite extensions of K of relatively prime degrees, i.e., $\gcd([K_i : K]) = 1$, and each K_i splits T, then T is split over K.

Proposition: Let G be the simple algebraic group of type E_8 over $\mathbb{C}$. If Serre's conjecture holds for G_K, for every field K containing $\mathbb{C}$, then Conjecture 4 holds.

Proof: Using Theorem 1, 2 and the proof of Theorem 3, we reduce to the case, where G is a simple group of type E_8 over $k = \mathbb{C}$. It now suffices to show that every G-torsor $T \to \mathrm{Spec}(K)$ over a solvably closed field K containing $\mathbb{C}$ is split.

Some evidence for Conjecture 4

Conjecture (Serre, 1995): Let K be a field, G be a smooth algebraic group over K, and $T \to \mathrm{Spec}(K)$ be a G-torsor. If K_i/K are finite extensions of K of relatively prime degrees, i.e., $\gcd([K_i : K]) = 1$, and each K_i splits T, then T is split over K.

Proposition: Let G be the simple algebraic group of type E_8 over $\mathbb{C}$. If Serre's conjecture holds for G_K, for every field K containing $\mathbb{C}$, then Conjecture 4 holds.

Proof: Using Theorem 1, 2 and the proof of Theorem 3, we reduce to the case, where G is a simple group of type E_8 over $k = \mathbb{C}$. It now suffices to show that every G-torsor $T \to \mathrm{Spec}(K)$ over a solvably closed field K containing $\mathbb{C}$ is split. To prove this, we will construct finite splitting field extensions K_2, K_3, K_5 and $K_{\geqslant 7}$ of K such that

Some evidence for Conjecture 4

Conjecture (Serre, 1995): Let K be a field, G be a smooth algebraic group over K, and $T \to \operatorname{Spec}(K)$ be a G-torsor. If K_i/K are finite extensions of K of relatively prime degrees, i.e., $\gcd([K_i : K]) = 1$, and each K_i splits T, then T is split over K.

Proposition: Let G be the simple algebraic group of type E_8 over $\mathbb{C}$. If Serre's conjecture holds for G_K, for every field K containing $\mathbb{C}$, then Conjecture 4 holds.

Proof: Using Theorem 1, 2 and the proof of Theorem 3, we reduce to the case, where G is a simple group of type E_8 over $k = \mathbb{C}$. It now suffices to show that every G-torsor $T \to \operatorname{Spec}(K)$ over a solvably closed field K containing $\mathbb{C}$ is split. To prove this, we will construct finite splitting field extensions K_2, K_3, K_5 and $K_{\geqslant 7}$ of K such that

- $[K_p : K]$ is prime to p for $p = 2, 3, 5$,

Some evidence for Conjecture 4

Conjecture (Serre, 1995): Let K be a field, G be a smooth algebraic group over K, and $T \to \mathrm{Spec}(K)$ be a G-torsor. If K_i/K are finite extensions of K of relatively prime degrees, i.e., $\gcd([K_i : K]) = 1$, and each K_i splits T, then T is split over K.

Proposition: Let G be the simple algebraic group of type E_8 over $\mathbb{C}$. If Serre's conjecture holds for G_K, for every field K containing $\mathbb{C}$, then Conjecture 4 holds.

Proof: Using Theorem 1, 2 and the proof of Theorem 3, we reduce to the case, where G is a simple group of type E_8 over $k = \mathbb{C}$. It now suffices to show that every G-torsor $T \to \mathrm{Spec}(K)$ over a solvably closed field K containing $\mathbb{C}$ is split. To prove this, we will construct finite splitting field extensions K_2, K_3, K_5 and $K_{\geqslant 7}$ of K such that

- $[K_p : K]$ is prime to p for $p = 2, 3, 5$,
- $[K_{\geqslant 7} : K]$ is not divisible for any prime $\geqslant 7$.

Construction of K_2, K_3, K_5 and $K_{\geqslant 7}$

$K_{\geqslant 7}$: Since the only exceptional primes of E_8 are 2, 3 and 5, every E_8-torsor over K can be split by a field extension $K_{\geqslant 7}/K$ of degree $2^a 3^b 5^c$.

Construction of K_2, K_3, K_5 and $K_{\geqslant 7}$

$K_{\geqslant 7}$: Since the only exceptional primes of E_8 are 2, 3 and 5, every E_8-torsor over K can be split by a field extension $K_{\geqslant 7}/K$ of degree $2^a 3^b 5^c$. This is a general fact, due to Tits; it does not use the assumption that K is solvably closed.

Construction of K_2, K_3, K_5 and $K_{\geqslant 7}$

$K_{\geqslant 7}$**:** Since the only exceptional primes of E_8 are 2, 3 and 5, every E_8-torsor over K can be split by a field extension $K_{\geqslant 7}/K$ of degree $2^a 3^b 5^c$. This is a general fact, due to Tits; it does not use the assumption that K is solvably closed.

K_3**:** Consider the mod 3 Rost Invariant $R_3 \colon H^1(*, E_8) \to H^3(*, \mu_3)$. By Bloch-Kato, $H^3(*, \mu_3) = 0$, since K is solvably closed. In other words, T lies in the kernel of R_3. By a theorem of Chernousov, $T \to \mathrm{Spec}(K)$ is split by some field extension K_3/K of degree prime to 3.

Construction of K_2, K_3, K_5 and $K_{\geqslant 7}$

$K_{\geqslant 7}$: Since the only exceptional primes of E_8 are 2, 3 and 5, every E_8-torsor over K can be split by a field extension $K_{\geqslant 7}/K$ of degree $2^a 3^b 5^c$. This is a general fact, due to Tits; it does not use the assumption that K is solvably closed.

K_3: Consider the mod 3 Rost Invariant $R_3 \colon H^1(*, E_8) \to H^3(*, \mu_3)$. By Bloch-Kato, $H^3(*, \mu_3) = 0$, since K is solvably closed. In other words, T lies in the kernel of R_3. By a theorem of Chernousov, $T \to \mathrm{Spec}(K)$ is split by some field extension K_3/K of degree prime to 3.

K_5 is constructed in the same way as K_3.

Construction of K_2, K_3, K_5 and $K_{\geqslant 7}$

$K_{\geqslant 7}$**:** Since the only exceptional primes of E_8 are 2, 3 and 5, every E_8-torsor over K can be split by a field extension $K_{\geqslant 7}/K$ of degree $2^a 3^b 5^c$. This is a general fact, due to Tits; it does not use the assumption that K is solvably closed.

K_3**:** Consider the mod 3 Rost Invariant $R_3 \colon H^1(*, E_8) \to H^3(*, \mu_3)$. By Bloch-Kato, $H^3(*, \mu_3) = 0$, since K is solvably closed. In other words, T lies in the kernel of R_3. By a theorem of Chernousov, $T \to \mathrm{Spec}(K)$ is split by some field extension K_3/K of degree prime to 3.

K_5 is constructed in the same way as K_3.

K_2**:** Using Bloch-Kato again, we see that T lies in the kernel of the mod 4 Rost invariant $R_4 \colon H^1(*, E_8) \to H^3(*, \mu_4)$

Construction of K_2, K_3, K_5 and $K_{\geqslant 7}$

$K_{\geqslant 7}$**:** Since the only exceptional primes of E_8 are 2, 3 and 5, every E_8-torsor over K can be split by a field extension $K_{\geqslant 7}/K$ of degree $2^a 3^b 5^c$. This is a general fact, due to Tits; it does not use the assumption that K is solvably closed.

K_3**:** Consider the mod 3 Rost Invariant $R_3 \colon H^1(*, E_8) \to H^3(*, \mu_3)$. By Bloch-Kato, $H^3(*, \mu_3) = 0$, since K is solvably closed. In other words, T lies in the kernel of R_3. By a theorem of Chernousov, $T \to \mathrm{Spec}(K)$ is split by some field extension K_3/K of degree prime to 3.

K_5 is constructed in the same way as K_3.

K_2**:** Using Bloch-Kato again, we see that T lies in the kernel of the mod 4 Rost invariant $R_4 \colon H^1(*, E_8) \to H^3(*, \mu_4)$ and in the kernel of the Semenov invariant $\mathrm{Ker(R_4)} \to H^5(K, \mu_2)$.

Construction of K_2, K_3, K_5 and $K_{\geqslant 7}$

$K_{\geqslant 7}$**:** Since the only exceptional primes of E_8 are 2, 3 and 5, every E_8-torsor over K can be split by a field extension $K_{\geqslant 7}/K$ of degree $2^a 3^b 5^c$. This is a general fact, due to Tits; it does not use the assumption that K is solvably closed.

K_3**:** Consider the mod 3 Rost Invariant $R_3 \colon H^1(*, E_8) \to H^3(*, \mu_3)$. By Bloch-Kato, $H^3(*, \mu_3) = 0$, since K is solvably closed. In other words, T lies in the kernel of R_3. By a theorem of Chernousov, $T \to \mathrm{Spec}(K)$ is split by some field extension K_3/K of degree prime to 3.

K_5 is constructed in the same way as K_3.

K_2**:** Using Bloch-Kato again, we see that T lies in the kernel of the mod 4 Rost invariant $R_4 \colon H^1(*, E_8) \to H^3(*, \mu_4)$ and in the kernel of the Semenov invariant $\mathrm{Ker(R_4)} \to H^5(K, \mu_2)$. Thus by a theorem of Semenov, T is split by an odd degree extension K_2/K. □

Construction of K_2 in prime characteristic

Note that Semenov's Theorem is only valid in characteristic 0.

Construction of K_2 in prime characteristic

Note that Semenov's Theorem is only valid in characteristic 0.

In prime characteristic, we use Theorem 2 to reduce to characteristic 0.

Construction of K_2 in prime characteristic

Note that Semenov's Theorem is only valid in characteristic 0.

In prime characteristic, we use Theorem 2 to reduce to characteristic 0.

In characteristic 0 the above argument shows that Serre's conjecture $\Longrightarrow$ positive answer to Tits' Question 1: every E_8-torsor $T \to \mathrm{Spec}(K)$ is split by some solvable extension L/K.