Algebraic Groups with Good Reduction

(joint work with V. Chernousov and I. Rapinchuk)

Andrei S. Rapinchuk

University of Virginia

GMU September 6, 2019

- Can be used to show that equations have **no** *integer* or *rational* solutions.

- Can be used to show that equations have **no** *integer* or *rational* solutions.

Consider equation

$$x^2 - 7y^2 = -1.$$

- Can be used to show that equations have **no** *integer* or *rational* solutions.

Consider equation

$$x^2 - 7y^2 = -1.$$

Let (x_0, y_0) be an integer solution.

- Can be used to show that equations have **no** *integer* or *rational* solutions.

Consider equation

$$x^2 - 7y^2 = -1.$$

Let (x_0, y_0) be an integer solution. Taking mod 7 yields

$$x_0^2 \equiv -1 (\mathrm{mod}\, 7).$$

- Can be used to show that equations have **no** *integer* or *rational* solutions.

Consider equation

$$x^2 - 7y^2 = -1.$$

Let (x_0, y_0) be an integer solution. Taking mod 7 yields

$$x_0^2 \equiv -1 (\mathrm{mod}\, 7).$$

But this congruence has **no** solutions!

- Can be used to show that equations have **no** *integer* or *rational* solutions.

Consider equation

$$x^2 - 7y^2 = -1.$$

Let (x_0, y_0) be an integer solution. Taking mod 7 yields

$$x_0^2 \equiv -1 (\mathrm{mod}\, 7).$$

But this congruence has **no** solutions! (Otherwise $(\mathbb{Z}/7\mathbb{Z})^\times$, which has order 6, would contain an element of order 4.)

- Can be used to show that equations have **no** *integer* or *rational* solutions.

Consider equation

$$x^2 - 7y^2 = -1.$$

Let (x_0, y_0) be an integer solution. Taking mod 7 yields

$$x_0^2 \equiv -1 (\mathrm{mod}\, 7).$$

But this congruence has **no** solutions! (Otherwise $(\mathbb{Z}/7\mathbb{Z})^\times$, which has order 6, would contain an element of order 4.)

Thus, original equation has no integer solutions.

- Can aid in understanding *structure of solution set*, i.e. set of *rational points*.

- Can aid in understanding *structure of solution set*, i.e. set of *rational points*.

Recall:

- An elliptic curve E is a smooth cubic in $\mathbb{P}^2$ (with a rational point)
- Over a field K of characteristic $\neq 2, 3$, "affine" part of E can be given by equation

$$y^2 = f(x)$$

where $f(x) = x^3 + ax + b$ $(a, b \in K)$ has **no** multiple roots;

- E has one point "at infinity;"
- K-rational points $E(K)$ form abelian group for tangent-chord group law;

- Can aid in understanding *structure of solution set*, i.e. set of *rational points*.

Recall:

- An elliptic curve E is a smooth cubic in $\mathbb{P}^2$ (with a rational point)
- Over a field K of characteristic $\neq 2, 3$, "affine" part of E can be given by equation

$$y^2 = f(x)$$

where $f(x) = x^3 + ax + b$ $(a, b \in K)$ has **no** multiple roots;

- E has one point "at infinity;"
- K-rational points $E(K)$ form abelian group for tangent-chord group law;

- Can aid in understanding *structure of solution set*, i.e. set of *rational points*.

Recall:

- An elliptic curve E is a smooth cubic in $\mathbb{P}^2$ (with a rational point)
- Over a field K of characteristic $\neq 2, 3$, "affine" part of E can be given by equation

$$y^2 = f(x)$$

where $f(x) = x^3 + ax + b$ $(a, b \in K)$ has **no** multiple roots;

- E has one point "at infinity;"
- K-rational points $E(K)$ form abelian group for tangent-chord group law;

- Can aid in understanding *structure of solution set*, i.e. set of *rational points*.

Recall:

- An elliptic curve E is a smooth cubic in $\mathbb{P}^2$ (with a rational point)
- Over a field K of characteristic $\neq 2, 3$, "affine" part of E can be given by equation

$$y^2 = f(x)$$

where $f(x) = x^3 + ax + b$ $(a, b \in K)$ has **no** multiple roots;

- E has one point "at infinity;"
- K-rational points $E(K)$ form abelian group for tangent-chord group law;

- Can aid in understanding *structure of solution set*, i.e. set of *rational points*.

Recall:

- An elliptic curve E is a smooth cubic in $\mathbb{P}^2$ (with a rational point)
- Over a field K of characteristic $\neq 2, 3$, "affine" part of E can be given by equation

$$y^2 = f(x)$$

where $f(x) = x^3 + ax + b$ $(a, b \in K)$ has **no** multiple roots;

- E has one point "at infinity;"
- K-rational points $E(K)$ form abelian group for tangent-chord group law;

- Can aid in understanding *structure of solution set*, i.e. set of *rational points*.

Recall:

- An elliptic curve E is a smooth cubic in $\mathbb{P}^2$ (with a rational point)
- Over a field K of characteristic $\neq 2, 3$, "affine" part of E can be given by equation

$$y^2 = f(x)$$

where $f(x) = x^3 + ax + b$ $(a, b \in K)$ has **no** multiple roots;

- E has one point "at infinity;"
- K-rational points $E(K)$ form abelian group for tangent-chord group law; identity element = point at infinity.

Theorem (Mordell – Weil)

Let E be an elliptic curve over a number field K.

Theorem (Mordell – Weil)

Let E be an elliptic curve over a number field K.
Then the group $E(K)$ is finitely generated.

Theorem (Mordell – Weil)

Let E be an elliptic curve over a number field K.
Then the group $E(K)$ is finitely generated.

Remark. Conclusion remains valid for abelian varieties over finitely generated fields.

Theorem (Mordell – Weil)

Let E be an elliptic curve over a number field K.
Then the group $E(K)$ is finitely generated.

Remark. Conclusion remains valid for abelian varieties over finitely generated fields.

PROOF for elliptic curves E over $K = \mathbb{Q}$ was found by Louis Mordell in 1922.

Theorem (Mordell – Weil)

Let E be an elliptic curve over a number field K.
Then the group $E(K)$ is finitely generated.

Remark. Conclusion remains valid for abelian varieties over finitely generated fields.

PROOF for elliptic curves E over $K = \mathbb{Q}$ was found by Louis Mordell in 1922.

Important step - Weak Mordell Theorem:

Theorem (Mordell – Weil)

Let E be an elliptic curve over a number field K.
Then the group $E(K)$ is finitely generated.

Remark. Conclusion remains valid for abelian varieties over finitely generated fields.

PROOF for elliptic curves E over $K = \mathbb{Q}$ was found by Louis Mordell in 1922.

Important step - Weak Mordell Theorem:

$E(\mathbb{Q})/2 \cdot E(\mathbb{Q})$ *is finite.*

Theorem (Mordell – Weil)

Let E be an elliptic curve over a number field K.
Then the group $E(K)$ is finitely generated.

Remark. Conclusion remains valid for abelian varieties over finitely generated fields.

PROOF for elliptic curves E over $K = \mathbb{Q}$ was found by Louis Mordell in 1922.

Important step - Weak Mordell Theorem:

$$E(\mathbb{Q})/2 \cdot E(\mathbb{Q}) \text{ is finite.}$$

Argument heavily relies on *reduction*.

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Assume that $a, b \in \mathbb{Z}$ and pick a prime $p > 2$.

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Assume that $a, b \in \mathbb{Z}$ and pick a prime $p > 2$.

Reducing modulo p, we obtain:

$$y^2 = \bar{f}(x) \quad \text{where} \quad \bar{f}(x) = x^3 + \bar{a}x + \bar{b}. \qquad \text{(R)}$$

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Assume that $a, b \in \mathbb{Z}$ and pick a prime $p > 2$.

Reducing modulo p, we obtain:

$$y^2 = \bar{f}(x) \quad \text{where} \quad \bar{f}(x) = x^3 + \bar{a}x + \bar{b}. \qquad \text{(R)}$$

Two possibilities:

- *$\bar{f}$ has no multiple roots.*
- *$\bar{f}$ has multiple roots.*

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Assume that $a, b \in \mathbb{Z}$ and pick a prime $p > 2$.

Reducing modulo p, we obtain:

$$y^2 = \bar{f}(x) \quad \text{where} \quad \bar{f}(x) = x^3 + \bar{a}x + \bar{b}. \qquad \text{(R)}$$

Two possibilities:

- $\bar{f}$ *has no multiple roots.*
- $\bar{f}$ *has multiple roots.*

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Assume that $a, b \in \mathbb{Z}$ and pick a prime $p > 2$.

Reducing modulo p, we obtain:

$$y^2 = \bar{f}(x) \quad \text{where} \quad \bar{f}(x) = x^3 + \bar{a}x + \bar{b}. \qquad \text{(R)}$$

Two possibilities:

- $\bar{f}$ *has no multiple roots.* Then (R) still defines an elliptic curve, and we say that (E) has good reduction at p.
- $\bar{f}$ *has multiple roots.*

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Assume that $a, b \in \mathbb{Z}$ and pick a prime $p > 2$.

Reducing modulo p, we obtain:

$$y^2 = \bar{f}(x) \quad \text{where} \quad \bar{f}(x) = x^3 + \bar{a}x + \bar{b}. \qquad \text{(R)}$$

Two possibilities:

- $\bar{f}$ *has no multiple roots.* Then (R) still defines an elliptic curve, and we say that (E) has good reduction at p.
- $\bar{f}$ *has multiple roots.*

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Assume that $a, b \in \mathbb{Z}$ and pick a prime $p > 2$.

Reducing modulo p, we obtain:

$$y^2 = \bar{f}(x) \quad \text{where} \quad \bar{f}(x) = x^3 + \bar{a}x + \bar{b}. \qquad \text{(R)}$$

Two possibilities:

- $\bar{f}$ *has no multiple roots.* Then (R) still defines an elliptic curve, and we say that (E) has good reduction at p.
- $\bar{f}$ *has multiple roots.* Then (R) defines a singular rational curve, and we say that (E) has bad reduction at p.

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Assume that $a, b \in \mathbb{Z}$ and pick a prime $p > 2$.

Reducing modulo p, we obtain:

$$y^2 = \bar{f}(x) \quad \text{where} \quad \bar{f}(x) = x^3 + \bar{a}x + \bar{b}. \qquad \text{(R)}$$

Two possibilities:

- $\bar{f}$ *has no multiple roots.* Then (R) still defines an elliptic curve, and we say that (E) has good reduction at p.
- $\bar{f}$ *has multiple roots.* Then (R) defines a singular rational curve, and we say that (E) has bad reduction at p.

Primes of bad reduction are those that divide discriminant of f.

Consider an affine equation of elliptic curve:

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^3 + ax + b \quad \text{(NO multiple roots!)} \quad \text{(E)}$$

Assume that $a, b \in \mathbb{Z}$ and pick a prime $p > 2$.

Reducing modulo p, we obtain:

$$y^2 = \bar{f}(x) \quad \text{where} \quad \bar{f}(x) = x^3 + \bar{a}x + \bar{b}. \qquad \text{(R)}$$

Two possibilities:

- $\bar{f}$ *has no multiple roots.* Then (R) still defines an elliptic curve, and we say that (E) has good reduction at p.
- $\bar{f}$ *has multiple roots.* Then (R) defines a singular rational curve, and we say that (E) has bad reduction at p.

Primes of bad reduction are those that divide discriminant of f.

So, they constitute a finite set.

Definition. Elliptic curve E has good reduction at $p > 3$

Definition. Elliptic curve E has good reduction at $p > 3$ **if** it admits an equation (E) that has good reduction at p,

Definition. Elliptic curve E has good reduction at $p > 3$ **if** it admits an equation (E) that has good reduction at p, and bad reduction otherwise.

Definition. Elliptic curve E has good reduction at $p > 3$ **if** it admits an equation (E) that has good reduction at p, and bad reduction otherwise.

More precisely, E has good reduction if it is isomorphic to E' that can be given by equation (E) having good reduction at p.

Definition. Elliptic curve E has good reduction at $p > 3$ **if** it admits an equation (E) that has good reduction at p, and bad reduction otherwise.

More precisely, E has good reduction if it is isomorphic to E' that can be given by equation (E) having good reduction at p.

In technical language, this means that there exists an abelian scheme $E_{(p)}$ over valuation ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ with generic fiber E (this scheme $E_{(p)}$ is then unique)

Definition. Elliptic curve E has good reduction at $p > 3$ **if** it admits an equation (E) that has good reduction at p, and bad reduction otherwise.

More precisely, E has good reduction if it is isomorphic to E' that can be given by equation (E) having good reduction at p.

In technical language, this means that there exists an abelian scheme $E_{(p)}$ over valuation ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ with generic fiber E (this scheme $E_{(p)}$ is then unique)

Example.

Equation $y^2 = x^3 - 625x$ has *bad* reduction at $p = 5$,

Definition. Elliptic curve E has good reduction at $p > 3$ **if** it admits an equation (E) that has good reduction at p, and bad reduction otherwise.

More precisely, E has good reduction if it is isomorphic to E' that can be given by equation (E) having good reduction at p.

In technical language, this means that there exists an abelian scheme $E_{(p)}$ over valuation ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ with generic fiber E (this scheme $E_{(p)}$ is then unique)

Example.

Equation $y^2 = x^3 - 625x$ has *bad* reduction at $p = 5$, **but** elliptic curve E it defines is isomorphic to elliptic curve E' given by $y^2 = x^3 - x$ which has *good* reduction at $p = 5$.

Definition. Elliptic curve E has good reduction at $p > 3$ **if** it admits an equation (E) that has good reduction at p, and bad reduction otherwise.

More precisely, E has good reduction if it is isomorphic to E' that can be given by equation (E) having good reduction at p.

In technical language, this means that there exists an abelian scheme $E_{(p)}$ over valuation ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ with generic fiber E (this scheme $E_{(p)}$ is then unique)

Example.

Equation $y^2 = x^3 - 625x$ has *bad* reduction at $p = 5$, **but** elliptic curve E it defines is isomorphic to elliptic curve E' given by $y^2 = x^3 - x$ which has *good* reduction at $p = 5$.

So, E has good reduction at $p = 5$.

Sketch of proof of Weak Mordell Theorem

Sketch of proof of Weak Mordell Theorem

Let E be an elliptic curve over $\mathbb{Q}$.

Sketch of proof of Weak Mordell Theorem

Let E be an elliptic curve over $\mathbb{Q}$.

- Let Π be (finite) set of primes of **bad** reduction $\cup \{2\}$.

Sketch of proof of Weak Mordell Theorem

Let E be an elliptic curve over $\mathbb{Q}$.

- Let Π be (finite) set of primes of **bad** reduction $\cup \{2\}$.
- For $P \in E(\overline{\mathbb{Q}})$, we let $\mathbb{Q}(P)$ denote *residue field* of P

Sketch of proof of Weak Mordell Theorem

Let E be an elliptic curve over $\mathbb{Q}$.

- Let Π be (finite) set of primes of **bad** reduction $\cup \{2\}$.
- For $P \in E(\overline{\mathbb{Q}})$, we let $\mathbb{Q}(P)$ denote *residue field* of P

(i.e., $\mathbb{Q}(P) = \mathbb{Q}$ if P is the point at infinity, and $\mathbb{Q}(P)$ is generated by affine coordinates of P otherwise).

Sketch of proof of Weak Mordell Theorem

Let E be an elliptic curve over $\mathbb{Q}$.

- Let Π be (finite) set of primes of **bad** reduction $\cup \{2\}$.
- For $P \in E(\overline{\mathbb{Q}})$, we let $\mathbb{Q}(P)$ denote *residue field* of P

(i.e., $\mathbb{Q}(P) = \mathbb{Q}$ if P is the point at infinity, and $\mathbb{Q}(P)$ is generated by affine coordinates of P otherwise).

- Let $\pi \colon E \to E$ be isogeny $P \mapsto 2 \cdot P$.

Sketch of proof of Weak Mordell Theorem

Let E be an elliptic curve over $\mathbb{Q}$.

- Let Π be (finite) set of primes of **bad** reduction $\cup \{2\}$.
- For $P \in E(\overline{\mathbb{Q}})$, we let $\mathbb{Q}(P)$ denote *residue field* of P

(i.e., $\mathbb{Q}(P) = \mathbb{Q}$ if P is the point at infinity, and $\mathbb{Q}(P)$ is generated by affine coordinates of P otherwise).

- Let $\pi \colon E \to E$ be isogeny $P \mapsto 2 \cdot P$.

Since π has degree 4, for any $P \in E(\mathbb{Q})$ and any $R \in \pi^{-1}(P)$,

$$[\mathbb{Q}(R) : \mathbb{Q}] \leqslant 4.$$

Sketch of proof of Weak Mordell Theorem

Sketch of proof of Weak Mordell Theorem

For $p \notin \Pi$, using good reduction at p, one shows that

$$\mathbb{Q}(R)/\mathbb{Q} \text{ is } \textit{unramified} \text{ at } p.$$

Sketch of proof of Weak Mordell Theorem

For $p \notin \Pi$, using good reduction at p, one shows that

$$\mathbb{Q}(R)/\mathbb{Q} \text{ is } \textit{unramified} \text{ at } p.$$

HERMITE: *There are only finitely many extensions of $\mathbb{Q}$ of a given degree and unramified outside a given finite set of primes.*

Sketch of proof of Weak Mordell Theorem

For $p \notin \Pi$, using good reduction at p, one shows that

$$\mathbb{Q}(R)/\mathbb{Q} \text{ is } \textit{unramified} \text{ at } p.$$

HERMITE: *There are only finitely many extensions of $\mathbb{Q}$ of a given degree and unramified outside a given finite set of primes.*

Thus, among field extensions $\mathbb{Q}(R)$, $R \in \pi^{-1}(E(\mathbb{Q}))$, there are only finitely many distinct

Sketch of proof of Weak Mordell Theorem

For $p \notin \Pi$, using good reduction at p, one shows that

$$\mathbb{Q}(R)/\mathbb{Q} \text{ is } \textit{unramified} \text{ at } p.$$

HERMITE: *There are only finitely many extensions of $\mathbb{Q}$ of a given degree and unramified outside a given finite set of primes.*

Thus, among field extensions $\mathbb{Q}(R)$, $R \in \pi^{-1}(E(\mathbb{Q}))$, there are only finitely many distinct $\Rightarrow$

Sketch of proof of Weak Mordell Theorem

For $p \notin \Pi$, using good reduction at p, one shows that

$$\mathbb{Q}(R)/\mathbb{Q} \text{ is } \textit{unramified} \text{ at } p.$$

HERMITE: *There are only finitely many extensions of $\mathbb{Q}$ of a given degree and unramified outside a given finite set of primes.*

Thus, among field extensions $\mathbb{Q}(R)$, $R \in \pi^{-1}(E(\mathbb{Q}))$, there are only finitely many distinct $\Rightarrow$

their compositum $\mathbb{Q}(\pi^{-1}(E(\mathbb{Q})))$ is a finite extension of $\mathbb{Q}$.

Sketch of proof of Weak Mordell Theorem

For $p \notin \Pi$, using good reduction at p, one shows that

$$\mathbb{Q}(R)/\mathbb{Q} \text{ is } \textit{unramified} \text{ at } p.$$

HERMITE: *There are only finitely many extensions of $\mathbb{Q}$ of a given degree and unramified outside a given finite set of primes.*

Thus, among field extensions $\mathbb{Q}(R)$, $R \in \pi^{-1}(E(\mathbb{Q}))$, there are only finitely many distinct $\Rightarrow$

their compositum $\mathbb{Q}(\pi^{-1}(E(\mathbb{Q})))$ is a finite extension of $\mathbb{Q}$.

Then a formal argument using Galois cohomology ("Kummer sequence") shows $E(\mathbb{Q})/2 \cdot E(\mathbb{Q})$ is finite.

SHAFAREVICH (ICM, 1962): *If* Π *is a finite set of primes then there are* finitely many *isomorphism classes of elliptic curves* E *over* $\mathbb{Q}$ *having good reduction at all* $p \notin \Pi$.

SHAFAREVICH (ICM, 1962): *If* Π *is a finite set of primes then there are* finitely many *isomorphism classes of elliptic curves* E *over* $\mathbb{Q}$ *having good reduction at all* $p \notin \Pi$.

(Shaferevich stated his theorem for an arbitrary number field K and a finite set of places S.)

SHAFAREVICH (ICM, 1962): *If* Π *is a finite set of primes then there are* finitely many *isomorphism classes of elliptic curves* E *over* $\mathbb{Q}$ *having good reduction at all* $p \notin \Pi$.

(Shaferevich stated his theorem for an arbitrary number field K and a finite set of places S.)

Sketch of proof

SHAFAREVICH (ICM, 1962): *If* Π *is a finite set of primes then there are* finitely many *isomorphism classes of elliptic curves* E *over* $\mathbb{Q}$ *having good reduction at all* $p \notin \Pi$.

(Shaferevich stated his theorem for an arbitrary number field K and a finite set of places S.)

Sketch of proof (attributed to Tate by Serre in *Abelian* ℓ*-adic Representations and Elliptic Curves*)

SHAFAREVICH (ICM, 1962): *If* Π *is a finite set of primes then there are* finitely many *isomorphism classes of elliptic curves* E *over* $\mathbb{Q}$ *having good reduction at all* $p \notin \Pi$.

(Shaferevich stated his theorem for an arbitrary number field K and a finite set of places S.)

Sketch of proof (attributed to Tate by Serre in *Abelian* ℓ*-adic Representations and Elliptic Curves*)

- We can assume that $2, 3 \in \Pi$, and let A be localization of $\mathbb{Z}$ w.r.t. Π.

SHAFAREVICH (ICM, 1962): *If* Π *is a finite set of primes then there are* finitely many *isomorphism classes of elliptic curves* E *over* $\mathbb{Q}$ *having good reduction at all* $p \notin \Pi$.

(Shaferevich stated his theorem for an arbitrary number field K and a finite set of places S.)

Sketch of proof (attributed to Tate by Serre in *Abelian ℓ-adic Representations and Elliptic Curves*)

- We can assume that $2, 3 \in \Pi$, and let A be localization of $\mathbb{Z}$ w.r.t. Π.
- Using that A is UFD, one shows that E can be given by

$$y^2 = f(x) \quad \text{where} \quad f(x) = x^2 + ax + b \tag{E}$$

with $a, b \in A$ and discriminant $\Delta = -4a^3 - 27b^2$ in $A^\times$.

- Note that if elliptic curves E_1, E_2 given by equations (E) have discriminants $\Delta_1, \Delta_2 \in A^\times$ and

$$\Delta_1 = \Delta_2 \, u^{12}, \; u \in A^\times,$$

- Note that if elliptic curves E_1, E_2 given by equations (E) have discriminants $\Delta_1, \Delta_2 \in A^\times$ and

$$\Delta_1 = \Delta_2 u^{12},\ u \in A^\times,$$

then one can replace E_1 by $E_1' \simeq E_1$ still given by (E) and such that $\Delta_1' = \Delta_2$.

- Note that if elliptic curves E_1, E_2 given by equations (E) have discriminants $\Delta_1, \Delta_2 \in A^\times$ and

$$\Delta_1 = \Delta_2 u^{12},\ u \in A^\times,$$

then one can replace E_1 by $E_1' \simeq E_1$ still given by (E) and such that $\Delta_1' = \Delta_2$.

- Since $A^\times/(A^\times)^{12}$ is finite,

- Note that if elliptic curves E_1, E_2 given by equations (E) have discriminants $\Delta_1, \Delta_2 \in A^\times$ and

$$\Delta_1 = \Delta_2 u^{12},\ u \in A^\times,$$

then one can replace E_1 by $E_1' \simeq E_1$ still given by (E) and such that $\Delta_1' = \Delta_2$.

- Since $A^\times/(A^\times)^{12}$ is finite, it is enough to show that for a *fixed* $\Delta_0 \in A^\times$, equation

$$-4a^3 - 27b^2 = \Delta_0 \tag{D}$$

has *finitely many* solutions $(a, b) \in A \times A$.

- Note that if elliptic curves E_1, E_2 given by equations (E) have discriminants $\Delta_1, \Delta_2 \in A^\times$ and

$$\Delta_1 = \Delta_2 u^{12},\ u \in A^\times,$$

then one can replace E_1 by $E_1' \simeq E_1$ still given by (E) and such that $\Delta_1' = \Delta_2$.

- Since $A^\times/(A^\times)^{12}$ is finite, it is enough to show that for a *fixed* $\Delta_0 \in A^\times$, equation

$$-4a^3 - 27b^2 = \Delta_0 \qquad \text{(D)}$$

has *finitely many* solutions $(a, b) \in A \times A$.

But since (D) defines a curve of genus 1, finiteness is guaranteed by Siegel's Theorem!

Shafarevich's Conjecture

Shafarevich's Conjecture

While this argument is specific to elliptic curves,

Shafarevich's Conjecture

While this argument is specific to elliptic curves, Shafarevich felt that his theorem was an instance of a far more general phenomenon.

Shafarevich's Conjecture

While this argument is specific to elliptic curves, Shafarevich felt that his theorem was an instance of a far more general phenomenon.

Conjecture.

Let K be a number field, and let S be a finite set of places of K.

Shafarevich's Conjecture

While this argument is specific to elliptic curves, Shafarevich felt that his theorem was an instance of a far more general phenomenon.

Conjecture.

Let K be a number field, and let S be a finite set of places of K. Then for every $g \geqslant 1$ there exist only finitely many isomorphism classes of abelian varieties of dimension g that have good reduction at all $\mathfrak{p} \notin S$.

Proof found by G. Faltings in 1982 was culmination of work in Diophantine geometry.

Proof found by G. Faltings in 1982 was culmination of work in Diophantine geometry.

Consequences include:

- Mordell conjecture: a smooth projective curve of genus $g \geqslant 2$ over a number field K has finitely many K-rational points;
- Shafarevich conjecture for curves: for $g \geqslant 2$, there are only finitely many isomorphism classes of curves of genus g having good reduction at all $\mathfrak{p} \notin S$.

Proof found by G. Faltings in 1982 was culmination of work in Diophantine geometry.

Consequences include:

- Mordell conjecture: a smooth projective curve of genus $g \geqslant 2$ over a number field K has finitely many K-rational points;
- Shafarevich conjecture for curves: for $g \geqslant 2$, there are only finitely many isomorphism classes of curves of genus g having good reduction at all $\mathfrak{p} \notin S$.

Proof found by G. Faltings in 1982 was culmination of work in Diophantine geometry.

Consequences include:

- Mordell conjecture: a smooth projective curve of genus $g \geqslant 2$ over a number field K has finitely many K-rational points;
- Shafarevich conjecture for curves: for $g \geqslant 2$, there are only finitely many isomorphism classes of curves of genus g having good reduction at all $\mathfrak{p} \notin S$.

Proof found by G. Faltings in 1982 was culmination of work in Diophantine geometry.

Consequences include:

- Mordell conjecture: a smooth projective curve of genus $g \geqslant 2$ over a number field K has finitely many K-rational points;
- Shafarevich conjecture for curves: for $g \geqslant 2$, there are only finitely many isomorphism classes of curves of genus g having good reduction at all $\mathfrak{p} \notin S$.

We would like to find analogs of these results for *linear algebraic groups*.

Basic definitions

- A *linear algebraic group* is a subgroup $G \subset \mathrm{GL}_n$ that can be defined by polynomial equations in terms of matrix entries x_{ij};
- If ideal of polynomials $p(x_{11}, \ldots, x_{nn})$ that vanish on G is generated by polynomials with coefficients in a (sub)field K then G is *K-defined*;
- *Morphisms* of algebraic groups are group homomorphisms that can be represented by polynomials in terms of x_{ij} and $\det(x_{ij})^{-1}$.

Basic definitions

- A *linear algebraic group* is a subgroup $G \subset \mathrm{GL}_n$ that can be defined by polynomial equations in terms of matrix entries x_{ij};
- If ideal of polynomials $p(x_{11}, \ldots, x_{nn})$ that vanish on G is generated by polynomials with coefficients in a (sub)field K then G is *K-defined*;
- *Morphisms* of algebraic groups are group homomorphisms that can be represented by polynomials in terms of x_{ij} and $\det(x_{ij})^{-1}$.

Basic definitions

- A *linear algebraic group* is a subgroup $G \subset \mathrm{GL}_n$ that can be defined by polynomial equations in terms of matrix entries x_{ij};
- If ideal of polynomials $p(x_{11}, \ldots, x_{nn})$ that vanish on G is generated by polynomials with coefficients in a (sub)field K then G is K-*defined*;
- *Morphisms* of algebraic groups are group homomorphisms that can be represented by polynomials in terms of x_{ij} and $\det(x_{ij})^{-1}$.

Basic definitions

- A *linear algebraic group* is a subgroup $G \subset \mathrm{GL}_n$ that can be defined by polynomial equations in terms of matrix entries x_{ij};
- If ideal of polynomials $p(x_{11}, \ldots, x_{nn})$ that vanish on G is generated by polynomials with coefficients in a (sub)field K then G is K-*defined*;

  (if $\mathrm{char}\, K = 0$ then it is enough to require that G be defined by polynomials with coefficients in K)
- *Morphisms* of algebraic groups are group homomorphisms that can be represented by polynomials in terms of x_{ij} and $\det(x_{ij})^{-1}$.

Basic definitions

- A *linear algebraic group* is a subgroup $G \subset \mathrm{GL}_n$ that can be defined by polynomial equations in terms of matrix entries x_{ij};
- If ideal of polynomials $p(x_{11}, \ldots, x_{nn})$ that vanish on G is generated by polynomials with coefficients in a (sub)field K then G is K-*defined*;

  (if $\mathrm{char}\, K = 0$ then it is enough to require that G be defined by polynomials with coefficients in K)
- *Morphisms* of algebraic groups are group homomorphisms that can be represented by polynomials in terms of x_{ij} and $\det(x_{ij})^{-1}$.

Classes of linear algebraic groups

- *Unipotent radical* of a (connected) algebraic group G is *largest* connected unipotent normal subgroup.
- A (connected) algebraic group G is *reductive* if unipotent radical is *trivial*.
- A (connected) algebraic group G is (absolutely almost) *simple* if it does not contain proper connected normal subgroups.

Classes of linear algebraic groups

- *Unipotent radical* of a (connected) algebraic group G is *largest* connected unipotent normal subgroup.
- A (connected) algebraic group G is *reductive* if unipotent radical is *trivial*.
- A (connected) algebraic group G is (absolutely almost) *simple* if it does not contain proper connected normal subgroups.

Classes of linear algebraic groups

- *Unipotent radical* of a (connected) algebraic group G is *largest* connected unipotent normal subgroup.
- A (connected) algebraic group G is *reductive* if unipotent radical is *trivial*.
- A (connected) algebraic group G is (absolutely almost) *simple* if it does not contain proper connected normal subgroups.

Classes of linear algebraic groups

- *Unipotent radical* of a (connected) algebraic group G is *largest* connected unipotent normal subgroup.
- A (connected) algebraic group G is *reductive* if unipotent radical is *trivial*.

  Examples: GL_n, SL_n, Sp_{2n}, $\mathrm{SO}_n(q)$, ...
- A (connected) algebraic group G is (absolutely almost) *simple* if it does not contain proper connected normal subgroups.

Classes of linear algebraic groups

- *Unipotent radical* of a (connected) algebraic group G is *largest* connected unipotent normal subgroup.
- A (connected) algebraic group G is *reductive* if unipotent radical is *trivial*.

  Examples: GL_n, SL_n, Sp_{2n}, $\mathrm{SO}_n(q)$, ...
- A (connected) algebraic group G is (absolutely almost) *simple* if it does not contain proper connected normal subgroups.

Classes of linear algebraic groups

- *Unipotent radical* of a (connected) algebraic group G is *largest* connected unipotent normal subgroup.
- A (connected) algebraic group G is *reductive* if unipotent radical is *trivial*.

  Examples: GL_n, SL_n, Sp_{2n}, $\mathrm{SO}_n(q)$, ...
- A (connected) algebraic group G is (absolutely almost) *simple* if it does not contain proper connected normal subgroups.

  Examples: SL_n, Sp_{2n}, $\mathrm{SO}_n(q)$ $(n = 3$ or $\geqslant 5)$, ...

Classes of linear algebraic groups

- *Unipotent radical* of a (connected) algebraic group G is *largest* connected unipotent normal subgroup.
- A (connected) algebraic group G is *reductive* if unipotent radical is *trivial*.

  Examples: GL_n, SL_n, Sp_{2n}, $\mathrm{SO}_n(q)$, ...
- A (connected) algebraic group G is (absolutely almost) *simple* if it does not contain proper connected normal subgroups.

  Examples: SL_n, Sp_{2n}, $\mathrm{SO}_n(q)$ $(n = 3$ or $\geqslant 5)$, ...

  It is *semi-simple* if it admits a surjective morphism from a direct product of simple groups.

Classes of linear algebraic groups

- *Unipotent radical* of a (connected) algebraic group G is *largest* connected unipotent normal subgroup.
- A (connected) algebraic group G is *reductive* if unipotent radical is *trivial*.

  Examples: GL_n, SL_n, Sp_{2n}, $\mathrm{SO}_n(q)$, ...
- A (connected) algebraic group G is (absolutely almost) *simple* if it does not contain proper connected normal subgroups.

  Examples: SL_n, Sp_{2n}, $\mathrm{SO}_n(q)$ $(n = 3$ or $\geqslant 5)$, ...

  It is *semi-simple* if it admits a surjective morphism from a direct product of simple groups. **Example:** $\mathrm{SO}_4(q)$

Examples of reductions of algebraic group modulo p

Examples of reductions of algebraic group modulo p

Example 1. Let $G = \mathrm{GL}_n$ over $\mathbb{Q}$.

Examples of reductions of algebraic group modulo p

Example 1. Let $G = \mathrm{GL}_n$ over $\mathbb{Q}$. One can think of G as $\mathbb{Z}$-group scheme $\operatorname{Spec} A$ where

$$A = \mathbb{Z}\left[x_{11}, \ldots, x_{nn}, \frac{1}{\det(x_{ij})}\right].$$

Examples of reductions of algebraic group modulo p

Example 1. Let $G = \mathrm{GL}_n$ over $\mathbb{Q}$. One can think of G as $\mathbb{Z}$-group scheme $\operatorname{Spec} A$ where

$$A = \mathbb{Z}\left[x_{11}, \ldots, x_{nn}, \frac{1}{\det(x_{ij})}\right].$$

Viz., for any commutative ring R, $\mathrm{GL}_n(R)$ can be identified with $\mathrm{Hom}_{\mathbb{Z}\text{-alg}}(A, R)$.

Examples of reductions of algebraic group modulo p

Example 1. Let $G = \mathrm{GL}_n$ over $\mathbb{Q}$. One can think of G as $\mathbb{Z}$-group scheme $\operatorname{Spec} A$ where

$$A = \mathbb{Z}\left[x_{11}, \ldots, x_{nn}, \frac{1}{\det(x_{ij})}\right].$$

Viz., for any commutative ring R, $\mathrm{GL}_n(R)$ can be identified with $\mathrm{Hom}_{\mathbb{Z}\text{-alg}}(A, R)$.

Given a prime p, we can reduce modulo p:

Examples of reductions of algebraic group modulo p

Example 1. Let $G = \mathrm{GL}_n$ over $\mathbb{Q}$. One can think of G as $\mathbb{Z}$-group scheme $\operatorname{Spec} A$ where

$$A = \mathbb{Z}\left[x_{11}, \ldots, x_{nn}, \frac{1}{\det(x_{ij})}\right].$$

Viz., for any commutative ring R, $\mathrm{GL}_n(R)$ can be identified with $\mathrm{Hom}_{\mathbb{Z}\text{-alg}}(A, R)$.

Given a prime p, we can reduce modulo p:

$$A_p := A \otimes_{\mathbb{Z}} \mathbb{F}_p = \mathbb{F}_p\left[x_{11}, \ldots, x_{nn}, \frac{1}{\det(x_{ij})}\right].$$

Examples of reductions of algebraic group modulo p

Example 1. Let $G = \mathrm{GL}_n$ over $\mathbb{Q}$. One can think of G as $\mathbb{Z}$-group scheme $\operatorname{Spec} A$ where

$$A = \mathbb{Z}\left[x_{11}, \ldots, x_{nn}, \frac{1}{\det(x_{ij})}\right].$$

Viz., for any commutative ring R, $\mathrm{GL}_n(R)$ can be identified with $\mathrm{Hom}_{\mathbb{Z}\text{-alg}}(A, R)$.

Given a prime p, we can reduce modulo p:

$$A_p := A \otimes_{\mathbb{Z}} \mathbb{F}_p = \mathbb{F}_p\left[x_{11}, \ldots, x_{nn}, \frac{1}{\det(x_{ij})}\right].$$

Then A_p represents GL_n over rings of characteristic p.

Examples of reductions of algebraic group modulo p

Example 1. Let $G = \mathrm{GL}_n$ over $\mathbb{Q}$. One can think of G as $\mathbb{Z}$-group scheme $\operatorname{Spec} A$ where

$$A = \mathbb{Z}\left[x_{11}, \ldots, x_{nn}, \frac{1}{\det(x_{ij})}\right].$$

Viz., for any commutative ring R, $\mathrm{GL}_n(R)$ can be identified with $\mathrm{Hom}_{\mathbb{Z}\text{-alg}}(A, R)$.

Given a prime p, we can reduce modulo p:

$$A_p := A \otimes_{\mathbb{Z}} \mathbb{F}_p = \mathbb{F}_p\left[x_{11}, \ldots, x_{nn}, \frac{1}{\det(x_{ij})}\right].$$

Then A_p represents GL_n over rings of characteristic p.

Thus, reduction of $\mathrm{GL}_n/\mathbb{Z}$ modulo p is $\mathrm{GL}_n/\mathbb{F}_p$.

Examples of reductions of algebraic group modulo p

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$.

,

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$. Its reduction modulo p is represented by $\mathbb{F}_p[x, x^{-1}]$,

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$. Its reduction modulo p is represented by $\mathbb{F}_p[x, x^{-1}]$, i.e. 1-dimensional split torus over $\mathbb{F}_p$.

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$. Its reduction modulo p is represented by $\mathbb{F}_p[x, x^{-1}]$, i.e. 1-dimensional split torus over $\mathbb{F}_p$.

More generally, reduction modulo p of d-dimensional split torus $\mathbb{G}_m^d$,

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$. Its reduction modulo p is represented by $\mathbb{F}_p[x, x^{-1}]$, i.e. 1-dimensional split torus over $\mathbb{F}_p$.

More generally, reduction modulo p of d-dimensional split torus $\mathbb{G}_m^d$, which is represented by $\mathbb{Z}[x_1, \dots, x_d, x_1^{-1}, \dots, x_d^{-1}]$,

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$. Its reduction modulo p is represented by $\mathbb{F}_p[x, x^{-1}]$, i.e. 1-dimensional split torus over $\mathbb{F}_p$.

More generally, reduction modulo p of d-dimensional split torus $\mathbb{G}_m^d$, which is represented by $\mathbb{Z}[x_1, \dots, x_d, x_1^{-1}, \dots, x_d^{-1}]$, is d-dimensional split torus over $\mathbb{F}_p$.

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$. Its reduction modulo p is represented by $\mathbb{F}_p[x, x^{-1}]$, i.e. 1-dimensional split torus over $\mathbb{F}_p$.

More generally, reduction modulo p of d-dimensional split torus $\mathbb{G}_m^d$, which is represented by $\mathbb{Z}[x_1, \dots, x_d, x_1^{-1}, \dots, x_d^{-1}]$, is d-dimensional split torus over $\mathbb{F}_p$.

Example 2. Let $G = \mathrm{SL}_n$.

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$. Its reduction modulo p is represented by $\mathbb{F}_p[x, x^{-1}]$, i.e. 1-dimensional split torus over $\mathbb{F}_p$.

More generally, reduction modulo p of d-dimensional split torus $\mathbb{G}_m^d$, which is represented by $\mathbb{Z}[x_1, \dots, x_d, x_1^{-1}, \dots, x_d^{-1}]$, is d-dimensional split torus over $\mathbb{F}_p$.

Example 2. Let $G = \mathrm{SL}_n$. Then G is represented by $\mathbb{Z}$-algebra

$$\mathbb{Z}[x_{11}, \dots, x_{nn}]/(\det(x_{ij}) - 1).$$

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$. Its reduction modulo p is represented by $\mathbb{F}_p[x, x^{-1}]$, i.e. 1-dimensional split torus over $\mathbb{F}_p$.

More generally, reduction modulo p of d-dimensional split torus $\mathbb{G}_m^d$, which is represented by $\mathbb{Z}[x_1, \dots, x_d, x_1^{-1}, \dots, x_d^{-1}]$, is d-dimensional split torus over $\mathbb{F}_p$.

Example 2. Let $G = \mathrm{SL}_n$. Then G is represented by $\mathbb{Z}$-algebra

$$\mathbb{Z}[x_{11}, \dots, x_{nn}]/(\det(x_{ij}) - 1).$$

Reduction modulo p is $\mathbb{F}_p[x_{11}, \dots, x_{nn}]/(\det(x_{ij}) - 1)$ which represents SL_n over rings of characteristic p.

Examples of reductions of algebraic group modulo p

In particular, 1-dimensional split torus $\mathbb{G}_m = \mathrm{GL}_1$ is represented $\mathbb{Z}[x, x^{-1}]$. Its reduction modulo p is represented by $\mathbb{F}_p[x, x^{-1}]$, i.e. 1-dimensional split torus over $\mathbb{F}_p$.

More generally, reduction modulo p of d-dimensional split torus $\mathbb{G}_m^d$, which is represented by $\mathbb{Z}[x_1, \dots, x_d, x_1^{-1}, \dots, x_d^{-1}]$, is d-dimensional split torus over $\mathbb{F}_p$.

Example 2. Let $G = \mathrm{SL}_n$. Then G is represented by $\mathbb{Z}$-algebra

$$\mathbb{Z}[x_{11}, \dots, x_{nn}]/(\det(x_{ij}) - 1).$$

Reduction modulo p is $\mathbb{F}_p[x_{11}, \dots, x_{nn}]/(\det(x_{ij}) - 1)$ which represents SL_n over rings of characteristic p.

Thus, reduction of $\mathrm{SL}_n/\mathbb{Z}$ modulo p is $\mathrm{SL}_n/\mathbb{F}_p$.

Examples of reductions of algebraic group modulo p

Examples of reductions of algebraic group modulo p

Example 3. Let $G = \mathrm{SO}_n(q)$ where $q = x_1^2 + \cdots + x_n^2$ and $n \geqslant 3$.

Examples of reductions of algebraic group modulo p

Example 3. Let $G = \mathrm{SO}_n(q)$ where $q = x_1^2 + \cdots + x_n^2$ and $n \geqslant 3$. Then reduction of G modulo any $p > 2$ is $\mathrm{SO}_n(\bar{q})$ where $\bar{q} = x_1^2 + \cdots + x_n^2$ over $\mathbb{F}_p$.

Examples of reductions of algebraic group modulo p

Example 3. Let $G = \mathrm{SO}_n(q)$ where $q = x_1^2 + \cdots + x_n^2$ and $n \geqslant 3$. Then reduction of G modulo any $p > 2$ is $\mathrm{SO}_n(\bar{q})$ where $\bar{q} = x_1^2 + \cdots + x_n^2$ over $\mathbb{F}_p$.

In all these examples, reduction modulo p of a given algebraic group/$\mathbb{Z}$ is an algebraic group of same type /$\mathbb{F}_p$.

Examples of reductions of algebraic group modulo p

Example 3. Let $G = \mathrm{SO}_n(q)$ where $q = x_1^2 + \cdots + x_n^2$ and $n \geqslant 3$. Then reduction of G modulo any $p > 2$ is $\mathrm{SO}_n(\bar{q})$ where $\bar{q} = x_1^2 + \cdots + x_n^2$ over $\mathbb{F}_p$.

In all these examples, reduction modulo p of a given algebraic group/$\mathbb{Z}$ is an algebraic group of same type /$\mathbb{F}_p$.

More precisely, groups in Example 1 (i.e., GL_n and split tori) are (connected and) *reductive*,

Examples of reductions of algebraic group modulo p

Example 3. Let $G = \mathrm{SO}_n(q)$ where $q = x_1^2 + \cdots + x_n^2$ and $n \geqslant 3$. Then reduction of G modulo any $p > 2$ is $\mathrm{SO}_n(\bar{q})$ where $\bar{q} = x_1^2 + \cdots + x_n^2$ over $\mathbb{F}_p$.

In all these examples, reduction modulo p of a given algebraic group/$\mathbb{Z}$ is an algebraic group of same type /$\mathbb{F}_p$.

More precisely, groups in Example 1 (i.e., GL_n and split tori) are (connected and) *reductive*, and so are their reductions modulo all p.

Examples of reductions of algebraic group modulo p

Example 3. Let $G = \mathrm{SO}_n(q)$ where $q = x_1^2 + \cdots + x_n^2$ and $n \geqslant 3$.

Then reduction of G modulo any $p > 2$ is $\mathrm{SO}_n(\bar{q})$ where $\bar{q} = x_1^2 + \cdots + x_n^2$ over $\mathbb{F}_p$.

In all these examples, reduction modulo p of a given algebraic group/$\mathbb{Z}$ is an algebraic group of same type /$\mathbb{F}_p$.

More precisely, groups in Example 1 (i.e., GL_n and split tori) are (connected and) *reductive*, and so are their reductions modulo all p.

Groups in Examples 2 and 3 are (connected and) *semi-simple*,

Examples of reductions of algebraic group modulo p

Example 3. Let $G = \mathrm{SO}_n(q)$ where $q = x_1^2 + \cdots + x_n^2$ and $n \geqslant 3$. Then reduction of G modulo any $p > 2$ is $\mathrm{SO}_n(\bar{q})$ where $\bar{q} = x_1^2 + \cdots + x_n^2$ over $\mathbb{F}_p$.

In all these examples, reduction modulo p of a given algebraic group/$\mathbb{Z}$ is an algebraic group of same type /$\mathbb{F}_p$.

More precisely, groups in Example 1 (i.e., GL_n and split tori) are (connected and) *reductive*, and so are their reductions modulo all p.

Groups in Examples 2 and 3 are (connected and) *semi-simple*, and their reductions (for $p \neq 2$ in Example 3) are (connected and) semi-simple.

Examples of reductions of algebraic group modulo p

Example 3. Let $G = \mathrm{SO}_n(q)$ where $q = x_1^2 + \cdots + x_n^2$ and $n \geqslant 3$.

Then reduction of G modulo any $p > 2$ is $\mathrm{SO}_n(\bar{q})$ where $\bar{q} = x_1^2 + \cdots + x_n^2$ over $\mathbb{F}_p$.

In all these examples, reduction modulo p of a given algebraic group/$\mathbb{Z}$ is an algebraic group of same type /$\mathbb{F}_p$.

More precisely, groups in Example 1 (i.e., GL_n and split tori) are (connected and) *reductive*, and so are their reductions modulo all p.

Groups in Examples 2 and 3 are (connected and) *semi-simple*, and their reductions (for $p \neq 2$ in Example 3) are (connected and) semi-simple.

Here are examples of a different nature.

Examples of reductions of algebraic group modulo p

Examples of reductions of algebraic group modulo p

Example 4. Fix a prime $p > 2$, and consider $L = \mathbb{Q}(\sqrt{p})$.

Examples of reductions of algebraic group modulo p

Example 4. Fix a prime $p > 2$, and consider $L = \mathbb{Q}(\sqrt{p})$.

Recall that for $z = a + b\sqrt{p} \in L$, the norm $\mathrm{N}_{L/\mathbb{Q}}(z) = a^2 - pb^2$.

Examples of reductions of algebraic group modulo p

Example 4. Fix a prime $p > 2$, and consider $L = \mathbb{Q}(\sqrt{p})$.

Recall that for $z = a + b\sqrt{p} \in L$, the norm $\mathrm{N}_{L/\mathbb{Q}}(z) = a^2 - pb^2$.

There exists algebraic $\mathbb{Q}$-group $G = \mathrm{R}^{(1)}_{L/\mathbb{Q}}(\mathbb{G}_m)$ (norm torus) such that

$$G(\mathbb{Q}) = \{z \in L^\times \mid \mathrm{N}_{L/\mathbb{Q}}(z) = 1\}.$$

Examples of reductions of algebraic group modulo p

Example 4. Fix a prime $p > 2$, and consider $L = \mathbb{Q}(\sqrt{p})$.

Recall that for $z = a + b\sqrt{p} \in L$, the norm $\mathrm{N}_{L/\mathbb{Q}}(z) = a^2 - pb^2$.

There exists algebraic $\mathbb{Q}$-group $G = \mathrm{R}^{(1)}_{L/\mathbb{Q}}(\mathbb{G}_m)$ (norm torus) such that

$$G(\mathbb{Q}) = \{z \in L^\times \mid \mathrm{N}_{L/\mathbb{Q}}(z) = 1\}.$$

Explicitly,

$$G = \left\{ X = \begin{pmatrix} a & pb \\ b & a \end{pmatrix} \mid \det(X) = 1 \right\}.$$

Examples of reductions of algebraic group modulo p

Example 4. Fix a prime $p > 2$, and consider $L = \mathbb{Q}(\sqrt{p})$.

Recall that for $z = a + b\sqrt{p} \in L$, the norm $\mathrm{N}_{L/\mathbb{Q}}(z) = a^2 - pb^2$.

There exists algebraic $\mathbb{Q}$-group $G = \mathrm{R}^{(1)}_{L/\mathbb{Q}}(\mathbb{G}_m)$ (norm torus) such that

$$G(\mathbb{Q}) = \{z \in L^\times \mid \mathrm{N}_{L/\mathbb{Q}}(z) = 1\}.$$

Explicitly,

$$G = \left\{ X = \begin{pmatrix} a & pb \\ b & a \end{pmatrix} \mid \det(X) = 1 \right\}.$$

Matrix $\begin{pmatrix} \sqrt{p} & -\sqrt{p} \\ 1 & 1 \end{pmatrix}$ conjugates G into

$$\left\{ \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \mid uv = 1 \right\},$$

Examples of reductions of algebraic group modulo p

Example 4. Fix a prime $p > 2$, and consider $L = \mathbb{Q}(\sqrt{p})$.

Recall that for $z = a + b\sqrt{p} \in L$, the norm $\mathrm{N}_{L/\mathbb{Q}}(z) = a^2 - pb^2$.

There exists algebraic $\mathbb{Q}$-group $G = \mathrm{R}^{(1)}_{L/\mathbb{Q}}(\mathbb{G}_m)$ (norm torus) such that

$$G(\mathbb{Q}) = \{z \in L^\times \mid \mathrm{N}_{L/\mathbb{Q}}(z) = 1\}.$$

Explicitly,

$$G = \left\{ X = \begin{pmatrix} a & pb \\ b & a \end{pmatrix} \mid \det(X) = 1 \right\}.$$

Matrix $\begin{pmatrix} \sqrt{p} & -\sqrt{p} \\ 1 & 1 \end{pmatrix}$ conjugates G into

$$\left\{ \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \mid uv = 1 \right\},$$

So, G is 1-dimensional ($\mathbb{Q}$-anisotropic) torus.

Examples of reductions of algebraic group modulo p

Examples of reductions of algebraic group modulo p

G is given by following equations on 2×2-matrix $X = (x_{ij})$:

$$x_{11} = x_{44}, \quad x_{12} = px_{21}, \quad x_{11}^2 - px_{21}^2 = 1. \tag{T}$$

Examples of reductions of algebraic group modulo p

G is given by following equations on 2×2-matrix $X = (x_{ij})$:

$$x_{11} = x_{44}, \quad x_{12} = px_{21}, \quad x_{11}^2 - px_{21}^2 = 1. \tag{T}$$

Reducing modulo p, we obtain:

$$x_{11} = x_{44}, \quad x_{12} = 0, \quad x_{11}^2 = 1.$$

Examples of reductions of algebraic group modulo p

G is given by following equations on 2×2-matrix $X = (x_{ij})$:

$$x_{11} = x_{44}, \quad x_{12} = px_{21}, \quad x_{11}^2 - px_{21}^2 = 1. \tag{T}$$

Reducing modulo p, we obtain:

$$x_{11} = x_{44}, \quad x_{12} = 0, \quad x_{11}^2 = 1.$$

Solutions are of the form $\pm \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$.

Examples of reductions of algebraic group modulo p

G is given by following equations on 2×2-matrix $X = (x_{ij})$:

$$x_{11} = x_{44}, \quad x_{12} = px_{21}, \quad x_{11}^2 - px_{21}^2 = 1. \tag{T}$$

Reducing modulo p, we obtain:

$$x_{11} = x_{44}, \quad x_{12} = 0, \quad x_{11}^2 = 1.$$

Solutions are of the form $\pm \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$.

So, reduction of (T) modulo p defines *disconnected* $\mathbb{F}_p$-group whose connected component is 1-dimensional unipotent group!

Examples of reductions of algebraic group modulo p

G is given by following equations on 2×2-matrix $X = (x_{ij})$:

$$x_{11} = x_{44}, \quad x_{12} = px_{21}, \quad x_{11}^2 - px_{21}^2 = 1. \tag{T}$$

Reducing modulo p, we obtain:

$$x_{11} = x_{44}, \quad x_{12} = 0, \quad x_{11}^2 = 1.$$

Solutions are of the form $\pm \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$.

So, reduction of (T) modulo p defines *disconnected* $\mathbb{F}_p$-group whose connected component is 1-dimensional unipotent group!

On the other hand, reducing (T) modulo any $q > 2$, $q \neq p$, one still gets 1-dimensional torus.

Examples of reductions of algebraic group modulo p

,

Examples of reductions of algebraic group modulo p

Example 5 (*noncommutative version of Example 4*)

,

Examples of reductions of algebraic group modulo p

Example 5 (*noncommutative version of Example 4*) Fix a prime $p > 2$,

Examples of reductions of algebraic group modulo p

Example 5 (*noncommutative version of Example 4*) Fix a prime $p > 2$, and let D be quaternion algebra corresponding to pair $(-1, p)$.

Examples of reductions of algebraic group modulo p

Example 5 (*noncommutative version of Example 4*) Fix a prime $p > 2$, and let D be quaternion algebra corresponding to pair $(-1, p)$. So, D has $\mathbb{Q}$-basis $1, i, j, k$ with multiplication table

Examples of reductions of algebraic group modulo p

Example 5 (*noncommutative version of Example 4*) Fix a prime $p > 2$, and let D be quaternion algebra corresponding to pair $(-1, p)$. So, D has $\mathbb{Q}$-basis $1, i, j, k$ with multiplication table

$$i^2 = -1, \quad j^2 = p, \quad k = ij = -ji, \quad k^2 = p.$$

Examples of reductions of algebraic group modulo p

Example 5 (*noncommutative version of Example 4*) Fix a prime $p > 2$, and let D be quaternion algebra corresponding to pair $(-1, p)$. So, D has $\mathbb{Q}$-basis $1, i, j, k$ with multiplication table

$$i^2 = -1, \quad j^2 = p, \quad k = ij = -ji, \quad k^2 = p.$$

For a quaternion $z = a + bi + cj + dk$, the *reduced norm* is

$$\mathrm{Nrd}_{D/\mathbb{Q}}(z) = a^2 + b^2 - pc^2 - pd^2.$$

Examples of reductions of algebraic group modulo p

Example 5 (*noncommutative version of Example 4*) Fix a prime $p > 2$, and let D be quaternion algebra corresponding to pair $(-1, p)$. So, D has $\mathbb{Q}$-basis $1, i, j, k$ with multiplication table

$$i^2 = -1, \quad j^2 = p, \quad k = ij = -ji, \quad k^2 = p.$$

For a quaternion $z = a + bi + cj + dk$, the *reduced norm* is

$$\mathrm{Nrd}_{D/\mathbb{Q}}(z) = a^2 + b^2 - pc^2 - pd^2.$$

There exists an algebraic $\mathbb{Q}$-group $G = \mathrm{SL}_{1,D}$ with

$$G(\mathbb{Q}) = \{z \in D^\times \mid \mathrm{Nrd}_{D/\mathbb{Q}}(z) = 1\}.$$

Examples of reductions of algebraic group modulo p

Examples of reductions of algebraic group modulo p

Using *regular representation* of D, one realizes G by matrices

Examples of reductions of algebraic group modulo p

Using *regular representation* of D, one realizes G by matrices

$$\begin{pmatrix} a & -b & pc & -pd \\ b & a & pd & -pc \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \quad \text{with} \quad a^2 + b^2 - pc^2 - pd^2 = 1. \qquad \text{(SL)}$$

Examples of reductions of algebraic group modulo p

Using *regular representation* of D, one realizes G by matrices

$$\begin{pmatrix} a & -b & pc & -pd \\ b & a & pd & -pc \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \quad \text{with} \quad a^2 + b^2 - pc^2 - pd^2 = 1. \tag{SL}$$

One can find matrix over $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{p})$ that *conjugates* G into matrices

$$\begin{pmatrix} A & O \\ O & A \end{pmatrix} \quad \text{with} \quad A \in \mathrm{SL}_2.$$

Examples of reductions of algebraic group modulo p

Using *regular representation* of D, one realizes G by matrices

$$\begin{pmatrix} a & -b & pc & -pd \\ b & a & pd & -pc \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \quad \text{with} \quad a^2 + b^2 - pc^2 - pd^2 = 1. \tag{SL}$$

One can find matrix over $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{p})$ that *conjugates* G into matrices

$$\begin{pmatrix} A & O \\ O & A \end{pmatrix} \quad \text{with} \quad A \in \mathrm{SL}_2.$$

So, $G \simeq \mathrm{SL}_2$ over either field, hence over $\overline{\mathbb{Q}}$.

Examples of reductions of algebraic group modulo p

Using *regular representation* of D, one realizes G by matrices

$$\begin{pmatrix} a & -b & pc & -pd \\ b & a & pd & -pc \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \quad \text{with} \quad a^2 + b^2 - pc^2 - pd^2 = 1. \tag{SL}$$

One can find matrix over $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{p})$ that *conjugates* G into matrices

$$\begin{pmatrix} A & O \\ O & A \end{pmatrix} \quad \text{with} \quad A \in \mathrm{SL}_2.$$

So, $G \simeq \mathrm{SL}_2$ over either field, hence over $\overline{\mathbb{Q}}$.

In other words, G is $\mathbb{Q}$-*form* of SL_2

Examples of reductions of algebraic group modulo p

Using *regular representation* of D, one realizes G by matrices

$$\begin{pmatrix} a & -b & pc & -pd \\ b & a & pd & -pc \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \quad \text{with} \quad a^2 + b^2 - pc^2 - pd^2 = 1. \tag{SL}$$

One can find matrix over $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{p})$ that *conjugates* G into matrices

$$\begin{pmatrix} A & O \\ O & A \end{pmatrix} \quad \text{with} \quad A \in \mathrm{SL}_2.$$

So, $G \simeq \mathrm{SL}_2$ over either field, hence over $\overline{\mathbb{Q}}$.

In other words, G is $\mathbb{Q}$-*form* of SL_2 (in particular, *simple* group).

Examples of reductions of algebraic group modulo p

Examples of reductions of algebraic group modulo p

Reducing equations that define (SL) yields system with solution set

$$\begin{pmatrix} a & -b & 0 & 0 \\ b & a & 0 & 0 \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \quad \text{with} \quad a^2 + b^2 = 1.$$

Examples of reductions of algebraic group modulo p

Reducing equations that define (SL) yields system with solution set

$$\begin{pmatrix} a & -b & 0 & 0 \\ b & a & 0 & 0 \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \quad \text{with} \quad a^2 + b^2 = 1.$$

This group is no longer simple!

Examples of reductions of algebraic group modulo p

Reducing equations that define (SL) yields system with solution set

$$\begin{pmatrix} a & -b & 0 & 0 \\ b & a & 0 & 0 \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \quad \text{with} \quad a^2 + b^2 = 1.$$

This group is no longer simple! In fact, it is solvable and has *nontrivial* unipotent radical, hence nonreductive.

Thus, reductive $\mathbb{Q}$-groups in Examples 1-3 can be described by polynomial systems with coefficients in $\mathbb{Z}$ (or valuation ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$) such that their reductions modulo p still define reductive groups.

Thus, reductive $\mathbb{Q}$-groups in Examples 1-3 can be described by polynomial systems with coefficients in $\mathbb{Z}$ (or valuation ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$) such that their reductions modulo p still define reductive groups.

On the contrary, systems in Examples 4-5 after reduction **no longer** define reductive group.

Thus, reductive $\mathbb{Q}$-groups in Examples 1-3 can be described by polynomial systems with coefficients in $\mathbb{Z}$ (or valuation ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$) such that their reductions modulo p still define reductive groups.

On the contrary, systems in Examples 4-5 after reduction **no longer** define reductive group.

In analogy with curves, we say that a reductive $\mathbb{Q}$-group G has good reduction at p

Thus, reductive $\mathbb{Q}$-groups in Examples 1-3 can be described by polynomial systems with coefficients in $\mathbb{Z}$ (or valuation ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$) such that their reductions modulo p still define reductive groups.

On the contrary, systems in Examples 4-5 after reduction **no longer** define reductive group.

In analogy with curves, we say that a reductive $\mathbb{Q}$-group G has good reduction at p if it can be defined by a system of equations with coefficients in $\mathbb{Z}_{(p)}$ such that reduced modulo p system defines reductive group;

Thus, reductive $\mathbb{Q}$-groups in Examples 1-3 can be described by polynomial systems with coefficients in $\mathbb{Z}$ (or valuation ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$) such that their reductions modulo p still define reductive groups.

On the contrary, systems in Examples 4-5 after reduction **no longer** define reductive group.

In analogy with curves, we say that a reductive $\mathbb{Q}$-group G has good reduction at p if it can be defined by a system of equations with coefficients in $\mathbb{Z}_{(p)}$ such that reduced modulo p system defines reductive group; otherwise, it has bad reduction.

(Note that choice of a system over $\mathbb{Z}_{(p)}$ defining G amounts to finding a group scheme over $\mathbb{Z}_{(p)}$ with generic fiber G.)

(Note that choice of a system over $\mathbb{Z}_{(p)}$ defining G amounts to finding a group scheme over $\mathbb{Z}_{(p)}$ with generic fiber G.)

So, groups in Examples 1-3 have good reduction.

(Note that choice of a system over $\mathbb{Z}_{(p)}$ defining G amounts to finding a group scheme over $\mathbb{Z}_{(p)}$ with generic fiber G.)

So, groups in Examples 1-3 have good reduction.

One can show that group in Example 4 has bad reduction for any $p > 2$,

(Note that choice of a system over $\mathbb{Z}_{(p)}$ defining G amounts to finding a group scheme over $\mathbb{Z}_{(p)}$ with generic fiber G.)

So, groups in Examples 1-3 have good reduction.

One can show that group in Example 4 has bad reduction for any $p > 2$, and group in Example 5 has bad reduction for all $p \equiv 3 (\mathrm{mod}\, 4)$.

(Note that choice of a system over $\mathbb{Z}_{(p)}$ defining G amounts to finding a group scheme over $\mathbb{Z}_{(p)}$ with generic fiber G.)

So, groups in Examples 1-3 have good reduction.

One can show that group in Example 4 has bad reduction for any $p > 2$, and group in Example 5 has bad reduction for all $p \equiv 3 (\mathrm{mod}\, 4)$.

(For $p \equiv 1 (\mathrm{mod}\, 4)$, group $\mathrm{SL}_{1,D}$ in Example 5 is isomorphic to SL_2, hence has good reduction,

(Note that choice of a system over $\mathbb{Z}_{(p)}$ defining G amounts to finding a group scheme over $\mathbb{Z}_{(p)}$ with generic fiber G.)

So, groups in Examples 1-3 have good reduction.

One can show that group in Example 4 has bad reduction for any $p > 2$, and group in Example 5 has bad reduction for all $p \equiv 3 (\mathrm{mod}\, 4)$.

(For $p \equiv 1 (\mathrm{mod}\, 4)$, group $\mathrm{SL}_{1,D}$ in Example 5 is isomorphic to SL_2, hence has good reduction, even though there is system defining it that has bad reduction).

Let K be a field, and v be a discrete valuation.

Let K be a field, and v be a discrete valuation.

Definition

Let K be a field, and v be a discrete valuation.

Definition

A reductive K-group G has *good reduction* at v

Let K be a field, and v be a discrete valuation.

Definition

A reductive K-group G has *good reduction* at v if there exists a reductive group scheme $\mathcal{G}$ over valuation ring $\mathcal{O}_v \subset K_v$ such that

Let K be a field, and v be a discrete valuation.

Definition

A reductive K-group G has *good reduction* at v if there exists a reductive group scheme $\mathcal{G}$ over valuation ring $\mathcal{O}_v \subset K_v$ such that

$$\textit{generic fiber } \mathcal{G} \otimes_{\mathcal{O}_v} K_v \text{ is isomorphic to } G \otimes_K K_v.$$

Let K be a field, and v be a discrete valuation.

Definition

A reductive K-group G has *good reduction* at v if there exists a reductive group scheme $\mathcal{G}$ over valuation ring $\mathcal{O}_v \subset K_v$ such that

$$\textit{generic fiber } \mathcal{G} \otimes_{\mathcal{O}_v} K_v \text{ is isomorphic to } G \otimes_K K_v.$$

Then *special fiber* (reduction)

$$\underline{G}^{(v)} = \mathcal{G} \otimes_{\mathcal{O}_v} K^{(v)}$$

is *a connected reductive* group ($K^{(v)}$ residue field)

Examples.

Examples.

0. If G is K-split then G has a good reduction at any v,

Examples.

0. If G is K-split then G has a good reduction at any v, given by Chevalley construction.

Examples.

0. If G is K-split then G has a good reduction at any v, given by Chevalley construction.

1. For a central simple K-algebra A, group $G = \mathrm{SL}_{1,A}$ has good reduction at v if there exists an Azumaya algebra $\mathcal{A}$ over $\mathcal{O}_v$ such that

$$A \otimes_K K_v \simeq \mathcal{A} \otimes_{\mathcal{O}_v} K_v$$

(in other words, A is *unramified* at v).

Examples.

0. If G is K-split then G has a good reduction at any v, given by Chevalley construction.

1. For a central simple K-algebra A, group $G = \mathrm{SL}_{1,A}$ has good reduction at v if there exists an Azumaya algebra $\mathcal{A}$ over $\mathcal{O}_v$ such that
$$A \otimes_K K_v \simeq \mathcal{A} \otimes_{\mathcal{O}_v} K_v$$
(in other words, A is *unramified* at v).

2. $G = \mathrm{Spin}_n(q)$ has good reduction at v if
$$q \sim \lambda(a_1 x_1^2 + \cdots + a_n x_n^2) \quad \text{with} \quad \lambda \in K_v^\times, \ a_i \in \mathcal{O}_v^\times$$
(assuming that $\mathrm{char}\, K^{(v)} \neq 2$).

Suppose K is equipped with a set V of discrete valuations.

Suppose K is equipped with a set V of discrete valuations.

We are interested in reductive K-groups of *same type* that have good reduction at all $v \in V$.

Suppose K is equipped with a set V of discrete valuations.

We are interested in reductive K-groups of *same type* that have good reduction at all $v \in V$.

To make requirement of "having same type" precise, we give

Suppose K is equipped with a set V of discrete valuations.

We are interested in reductive K-groups of *same type* that have good reduction at all $v \in V$.

To make requirement of "having same type" precise, we give

Definition

A K-group G' is a *K-form* (or $\overline{K}/K$-form) of G if

$$G' \otimes_K \overline{K} \simeq G \otimes_K \overline{K}.$$

Examples.

Examples.

1. If A is a central simple algebra of degree n over K, **then** $G' = \mathrm{SL}_{1,A}$ is a K-form of $G = \mathrm{SL}_n$.

Examples.

1. If A is a central simple algebra of degree n over K, **then** $G' = \mathrm{SL}_{1,A}$ is a K-form of $G = \mathrm{SL}_n$.

2. If q is a nondegenerate quadratic form in n variables over K ($\mathrm{char}\, K \neq 2$) and

$$G = \mathrm{Spin}_n(q),$$

Examples.

1. If A is a central simple algebra of degree n over K, **then** $G' = \mathrm{SL}_{1,A}$ is a K-form of $G = \mathrm{SL}_n$.

2. If q is a nondegenerate quadratic form in n variables over K ($\mathrm{char}\, K \neq 2$) and

$$G = \mathrm{Spin}_n(q),$$

then for any other nondegenerate quadratic form q' in n variables,

$$G' = \mathrm{Spin}_n(q')$$

is a K-form of G.

Examples.

1. If A is a central simple algebra of degree n over K, **then** $G' = \mathrm{SL}_{1,A}$ is a K-form of $G = \mathrm{SL}_n$.

2. If q is a nondegenerate quadratic form in n variables over K ($\mathrm{char}\, K \neq 2$) and

$$G = \mathrm{Spin}_n(q),$$

then for any other nondegenerate quadratic form q' in n variables,

$$G' = \mathrm{Spin}_n(q')$$

is a K-form of G.

If n is *odd* then these are **all** K-forms.

Examples.

1. If A is a central simple algebra of degree n over K, **then** $G' = \mathrm{SL}_{1,A}$ is a K-form of $G = \mathrm{SL}_n$.

2. If q is a nondegenerate quadratic form in n variables over K ($\mathrm{char}\, K \neq 2$) and

$$G = \mathrm{Spin}_n(q),$$

then for any other nondegenerate quadratic form q' in n variables,

$$G' = \mathrm{Spin}_n(q')$$

is a K-form of G.

If n is *odd* then these are **all** K-forms.

Otherwise, there may be K-forms coming from hermitian forms over noncommutative division algebras.

So, our main question becomes:

So, our main question becomes:

Given a reductive K-group G, find all (inner) forms of G that have good reduction at all $v \in V$.

So, our main question becomes:

Given a reductive K-group G, find all (inner) forms of G that have good reduction at all $v \in V$.

To make this question meaningful, one needs to specialize

K, V and G.

So, our main question becomes:

Given a reductive K-group G, find all (inner) forms of G that have good reduction at all $v \in V$.

To make this question meaningful, one needs to specialize

$$K, \ V \ \text{and} \ G.$$

Most popular case: K field of fractions of Dedekind ring R, and V consists of places associated with maximal ideals of R.

Inventiones math. 4, 165–191 (1967)

Halbeinfache Gruppenschemata über Dedekindringen

GÜNTER HARDER (Heidelberg)

Einleitung

Sei A ein Dedekindring ([4], S. 22), sei $S=\mathrm{Spec}(A)$. Mit K wollen wir den Quotientenkörper von A bezeichnen, und wir setzen $s=\mathrm{Spec}(K)$. Sei ferner $i\colon s\hookrightarrow S$ die natürliche Inklusion. Sei G ein halbeinfaches Gruppenschema über S (s. [6], S. 382), wir wollen dafür G/S oder auch G/A schreiben. Mit G_s bezeichnen wir die „allgemeine Faser" von G, d. h.

$$G_s=G\underset{S}{\times}s\,.$$

Mit anderen Worten, G_s ist die Konstantenerweiterung von G/A mit K, wir wollen daher auch G_K für G_s schreiben. Wir nennen das halbeinfache Gruppenschema G/A *rational quasitrivial*, wenn G_K eine Boreluntergruppe über K besitzt (s. [6], S. 392), es heiße *rational trivial*, wenn G_K ein Chevalleyschema über K ist (s. [6], S. 408). Ein Ziel dieser Arbeit ist, Strukturaussagen über solche Gruppenschemata zu gewinnen und sie zu klassifizieren.

Später wollen wir dann die Voraussetzung machen, daß K ein algebraischer Zahlkörper ist und A der affine Ring einer offenen Teilmenge $U\subset\mathrm{Spec}(A_0)$, wobei A_0 der Ring der ganzen Zahlen von K ist.

In diesem Fall können wir dann die Voraussetzung, daß G/A rational quasitrivial ist, durch eine wesentlich schwächere Voraussetzung ersetzen. Da wir aber vom Hasseprinzip für $H^1(K, G)$ Gebrauch machen müssen, werden wir den Fall, daß G Faktoren vom Typ E_8 enthält, ausschließen müssen.

In beiden Fällen wird der starke Approximationssatz (KNESER [15, 16]) eine entscheidende Rolle spielen. Einige unserer Hauptresultate erweisen sich als im wesentlichen äquivalent mit der Berechnung von Klassenzahlen, die KNESER in [15] auf Grund des starken Approximationssatzes andeutungsweise durchführt. Die Verbindung zwischen unserem Problem und dem der Bestimmung der Klassenzahl wird durch Satz 2.3.1 gegeben.

Wir werden uns in hohem Maße auf das Séminaire géometrie algébrique 1963/64 von GROTHENDIECK und DEMAZURE stützen (zitiert SGAD) und auch die dort entwickelte Terminologie ausgiebig verwenden. In der Thèse von DEMAZURE (zitiert TD) sind die für uns wesentlichen Begriffe

Inventiones math. 4, 165–191 (1967)

Halbeinfache Gruppenschemata über Dedekindringen

GÜNTER HARDER (Heidelberg)

Einleitung

Sei A ein Dedekindring ([4], S. 22), sei $S=\mathrm{Spec}(A)$. Mit K wollen wir den Quotientenkörper von A bezeichnen, und wir setzen $s=\mathrm{Spec}(K)$. Sei ferner $i\colon s\hookrightarrow S$ die natürliche Inklusion. Sei G ein halbeinfaches Gruppenschema über S (s. [6], S. 382), wir wollen dafür G/S oder auch G/A schreiben. Mit G_s bezeichnen wir die „allgemeine Faser" von G, d.h.

$$G_s=G\underset{S}{\times}s\,.$$

Mit anderen Worten, G_s ist die Konstantenerweiterung von G/A mit K, wir wollen daher auch G_K für G_s schreiben. Wir nennen das halbeinfache Gruppenschema G/A *rational quasitrivial*, wenn G_K eine Boreluntergruppe über K besitzt (s. [6], S. 392), es heiße *rational trivial*, wenn G_K ein Chevalleyschema über K ist (s. [6], S. 408). Ein Ziel dieser Arbeit ist, Strukturaussagen über solche Gruppenschemata zu gewinnen und sie zu klassifizieren.

Später wollen wir dann die Voraussetzung machen, daß K ein algebraischer Zahlkörper ist und A der affine Ring einer offenen Teilmenge $U\subset\mathrm{Spec}(A_0)$, wobei A_0 der Ring der ganzen Zahlen von K ist.

In diesem Fall können wir dann die Voraussetzung, daß G/A rational quasitrivial ist, durch eine wesentlich schwächere Voraussetzung ersetzen. Da wir aber vom Hasseprinzip für $H^1(K,G)$ Gebrauch machen müssen, werden wir den Fall, daß G Faktoren vom Typ E_8 enthält, ausschließen müssen.

In beiden Fällen wird der starke Approximationssatz (KNESER [15, 16]) eine entscheidende Rolle spielen. Einige unserer Hauptresultate erweisen sich als im wesentlichen äquivalent mit der Berechnung von Klassenzahlen, die KNESER in [15] auf Grund des starken Approximationssatzes andeutungsweise durchführt. Die Verbindung zwischen unserem Problem und dem der Bestimmung der Klassenzahl wird durch Satz 2.3.1 gegeben.

Wir werden uns in hohem Maße auf das Séminaire géometrie algébrique 1963/64 von GROTHENDIECK und DEMAZURE stützen (zitiert SGAD) und auch die dort entwickelte Terminologie ausgiebig verwenden. In der Thèse von DEMAZURE (zitiert TD) sind die für uns wesentlichen Begriffe

Lemma 4.1.3. *Sei G/A flach von endlichem Typ, sei G_K/K eine reduktive Gruppe, dann ist*

$$H^1_A(K,G)=\{\xi\mid \xi_\mathfrak{p}\in \mathrm{Im}\,H^1(\hat{A}_\mathfrak{p},G)\to H^1(\hat{K}_\mathfrak{p},G)\text{ für alle }\mathfrak{p}\in\mathrm{Spec}(A)\}.$$

Beweis. Es ist klar, daß die linke Seite in der rechten Seite enthalten ist. Sei $\xi\in H^1(K,G)$, und für alle $\mathfrak{p}$ sei

$$\xi_\mathfrak{p}\in\mathrm{Im}\big(H^1(\hat{A}_\mathfrak{p},G)\to H^1(\hat{K}_\mathfrak{p},G)\big).$$

Es gibt eine endliche Erweiterung K'/K, so daß $\xi\in H^1(K'/K,G)$. Wir können wegen der Sätze in § 2 die Erweiterung K' so groß wählen, daß für

$$G\underset{A}{\times}A'$$

der schwache Approximationssatz gilt. (Man wähle K' so groß, daß das Radikal R von G über K' auflösbar wird und G/R zerfällt.) Wir betrachten das Diagramm

$$1\longrightarrow G(K)\xrightarrow{q_0}G(K')\underset{q_2}{\overset{q_1}{\rightrightarrows}}G\big(K'\underset{K}{\otimes}K'\big)$$

und repräsentieren ξ durch einen Kozyklus

$$a\in G\big(K'\underset{K}{\otimes}K'\big).$$

Ist $U\subset\mathrm{Spec}(A)$ offen, so sei $A'(U)$ der Abschluß von $A(U)$ in K'. Es gibt jetzt sicher eine offene, nicht leere Menge $U_1\subset\mathrm{Spec}(A)$, so daß a im Bild der Abbildung

$$j_1\colon\ G\big(A'(U_1)\underset{A(U_1)}{\otimes}A'(U_1)\big)\to G\big(K'\underset{K}{\otimes}K'\big)$$

liegt, also ist $a=j_1(a_1)$, und weil G/A flach ist, ergibt sich, daß a_1 ein Kozyklus ist. Sei S die Menge der abgeschlossenen Primideale von A, die nicht in U_1 liegen, für jedes $\mathfrak{p}\in S$ gibt es nach Voraussetzung über ξ ein Element $b_\mathfrak{p}\in G'(\hat{K}_\mathfrak{p})$, so daß

$$a_\mathfrak{p}=p_1(b_\mathfrak{p})\cdot a\cdot p_2(b_\mathfrak{p})^{-1}\in\mathrm{Im}\big(G(\hat{A}'_\mathfrak{p}\underset{\hat{A}_\mathfrak{p}}{\otimes}\hat{A}'_\mathfrak{p})\to G(\hat{K}'_\mathfrak{p}\underset{\hat{K}_\mathfrak{p}}{\otimes}\hat{K}'_\mathfrak{p})\big).$$

Dafür muß man eventuell K' ein wenig größer machen, und es ist

$$\hat{A}'_\mathfrak{p}=\hat{A}_\mathfrak{p}\underset{A_\mathfrak{p}}{\otimes}A',$$

entsprechend ist $\hat{K}'_\mathfrak{p}$ definiert.

Nun gibt es wegen der Wahl von K' ein Element $b\in G(K')$, das an den endlich vielen Stellen $\mathfrak{p}\in S$ sehr dicht bei $b_\mathfrak{p}$ liegt, wir setzen

$$a'=p_1(b)\cdot a\cdot p_2(b)^{-1}.$$

Basic case $R = \mathbb{Z}$:

B.H. Gross (Invent. math. **124**(1996), 263-279) and B. Conrad.

Basic case $R = \mathbb{Z}$:

B.H. Gross (Invent. math. **124**(1996), 263-279) and B. Conrad.

Theorem (Gross)

Let G be an absolutely almost simple simply connected algebraic group over $\mathbb{Q}$. **Then** *G has good reduction at all primes p if and only if G is split over all $\mathbb{Q}_p$.*

Basic case $R = \mathbb{Z}$:

B.H. Gross (Invent. math. **124**(1996), 263-279) and B. Conrad.

Theorem (Gross)

Let G be an absolutely almost simple simply connected algebraic group over $\mathbb{Q}$. **Then** *G has good reduction at all primes p if and only if G is split over all $\mathbb{Q}_p$.*

Then *nonsplit* groups with good reduction can be constructed explicitly and in some cases even classified.

Basic case $R = \mathbb{Z}$:

B.H. Gross (Invent. math. **124**(1996), 263-279) and B. Conrad.

Theorem (Gross)

Let G be an absolutely almost simple simply connected algebraic group over $\mathbb{Q}$. **Then** *G has good reduction at all primes p if and only if G is split over all $\mathbb{Q}_p$.*

Then *nonsplit* groups with good reduction can be constructed explicitly and in some cases even classified.

Proposition

Let G be an absolutely almost simple simply connected algebraic group over a number field K, and assume that V contains almost all places of K. **Then** *the number of K-forms of G that have good reduction at all $v \in V$ is finite.*

Case $R = k[x], \quad K = k(x), \quad$ and

$$V \;=\; \{\, v_{p(x)} \;\mid\; p(x) \in k[x] \quad \text{irreducible} \,\}.$$

Case $R = k[x]$, $K = k(x)$, and

$$V = \{ v_{p(x)} \mid p(x) \in k[x] \text{ irreducible} \}.$$

Theorem (Raghunathan–Ramanathan, 1984)

Let k be a field of characteristic zero, and let G_0 be a connected reductive group over k. If G' is a K-form of $G_0 \otimes_k K$ that has good reduction at all $v \in V$ then

$$G' = G'_0 \otimes_k K$$

for some k-form G'_0 of G_0.

Case $R = k[x, x^{-1}]$, $K = k(x)$, and

$$V = \{ v_{p(x)} \mid p(x) \in k[x] \text{ irreducible}, \neq x \}.$$

Case $R = k[x, x^{-1}]$, $K = k(x)$, and

$$V = \{ v_{p(x)} \mid p(x) \in k[x] \text{ irreducible}, \neq x \}.$$

Theorem (Chernousov–Gille–Pianzola, 2012)

Let k be a field of characteristic zero, and let G_0 be a connected reductive group over k. **Then** *K-forms of $G_0 \otimes_k K$ that have good reduction at all $v \in V$ are in bijection with $H^1(k((x)), G_0)$.*

Case $R = k[x, x^{-1}]$, $K = k(x)$, and

$$V = \{ v_{p(x)} \mid p(x) \in k[x] \text{ irreducible}, \neq x \}.$$

Theorem (Chernousov–Gille–Pianzola, 2012)

Let k be a field of characteristic zero, and let G_0 be a connected reductive group over k. **Then** *K-forms of $G_0 \otimes_k K$ that have good reduction at all $v \in V$ are in bijection with $H^1(k((x)), G_0)$.*

This was used to prove conjugacy of Cartan subalgebras in some infinite-dimensional Lie algebras.

We analyze higher-dimensional situation.

We analyze higher-dimensional situation.

- Let K be a finitely generated field.
- Pick a model $X = \operatorname{Spec} A$ for K where A is a nice (regular, ...) finitely generated $\mathbb{Z}$-algebra.
- Let V be set of places associated with prime divisors on X (*divisorial* set).

We analyze higher-dimensional situation.

- Let K be a finitely generated field.
- Pick a model $X = \operatorname{Spec} A$ for K where A is a nice (regular, ...) finitely generated $\mathbb{Z}$-algebra.
- Let V be set of places associated with prime divisors on X (*divisorial* set).

We analyze higher-dimensional situation.

- Let K be a finitely generated field.
- Pick a model $X = \operatorname{Spec} A$ for K where A is a nice (regular, ...) finitely generated $\mathbb{Z}$-algebra.
- Let V be set of places associated with prime divisors on X (*divisorial* set).

We analyze higher-dimensional situation.

- Let K be a finitely generated field.
- Pick a model $X = \operatorname{Spec} A$ for K where A is a nice (regular, ...) finitely generated $\mathbb{Z}$-algebra.
- Let V be set of places associated with prime divisors on X (*divisorial* set).

We analyze higher-dimensional situation.

- Let K be a finitely generated field.
- Pick a model $X = \operatorname{Spec} A$ for K where A is a nice (regular, ...) finitely generated $\mathbb{Z}$-algebra.
- Let V be set of places associated with prime divisors on X (*divisorial* set).

This situation arises when one tries to understand simple groups having same isomorphism classes of maximal tori.

We analyze higher-dimensional situation.

- Let K be a finitely generated field.
- Pick a model $X = \operatorname{Spec} A$ for K where A is a nice (regular, ...) finitely generated $\mathbb{Z}$-algebra.
- Let V be set of places associated with prime divisors on X (*divisorial* set).

This situation arises when one tries to understand simple groups having same isomorphism classes of maximal tori.

Prasad and I observed that such problems are relevant for analysis of length-commensurable and isospectral locally symmetric spaces.

We analyze higher-dimensional situation.

- Let K be a finitely generated field.
- Pick a model $X = \operatorname{Spec} A$ for K where A is a nice (regular, ...) finitely generated $\mathbb{Z}$-algebra.
- Let V be set of places associated with prime divisors on X (*divisorial* set).

This situation arises when one tries to understand simple groups having same isomorphism classes of maximal tori.

Prasad and I observed that such problems are relevant for analysis of length-commensurable and isospectral locally symmetric spaces.

Using results over number fields, we showed that

We analyze higher-dimensional situation.

- Let K be a finitely generated field.
- Pick a model $X = \operatorname{Spec} A$ for K where A is a nice (regular, ...) finitely generated $\mathbb{Z}$-algebra.
- Let V be set of places associated with prime divisors on X (*divisorial* set).

This situation arises when one tries to understand simple groups having same isomorphism classes of maximal tori.

Prasad and I observed that such problems are relevant for analysis of length-commensurable and isospectral locally symmetric spaces.

Using results over number fields, we showed that *in certain situations isospectral locally symmetric spaces are commensurable*
(Publ. math. IHES **109**(2009), 113-184)

Consider the following question:

Consider the following question:

$(*)$ *Let* D_1 *and* D_2 *be finite-dimensional central division algebras over a field* K*. How are* D_1 *and* D_2 *related* **if** *they have same maximal subfields?*

Consider the following question:

(∗) *Let D_1 and D_2 be finite-dimensional central division algebras over a field K. How are D_1 and D_2 related* **if** *they have same maximal subfields?*

- D_1 and D_2 have same maximal subfields **if**
  - $\deg D_1 = \deg D_2 =: n$;
  - for P/K of degree n, $P \hookrightarrow D_1 \Leftrightarrow P \hookrightarrow D_2$.

Consider the following question:

(∗) *Let D_1 and D_2 be finite-dimensional central division algebras over a field K. How are D_1 and D_2 related* **if** *they have same maximal subfields?*

- D_1 and D_2 have same maximal subfields **if**
  - $\deg D_1 = \deg D_2 =: n$;
  - for P/K of degree n, $P \hookrightarrow D_1 \Leftrightarrow P \hookrightarrow D_2$.

Consider the following question:

(∗) *Let D_1 and D_2 be finite-dimensional central division algebras over a field K. How are D_1 and D_2 related* **if** *they have same maximal subfields?*

- D_1 and D_2 have same maximal subfields **if**
  - $\deg D_1 = \deg D_2 =: n$;
  - for P/K of degree n, $P \hookrightarrow D_1 \Leftrightarrow P \hookrightarrow D_2$.

Geometry

Prasad-A.R.: *In many (although not all) situations, two arithmetically defined locally symmetric spaces having same lengths of closed geodesics are commensurable.*

Geometry

Prasad-A.R.: *In many (although not all) situations, two arithmetically defined locally symmetric spaces having same lengths of closed geodesics are commensurable.*

Arithmetic Riemann surfaces were considered by A. Reid.

Geometry

Prasad-A.R.: *In many (although not all) situations, two arithmetically defined locally symmetric spaces having same lengths of closed geodesics are commensurable.*

Arithmetic Riemann surfaces were considered by A. Reid.

Underlying algebraic fact:

Let D_1 and D_2 be two quaternion division algebras over a number field K. **If** *D_1 and D_2 have same maximal subfields* **then** $D_1 \simeq D_2$.

However, most Riemann surfaces are not arithmetic

However, most Riemann surfaces are not arithmetic $\Rightarrow$

One needs to understand to what degree this fact extends to more general fields

However, most Riemann surfaces are not arithmetic $\Rightarrow$

One needs to understand to what degree this fact extends to more general fields

- Let $\mathbb{H} = \{ x + iy \mid y > 0 \}$.

However, most Riemann surfaces are not arithmetic $\Rightarrow$

One needs to understand to what degree this fact extends to more general fields

- Let $\mathbb{H} = \{ x + iy \mid y > 0 \}$.

"Most" Riemann surfaces are of the form:

However, most Riemann surfaces are not arithmetic $\Rightarrow$

One needs to understand to what degree this fact extends to more general fields

- Let $\mathbb{H} = \{ x + iy \mid y > 0 \}$.

"Most" Riemann surfaces are of the form:

$$M = \mathbb{H}/\Gamma$$

where $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ is a *discrete torsion free subgroup*.

However, most Riemann surfaces are not arithmetic $\Rightarrow$

One needs to understand to what degree this fact extends to more general fields

- Let $\mathbb{H} = \{ x + iy \mid y > 0 \}$.

"Most" Riemann surfaces are of the form:

$$M = \mathbb{H}/\Gamma$$

where $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ is a *discrete torsion free subgroup*.

- Some properties of M can be understood in terms of the *associated quaternion algebra.*

Let

- $\pi : \mathrm{SL}_2(\mathbb{R}) \to \mathrm{PSL}_2(\mathbb{R})$;

Let

- $\pi : \mathrm{SL}_2(\mathbb{R}) \to \mathrm{PSL}_2(\mathbb{R})$;
- $\tilde{\Gamma} = \pi^{-1}(\Gamma) \subset \mathrm{M}_2(\mathbb{R})$.

Let

- $\pi : \mathrm{SL}_2(\mathbb{R}) \to \mathrm{PSL}_2(\mathbb{R})$;
- $\tilde{\Gamma} = \pi^{-1}(\Gamma) \subset \mathrm{M}_2(\mathbb{R})$.

Set $A_\Gamma = \mathbb{Q}[\tilde{\Gamma}^{(2)}]$, $\tilde{\Gamma}^{(2)} \subset \tilde{\Gamma}$ generated by squares.

Let

- $\pi : \mathrm{SL}_2(\mathbb{R}) \to \mathrm{PSL}_2(\mathbb{R})$;
- $\tilde{\Gamma} = \pi^{-1}(\Gamma) \subset \mathrm{M}_2(\mathbb{R})$.

Set $A_\Gamma = \mathbb{Q}[\tilde{\Gamma}^{(2)}]$, $\tilde{\Gamma}^{(2)} \subset \tilde{\Gamma}$ generated by squares.

One shows: A_Γ is a *quaternion algebra* with center

$$K_\Gamma = \mathbb{Q}(\operatorname{tr}\gamma \mid \gamma \in \Gamma^{(2)})$$

(trace field).

Let

- $\pi : \mathrm{SL}_2(\mathbb{R}) \to \mathrm{PSL}_2(\mathbb{R})$;
- $\tilde{\Gamma} = \pi^{-1}(\Gamma) \subset \mathrm{M}_2(\mathbb{R})$.

Set $A_\Gamma = \mathbb{Q}[\tilde{\Gamma}^{(2)}]$, $\tilde{\Gamma}^{(2)} \subset \tilde{\Gamma}$ generated by squares.

One shows: A_Γ is a *quaternion algebra* with center

$$K_\Gamma = \mathbb{Q}(\operatorname{tr}\gamma \mid \gamma \in \Gamma^{(2)})$$

(trace field).

(**Note** that for general Fuchsian groups, K_Γ is not necessarily a number field.)

- **If** Γ is *arithmetic*, **then** A_Γ is the quaternion algebra involved in its description;

- **If** Γ is *arithmetic*, **then** A_Γ is the quaternion algebra involved in its description;

- In general, A_Γ **does not** determine Γ, **but** is an invariant of the commensurability class of Γ.

- **If** Γ is *arithmetic*, **then** A_Γ is the quaternion algebra involved in its description;
- In general, A_Γ **does not** determine Γ, **but** is an invariant of the commensurability class of Γ.

To a (nontrivial) semi-simple $\gamma \in \tilde{\Gamma}^{(2)}$ there corresponds:

- **If** Γ is *arithmetic*, **then** A_Γ is the quaternion algebra involved in its description;

- In general, A_Γ **does not** determine Γ, **but** is an invariant of the commensurability class of Γ.

To a (nontrivial) semi-simple $\gamma \in \tilde{\Gamma}^{(2)}$ there corresponds:

- *geometrically*: a closed geodesic $c_\gamma \subset M$,
  if $\gamma \sim \pm \begin{pmatrix} t_\gamma & 0 \\ 0 & t_\gamma^{-1} \end{pmatrix}$ $(t_\gamma > 1)$ then *length* $\ell(c_\gamma) = 2 \log t_\gamma$;

- **If** Γ is *arithmetic*, **then** A_Γ is the quaternion algebra involved in its description;

- In general, A_Γ **does not** determine Γ, **but** is an invariant of the commensurability class of Γ.

To a (nontrivial) semi-simple $\gamma \in \tilde{\Gamma}^{(2)}$ there corresponds:

- *geometrically*: a closed geodesic $c_\gamma \subset M$,
  if $\gamma \sim \pm \begin{pmatrix} t_\gamma & 0 \\ 0 & t_\gamma^{-1} \end{pmatrix}$ $(t_\gamma > 1)$ then *length* $\ell(c_\gamma) = 2 \log t_\gamma$;

- *algebraically*: a maximal etale subalgebra $K_\Gamma[\gamma] \subset A_\Gamma$.

For a Riemannian manifold M:

$L(M)$ = set of lengths of closed geodesics in M

((weak) length spectrum of M)

For a Riemannian manifold M:

$L(M)$ = set of lengths of closed geodesics in M

((weak) length spectrum of M)

Definition.

Riemannian manifolds M_1 and M_2 are

For a Riemannian manifold M:

$L(M)$ = set of lengths of closed geodesics in M

((weak) length spectrum of M)

Definition.

Riemannian manifolds M_1 and M_2 are

- *iso-length spectral* if $L(M_1) = L(M_2)$;

For a Riemannian manifold M:

$L(M)$ = set of lengths of closed geodesics in M

((weak) length spectrum of M)

Definition.

Riemannian manifolds M_1 and M_2 are

- *iso-length spectral* if $L(M_1) = L(M_2)$;
- *length-commensurable* if $\mathbb{Q} \cdot L(M_1) = \mathbb{Q} \cdot L(M_2)$.

Let $M_i = \mathbb{H}/\Gamma_i \, (i = 1, 2)$ be Riemann surfaces.

Let $M_i = \mathbb{H}/\Gamma_i \, (i = 1, 2)$ be Riemann surfaces.

If M_1 and M_2 are length-commensurable **then:**

Let $M_i = \mathbb{H}/\Gamma_i \ (i = 1,2)$ be Riemann surfaces.

If M_1 and M_2 are length-commensurable **then:**

1. $K_{\Gamma_1} = K_{\Gamma_2} =: K$;
2. Given closed geodesics $c_{\gamma_i} \subset M_i$ for $i = 1,2$ such that
$$\ell(c_{\gamma_2})/\ell(c_{\gamma_1}) = m/n \quad (m,n \in \mathbb{Z})$$
elements γ_1^m and γ_2^n are conjugate $\Rightarrow$

Let $M_i = \mathbb{H}/\Gamma_i$ $(i = 1,2)$ be Riemann surfaces.

If M_1 and M_2 are length-commensurable **then:**

1. $K_{\Gamma_1} = K_{\Gamma_2} =: K$;
2. Given closed geodesics $c_{\gamma_i} \subset M_i$ for $i = 1,2$ such that
$$\ell(c_{\gamma_2})/\ell(c_{\gamma_1}) = m/n \quad (m,n \in \mathbb{Z})$$
elements γ_1^m and γ_2^n are conjugate $\Rightarrow$

Let $M_i = \mathbb{H}/\Gamma_i \ (i = 1, 2)$ be Riemann surfaces.

If M_1 and M_2 are length-commensurable **then:**

1. $K_{\Gamma_1} = K_{\Gamma_2} =: K$;
2. Given closed geodesics $c_{\gamma_i} \subset M_i$ for $i = 1, 2$ such that
$$\ell(c_{\gamma_2})/\ell(c_{\gamma_1}) = m/n \quad (m, n \in \mathbb{Z})$$
elements γ_1^m and γ_2^n are conjugate $\Rightarrow$

Let $M_i = \mathbb{H}/\Gamma_i$ $(i = 1, 2)$ be Riemann surfaces.

If M_1 and M_2 are length-commensurable **then:**

1. $K_{\Gamma_1} = K_{\Gamma_2} =: K$;
2. Given closed geodesics $c_{\gamma_i} \subset M_i$ for $i = 1, 2$ such that
$$\ell(c_{\gamma_2})/\ell(c_{\gamma_1}) = m/n \quad (m, n \in \mathbb{Z})$$
elements γ_1^m and γ_2^n are conjugate $\Rightarrow$
$K[\gamma_1] \subset A_{\Gamma_1}$ and $K[\gamma_2] \subset A_{\Gamma_2}$ are isomorphic.

Let $M_i = \mathbb{H}/\Gamma_i$ $(i = 1, 2)$ be Riemann surfaces.

If M_1 and M_2 are length-commensurable **then:**

1. $K_{\Gamma_1} = K_{\Gamma_2} =: K$;
2. Given closed geodesics $c_{\gamma_i} \subset M_i$ for $i = 1, 2$ such that
$$\ell(c_{\gamma_2})/\ell(c_{\gamma_1}) = m/n \quad (m, n \in \mathbb{Z})$$
elements γ_1^m and γ_2^n are conjugate $\Rightarrow$
$K[\gamma_1] \subset A_{\Gamma_1}$ and $K[\gamma_2] \subset A_{\Gamma_2}$ are isomorphic.

So, A_{Γ_1} and A_{Γ_2} share "lots" of maximal etale subalgebras.

Let $M_i = \mathbb{H}/\Gamma_i$ $(i = 1, 2)$ be Riemann surfaces.

If M_1 and M_2 are length-commensurable **then:**

1. $K_{\Gamma_1} = K_{\Gamma_2} =: K$;
2. Given closed geodesics $c_{\gamma_i} \subset M_i$ for $i = 1, 2$ such that
$$\ell(c_{\gamma_2})/\ell(c_{\gamma_1}) = m/n \quad (m, n \in \mathbb{Z})$$
elements γ_1^m and γ_2^n are conjugate $\Rightarrow$
$K[\gamma_1] \subset A_{\Gamma_1}$ and $K[\gamma_2] \subset A_{\Gamma_2}$ are isomorphic.

So, A_{Γ_1} and A_{Γ_2} share "lots" of maximal etale subalgebras.

(Not all – but we will ignore it for now ...)

- For M_1 and M_2 to be commensurable, A_{Γ_1} and A_{Γ_2} must be isomorphic.

- For M_1 and M_2 to be commensurable, A_{Γ_1} and A_{Γ_2} must be isomorphic.

So, proving that length-commensurable M_1 and M_2 are commensurable implicitly involves answering a version of $(*)$.

- For M_1 and M_2 to be commensurable, A_{Γ_1} and A_{Γ_2} must be isomorphic.

So, proving that length-commensurable M_1 and M_2 are commensurable implicitly involves answering a version of $(*)$.

- **Recall:** If $M = \mathbb{H}/\Gamma$ is a compact Riemann surface then compact Riemann surfaces *isospectral* to M split into finitely many isometry classes.

• For M_1 and M_2 to be commensurable, A_{Γ_1} and A_{Γ_2} must be isomorphic.

So, proving that length-commensurable M_1 and M_2 are commensurable implicitly involves answering a version of $(*)$.

• **Recall:** If $M = \mathbb{H}/\Gamma$ is a compact Riemann surface then compact Riemann surfaces *isospectral* to M split into finitely many isometry classes.

What about *length-commensurable* Riemann surfaces?

• For M_1 and M_2 to be commensurable, A_{Γ_1} and A_{Γ_2} must be isomorphic.

So, proving that length-commensurable M_1 and M_2 are commensurable implicitly involves answering a version of $(*)$.

• **Recall:** If $M = \mathbb{H}/\Gamma$ is a compact Riemann surface then compact Riemann surfaces *isospectral* to M split into finitely many isometry classes.

What about *length-commensurable* Riemann surfaces?

Theorem

Let $M_i = \mathbb{H}/\Gamma_i$ $(i \in I)$ *be a family of* length-commensurable *Riemann surfaces where* $\Gamma_i \subset \mathrm{PSL}_2(\mathbb{R})$ *is finitely generated and Zariski- dense.* **Then** *quaternion algebras* A_{Γ_i} $(i \in I)$ *split into finitely many isomorphism classes (over common center).*

Algebra

Algebra

Amitsur's Theorem

Let D_1 and D_2 be central division algebras over K.

Algebra

Amitsur's Theorem

Let D_1 and D_2 be central division algebras over K.

If D_1 and D_2 have same splitting fields,

Algebra

Amitsur's Theorem

Let D_1 and D_2 be central division algebras over K.

If D_1 and D_2 have same splitting fields, i.e. for F/K we have

$$D_1 \otimes_K F \simeq M_{n_1}(F) \quad \Leftrightarrow \quad D_2 \otimes_K F \simeq M_{n_2}(F),$$

Algebra

Amitsur's Theorem

Let D_1 and D_2 be central division algebras over K.

If D_1 and D_2 have same splitting fields, i.e. for F/K we have

$$D_1 \otimes_K F \simeq M_{n_1}(F) \quad \Leftrightarrow \quad D_2 \otimes_K F \simeq M_{n_2}(F),$$

then $\langle [D_1] \rangle = \langle [D_2] \rangle$ in $\mathrm{Br}(K)$.

Algebra

Amitsur's Theorem

Let D_1 and D_2 be central division algebras over K.

If D_1 and D_2 have same splitting fields, i.e. for F/K we have

$$D_1 \otimes_K F \simeq M_{n_1}(F) \quad \Leftrightarrow \quad D_2 \otimes_K F \simeq M_{n_2}(F),$$

then $\langle [D_1] \rangle = \langle [D_2] \rangle$ in $\mathrm{Br}(K)$.

Proof of Amitsur's Theorem uses *generic splitting fields* (function fields of Severi-Brauer varieties),

Algebra

Amitsur's Theorem

Let D_1 and D_2 be central division algebras over K.

If D_1 and D_2 have same splitting fields, i.e. for F/K we have

$$D_1 \otimes_K F \simeq M_{n_1}(F) \quad \Leftrightarrow \quad D_2 \otimes_K F \simeq M_{n_2}(F),$$

then $\langle [D_1] \rangle = \langle [D_2] \rangle$ in $\mathrm{Br}(K)$.

Proof of Amitsur's Theorem uses *generic splitting fields* (function fields of Severi-Brauer varieties), which are infinite extensions of K.

Algebra

Amitsur's Theorem

Let D_1 and D_2 be central division algebras over K.

If D_1 and D_2 have same splitting fields, i.e. for F/K we have

$$D_1 \otimes_K F \simeq M_{n_1}(F) \quad \Leftrightarrow \quad D_2 \otimes_K F \simeq M_{n_2}(F),$$

then $\langle [D_1] \rangle = \langle [D_2] \rangle$ in $\mathrm{Br}(K)$.

Proof of Amitsur's Theorem uses *generic splitting fields* (function fields of Severi-Brauer varieties), which are infinite extensions of K.

What happens if one allows only splitting fields of finite degree, or just maximal subfields?

- Amitsur's Theorem is no longer true in this setting.

- Amitsur's Theorem is no longer true in this setting.

  (Counterexamples can be found using cubic algebras over number fields.)

- Amitsur's Theorem is no longer true in this setting.

  (Counterexamples can be found using cubic algebras over number fields.)

This leads to question $(*)$ and its variations.

- Amitsur's Theorem is no longer true in this setting.

  (Counterexamples can be found using cubic algebras over number fields.)

This leads to question $(*)$ and its variations.

Question (Prasad-A.R.)

Are quaternion algebras over $K = \mathbb{Q}(x)$ determined by their maximal subfields?

- Amitsur's Theorem is no longer true in this setting.

  (Counterexamples can be found using cubic algebras over number fields.)

This leads to question $(*)$ and its variations.

Question (Prasad-A.R.)

Are quaternion algebras over $K = \mathbb{Q}(x)$ determined by their maximal subfields?

- Yes – D. Saltman

- Amitsur's Theorem is no longer true in this setting.

  (Counterexamples can be found using cubic algebras over number fields.)

This leads to question $(*)$ and its variations.

Question (Prasad-A.R.)

Are quaternion algebras over $K = \mathbb{Q}(x)$ determined by their maximal subfields?

- Yes – D. Saltman
- Same over $K = k(x)$, k a number field

  (S. Garibaldi - D. Saltman)

Definition.

Let D be a finite-dimensional central division algebra over K.

Definition.

Let D be a finite-dimensional central division algebra over K. The *genus* of D is

$$\mathbf{gen}(D) = \{\, [D'] \in \mathrm{Br}(K) \mid D' \text{ has same maximal subfields as } D \,\}$$

Definition.

Let D be a finite-dimensional central division algebra over K. The *genus* of D is

$$\mathbf{gen}(D) = \{\, [D'] \in \mathrm{Br}(K) \mid D' \text{ has same maximal subfields as } D \,\}$$

Question 1. *When does* $\mathbf{gen}(D)$ *reduce to a single element?*

Definition.

Let D be a finite-dimensional central division algebra over K. The *genus* of D is

$$\mathbf{gen}(D) = \{\, [D'] \in \mathrm{Br}(K) \mid D' \text{ has same maximal subfields as } D \,\}$$

Question 1. *When does* $\mathbf{gen}(D)$ *reduce to a single element?*

(This means that D is uniquely determined by maximal subfields.)

Definition.

Let D be a finite-dimensional central division algebra over K. The *genus* of D is

$$\mathbf{gen}(D) = \{\, [D'] \in \mathrm{Br}(K) \mid D' \text{ has same maximal subfields as } D \,\}$$

Question 1. *When does* $\mathbf{gen}(D)$ *reduce to a single element?*

(This means that D is uniquely determined by maximal subfields.)

Question 2. *When is* $\mathbf{gen}(D)$ *finite?*

Definition.

Let D be a finite-dimensional central division algebra over K. The *genus* of D is

$$\mathbf{gen}(D) = \{\, [D'] \in \mathrm{Br}(K) \mid D' \text{ has same maximal subfields as } D \,\}$$

Question 1. *When does* $\mathbf{gen}(D)$ *reduce to a single element?*

(This means that D is uniquely determined by maximal subfields.)

Question 2. *When is* $\mathbf{gen}(D)$ *finite?*

Over number fields:

Definition.

Let D be a finite-dimensional central division algebra over K. The *genus* of D is

$$\mathbf{gen}(D) = \{\, [D'] \in \mathrm{Br}(K) \mid D' \text{ has same maximal subfields as } D \,\}$$

Question 1. *When does* $\mathbf{gen}(D)$ *reduce to a single element?*

(This means that D is uniquely determined by maximal subfields.)

Question 2. *When is* $\mathbf{gen}(D)$ *finite?*

Over number fields:

- genus of every quaternion algebra reduces to one element;
- genus of every division algebra is finite.

Definition.

Let D be a finite-dimensional central division algebra over K. The *genus* of D is

$$\mathbf{gen}(D) = \{\, [D'] \in \mathrm{Br}(K) \mid D' \text{ has same maximal subfields as } D \,\}$$

Question 1. *When does* $\mathbf{gen}(D)$ *reduce to a single element?*

(This means that D is uniquely determined by maximal subfields.)

Question 2. *When is* $\mathbf{gen}(D)$ *finite?*

Over number fields:

- genus of every quaternion algebra reduces to one element;
- genus of every division algebra is finite.

Definition.

Let D be a finite-dimensional central division algebra over K. The *genus* of D is

$$\mathbf{gen}(D) = \{\, [D'] \in \mathrm{Br}(K) \mid D' \text{ has same maximal subfields as } D \,\}$$

Question 1. *When does* $\mathbf{gen}(D)$ *reduce to a single element?*

(This means that D is uniquely determined by maximal subfields.)

Question 2. *When is* $\mathbf{gen}(D)$ *finite?*

Over number fields:

- genus of every quaternion algebra reduces to one element;
- genus of every division algebra is finite.

(Follows from Albert-Hasse-Brauer-Noether Theorem.)

Theorem 1 (Stability Theorem)

Let $\operatorname{char} k \neq 2$. *If* $|\mathbf{gen}(D)| = 1$ *for every quaternion algebra* D *over* k, *then* $|\mathbf{gen}(D')| = 1$ *for any quaternion algebra* D' *over* $k(x)$.

Theorem 1 (Stability Theorem)

Let $\operatorname{char} k \neq 2$. *If* $|\mathbf{gen}(D)| = 1$ *for every quaternion algebra* D *over* k, *then* $|\mathbf{gen}(D')| = 1$ *for any quaternion algebra* D' *over* $k(x)$.

- Same statement is true for division algebras of *exponent* 2.

Theorem 1 (Stability Theorem)

Let $\operatorname{char} k \neq 2$. *If* $|\mathbf{gen}(D)| = 1$ *for every quaternion algebra* D *over* k, *then* $|\mathbf{gen}(D')| = 1$ *for any quaternion algebra* D' *over* $k(x)$.

- Same statement is true for division algebras of *exponent* 2.
- $|\mathbf{gen}(D)| > 1$ if D is not of exponent 2.

Theorem 1 (Stability Theorem)

Let $\operatorname{char} k \neq 2$. *If* $|\mathbf{gen}(D)| = 1$ *for every quaternion algebra* D *over* k, *then* $|\mathbf{gen}(D')| = 1$ *for any quaternion algebra* D' *over* $k(x)$.

- Same statement is true for division algebras of *exponent* 2.
- $|\mathbf{gen}(D)| > 1$ if D is not of exponent 2.

- $\mathbf{gen}(D)$ can be infinite.

Theorem 1 (Stability Theorem)

Let $\operatorname{char} k \neq 2$. *If* $|\mathbf{gen}(D)| = 1$ *for every quaternion algebra* D *over* k, *then* $|\mathbf{gen}(D')| = 1$ *for any quaternion algebra* D' *over* $k(x)$.

- Same statement is true for division algebras of *exponent* 2.
- $|\mathbf{gen}(D)| > 1$ if D is not of exponent 2.
- $\mathbf{gen}(D)$ can be infinite.

Construction yields examples over fields that are infinitely generated

Theorem 1 (Stability Theorem)

Let $\operatorname{char} k \neq 2$. *If* $|\mathbf{gen}(D)| = 1$ *for every quaternion algebra* D *over* k, *then* $|\mathbf{gen}(D')| = 1$ *for any quaternion algebra* D' *over* $k(x)$.

- Same statement is true for division algebras of *exponent* 2.
- $|\mathbf{gen}(D)| > 1$ if D is not of exponent 2.
- $\mathbf{gen}(D)$ can be infinite.

Construction yields examples over fields that are infinitely generated

(in fact, HUGE)

Theorem 2.

Let K be a finitely generated *field. Then for any central division K-algebra D the genus* $\mathbf{gen}(D)$ *is finite.*

Theorem 2.

Let K be a finitely generated *field. Then for any central division K-algebra D the genus* $\mathbf{gen}(D)$ *is finite.*

- Proofs of both theorems use *analysis of ramification* and info about *unramified Brauer group*.

Theorem 2.

Let K be a finitely generated *field. Then for any central division K-algebra D the genus* $\mathbf{gen}(D)$ *is finite.*

- Proofs of both theorems use *analysis of ramification* and info about *unramified Brauer group*.

BASIC FACT: *Let v be a discrete valuation of K, and n be prime to characteristic of residue field $K^{(v)}$.*

Theorem 2.

Let K be a finitely generated *field. Then for any central division K-algebra D the genus* $\mathbf{gen}(D)$ *is finite.*

- Proofs of both theorems use *analysis of ramification* and info about *unramified Brauer group*.

BASIC FACT: *Let v be a discrete valuation of K, and n be prime to characteristic of residue field $K^{(v)}$.*
If D_1 and D_2 are central division K-algebras of degree n having same maximal subfields, then either both algebras are ramified *at v or both are* unramified.

Theorem 2.

Let K be a finitely generated *field. Then for any central division K-algebra D the genus* $\mathbf{gen}(D)$ *is finite.*

- Proofs of both theorems use *analysis of ramification* and info about *unramified Brauer group*.

BASIC FACT: *Let v be a discrete valuation of K, and n be prime to characteristic of residue field $K^{(v)}$.*
If D_1 and D_2 are central division K-algebras of degree n having same maximal subfields, then either both algebras are ramified *at v or both are* unramified.

(When n is divisible by $\operatorname{char} K^{(v)}$, we need some additional assumptions)

- Recall that a c. s. a. A over K (or its class $[A] \in \mathrm{Br}(K)$) is *unramified* at v if

- Recall that a c. s. a. A over K (or its class $[A] \in \mathrm{Br}(K)$) is *unramified* at v if there exists Azumaya algebra $\mathcal{A}/\mathcal{O}_v$ such that

$$A \otimes_K K_v \simeq \mathcal{A} \otimes_{\mathcal{O}_v} K_v.$$

- Recall that a c. s. a. A over K (or its class $[A] \in \mathrm{Br}(K)$) is *unramified* at v if there exists Azumaya algebra $\mathcal{A}/\mathcal{O}_v$ such that

$$A \otimes_K K_v \simeq \mathcal{A} \otimes_{\mathcal{O}_v} K_v.$$

If $(n\,, \operatorname{char} K^{(v)}) = 1$ or $K^{(v)}$ is perfect, there is a *residue map*

$$r_v \colon {}_n\mathrm{Br}(K) \longrightarrow H^1(\mathcal{G}^{(v)}, \mathbb{Z}/n\mathbb{Z}),$$

where $\mathcal{G}^{(v)}$ is absolute Galois group of $K^{(v)}$.

- Recall that a c. s. a. A over K (or its class $[A] \in \mathrm{Br}(K)$) is *unramified* at v if there exists Azumaya algebra $\mathcal{A}/\mathcal{O}_v$ such that

$$A \otimes_K K_v \simeq \mathcal{A} \otimes_{\mathcal{O}_v} K_v.$$

If $(n\,, \operatorname{char} K^{(v)}) = 1$ or $K^{(v)}$ is perfect, there is a *residue map*

$$r_v \colon {}_n\mathrm{Br}(K) \longrightarrow H^1(\mathcal{G}^{(v)}, \mathbb{Z}/n\mathbb{Z}),$$

where $\mathcal{G}^{(v)}$ is absolute Galois group of $K^{(v)}$.

- **Then** $x \in {}_n\mathrm{Br}(K)$ is unramified at $v \Leftrightarrow r_v(x) = 0$.

- Recall that a c. s. a. A over K (or its class $[A] \in \mathrm{Br}(K)$) is *unramified* at v if there exists Azumaya algebra $\mathcal{A}/\mathcal{O}_v$ such that

$$A \otimes_K K_v \simeq \mathcal{A} \otimes_{\mathcal{O}_v} K_v.$$

If $(n\,, \operatorname{char} K^{(v)}) = 1$ or $K^{(v)}$ is perfect, there is a *residue map*

$$r_v \colon {}_n\mathrm{Br}(K) \longrightarrow H^1(\mathcal{G}^{(v)}, \mathbb{Z}/n\mathbb{Z}),$$

where $\mathcal{G}^{(v)}$ is absolute Galois group of $K^{(v)}$.

- **Then** $x \in {}_n\mathrm{Br}(K)$ is unramified at $v \Leftrightarrow r_v(x) = 0$.

Given a set V of discrete valuations of K, one defines corresponding *unramified Brauer group:*

$$\mathrm{Br}(K)_V = \{\, x \in \mathrm{Br}(K) \mid x \text{ unramified at all } v \in V \,\}.$$

- To prove Theorem 1 (Stability Theorem) we use:
  if $K = k(x)$ *and* $V =$ *set of geometric places, then*

$$ {}_n\mathrm{Br}(K)_V = {}_n\mathrm{Br}(k) $$

  when $(n, \mathrm{char}\, k) = 1$ (Faddeev)

- To prove Theorem 1 (Stability Theorem) we use:
  if $K = k(x)$ *and* $V =$ *set of geometric places, then*
  $$ {}_n\mathrm{Br}(K)_V = {}_n\mathrm{Br}(k) $$
  when $(n, \mathrm{char}\, k) = 1$ (Faddeev)

- There are **two** proofs of Theorem 2. **Both** show that a finitely generated field K can be equipped with set V of discrete valuations so that one can make some finiteness statements about unramified Brauer group.

- To prove Theorem 1 (Stability Theorem) we use:
  if $K = k(x)$ *and* $V =$ *set of geometric places, then*
  $$ {}_n\mathrm{Br}(K)_V = {}_n\mathrm{Br}(k) $$
  when $(n, \mathrm{char}\, k) = 1$ (Faddeev)

- There are **two** proofs of Theorem 2. **Both** show that a finitely generated field K can be equipped with set V of discrete valuations so that one can make some finiteness statements about unramified Brauer group.
  - More recent argument works in all characteristics, **but** gives no estimate of size of $\mathbf{gen}(D)$.
  - Earlier argument works when $(n\,,\,\mathrm{char}\, K) = 1$, gives finiteness of ${}_n\mathrm{Br}(K)_V$ and estimate
    $$ |\mathbf{gen}(D)| \leqslant |{}_n\mathrm{Br}(K)_V| \cdot \varphi(n)^r $$
    where r is number of $v \in V$ that ramify in D.

- To prove Theorem 1 (Stability Theorem) we use:
  if $K = k(x)$ *and* $V =$ *set of geometric places, then*
  $$ {}_n\mathrm{Br}(K)_V = {}_n\mathrm{Br}(k) $$
  when $(n, \mathrm{char}\, k) = 1$ (Faddeev)

- There are **two** proofs of Theorem 2. **Both** show that a finitely generated field K can be equipped with set V of discrete valuations so that one can make some finiteness statements about unramified Brauer group.

  - More recent argument works in all characteristics, **but** gives no estimate of size of $\mathbf{gen}(D)$.
  - Earlier argument works when $(n\,,\, \mathrm{char}\, K) = 1$, gives finiteness of ${}_n\mathrm{Br}(K)_V$ and estimate
    $$ |\mathbf{gen}(D)| \leqslant |{}_n\mathrm{Br}(K)_V| \cdot \varphi(n)^r $$
    where r is number of $v \in V$ that ramify in D.

- To prove Theorem 1 (Stability Theorem) we use:
  if $K = k(x)$ *and* $V =$ *set of geometric places, then*
  $$ {}_n\mathrm{Br}(K)_V = {}_n\mathrm{Br}(k) $$
  when $(n, \mathrm{char}\, k) = 1$ (Faddeev)

- There are **two** proofs of Theorem 2. **Both** show that a finitely generated field K can be equipped with set V of discrete valuations so that one can make some finiteness statements about unramified Brauer group.

  - More recent argument works in all characteristics, **but** gives no estimate of size of $\mathbf{gen}(D)$.
  - Earlier argument works when $(n\,,\,\mathrm{char}\, K) = 1$, gives finiteness of ${}_n\mathrm{Br}(K)_V$ and estimate
    $$ |\,\mathbf{gen}(D)\,| \leqslant |\,{}_n\mathrm{Br}(K)_V\,| \cdot \varphi(n)^r $$
    where r is number of $v \in V$ that ramify in D.

Question. *Does there exist a quaternion division algebra D over $K = k(C)$, where C is a smooth geometrically integral curve over a number field k, such that*

$$|\mathbf{gen}(D)| > 1?$$

Question. *Does there exist a quaternion division algebra D over $K = k(C)$, where C is a smooth geometrically integral curve over a number field k, such that*

$$|\mathbf{gen}(D)| > 1?$$

- The answer is **not** known for *any* finitely generated K.

Question. *Does there exist a quaternion division algebra D over $K = k(C)$, where C is a smooth geometrically integral curve over a number field k, such that*

$$|\mathbf{gen}(D)| > 1?$$

- The answer is **not** known for *any* finitely generated K.
- One can construct examples where ${}_2\mathrm{Br}(K)_V$ is "large."

- To define the genus of an algebraic group, we replace maximal subfields with *maximal tori* in the definition of genus of division algebra.

- To define the genus of an algebraic group, we replace maximal subfields with *maximal tori* in the definition of genus of division algebra.

Let G_1 and G_2 be semi-simple groups over a field K.

- To define the genus of an algebraic group, we replace maximal subfields with *maximal tori* in the definition of genus of division algebra.

Let G_1 and G_2 be semi-simple groups over a field K.

G_1 & G_2 have *same isomorphism classes of maximal K-tori* **if** every maximal K-torus T_1 of G_1 is K-isomorphic to a maximal K-torus T_2 of G_2, and vice versa.

- To define the genus of an algebraic group, we replace maximal subfields with *maximal tori* in the definition of genus of division algebra.

Let G_1 and G_2 be semi-simple groups over a field K.

G_1 & G_2 have *same isomorphism classes of maximal K-tori* **if** every maximal K-torus T_1 of G_1 is K-isomorphic to a maximal K-torus T_2 of G_2, and vice versa.

Let G be an absolutely almost simple K-group.

- To define the genus of an algebraic group, we replace maximal subfields with *maximal tori* in the definition of genus of division algebra.

Let G_1 and G_2 be semi-simple groups over a field K.

G_1 & G_2 have *same isomorphism classes of maximal K-tori* **if** every maximal K-torus T_1 of G_1 is K-isomorphic to a maximal K-torus T_2 of G_2, and vice versa.

Let G be an absolutely almost simple K-group.

$\mathbf{gen}_K(G) =$ set of isomorphism classes of K-forms G' of G having same K-isomorphism classes of maximal K-tori as G.

Question 1′. *When does* $\mathbf{gen}_K(G)$ *reduce to a single element?*

Question 1′. *When does* $\mathbf{gen}_K(G)$ *reduce to a single element?*

Question 2′. *When is* $\mathbf{gen}_K(G)$ *finite?*

Question 1′. *When does* $\mathbf{gen}_K(G)$ *reduce to a single element?*

Question 2′. *When is* $\mathbf{gen}_K(G)$ *finite?*

Theorem 3 (Prasad-A.R.)

Let G be an absolutely almost simple simply connected algebraic group over a number field K.

Question 1′. *When does* $\mathbf{gen}_K(G)$ *reduce to a single element?*

Question 2′. *When is* $\mathbf{gen}_K(G)$ *finite?*

Theorem 3 (Prasad-A.R.)

Let G be an absolutely almost simple simply connected algebraic group over a number field K.

(1) $\mathbf{gen}_K(G)$ *is finite;*

Question 1′. *When does* $\mathbf{gen}_K(G)$ *reduce to a single element?*

Question 2′. *When is* $\mathbf{gen}_K(G)$ *finite?*

Theorem 3 (Prasad-A.R.)

Let G be an absolutely almost simple simply connected algebraic group over a number field K.

(1) $\mathbf{gen}_K(G)$ *is finite;*

(2) *If G is not of type A_n, D_{2n+1} or E_6, then* $|\mathbf{gen}_K(G)| = 1$.

Question 1′. *When does* $\mathbf{gen}_K(G)$ *reduce to a single element?*

Question 2′. *When is* $\mathbf{gen}_K(G)$ *finite?*

Theorem 3 (Prasad-A.R.)

Let G be an absolutely almost simple simply connected algebraic group over a number field K.

(1) $\mathbf{gen}_K(G)$ *is finite;*

(2) *If G is not of type A_n, D_{2n+1} or E_6, then* $|\mathbf{gen}_K(G)| = 1$.

Conjecture. (1) *For $K = k(x)$, k a number field, and G an absolutely almost simple simply connected K-group with* $|Z(G)| \leqslant 2$, *we have* $|\mathbf{gen}_K(G)| = 1$;

Question 1′. *When does* $\mathbf{gen}_K(G)$ *reduce to a single element?*

Question 2′. *When is* $\mathbf{gen}_K(G)$ *finite?*

Theorem 3 (Prasad-A.R.)

Let G be an absolutely almost simple simply connected algebraic group over a number field K.

(1) $\mathbf{gen}_K(G)$ *is finite;*

(2) *If G is not of type A_n, D_{2n+1} or E_6, then* $|\mathbf{gen}_K(G)| = 1$.

Conjecture. (1) *For $K = k(x)$, k a number field, and G an absolutely almost simple simply connected K-group with* $|Z(G)| \leqslant 2$, *we have* $|\mathbf{gen}_K(G)| = 1$;

(2) *If G is an absolutely almost simple group over a finitely generated field K of "good" characteristic then* $\mathbf{gen}_K(G)$ *is finite.*

"Unramified division algebras" $\rightsquigarrow$ "groups with good reduction"

"Unramified division algebras" $\rightsquigarrow$ "groups with good reduction"

Theorem 3.

Let G be an absolutely almost simple simply connected group over K, and v be a discrete valuation of K.

"Unramified division algebras" $\rightsquigarrow$ "groups with good reduction"

Theorem 3.

Let G be an absolutely almost simple simply connected group over K, and v be a discrete valuation of K.

Assume that $K^{(v)}$ is finitely generated, and G has good reduction at v.

"Unramified division algebras" $\rightsquigarrow$ "groups with good reduction"

Theorem 3.

Let G be an absolutely almost simple simply connected group over K, and v be a discrete valuation of K.

Assume that $K^{(v)}$ is finitely generated, and G has good reduction at v.

Then *every* $G' \in \mathbf{gen}_K(G)$ *has good reduction at v, and reduction* $\underline{G'}^{(v)} \in \mathbf{gen}_{K^{(v)}}(\underline{G}^{(v)})$.

Let K be a finitely generated field equipped with a set V of discrete valuations such that:

(I) for any $a \in K^\times$, set $V(a) := \{v \in V \mid v(a) \neq 0\}$ is finite;

(II) for every $v \in V$, residue field $K^{(v)}$ is finitely generated.

Let K be a finitely generated field equipped with a set V of discrete valuations such that:

(I) for any $a \in K^\times$, set $V(a) := \{v \in V \mid v(a) \neq 0\}$ is finite;

(II) for every $v \in V$, residue field $K^{(v)}$ is finitely generated.

Let K be a finitely generated field equipped with a set V of discrete valuations such that:

(I) for any $a \in K^\times$, set $V(a) := \{v \in V \mid v(a) \neq 0\}$ is finite;

(II) for every $v \in V$, residue field $K^{(v)}$ is finitely generated.

Let K be a finitely generated field equipped with a set V of discrete valuations such that:

(I) for any $a \in K^\times$, set $V(a) := \{v \in V \mid v(a) \neq 0\}$ is finite;

(II) for every $v \in V$, residue field $K^{(v)}$ is finitely generated.

Corollary.

Let G be an absolutely almost simple simply connected K-group.

There exists a finite subset $S \subset V$ (depending on G) such that every $G' \in \mathbf{gen}_K(G)$ has good reduction at all $v \in V \setminus S$.

So, finiteness of $\mathbf{gen}_K(G)$ is related to following property:

So, finiteness of $\mathbf{gen}_K(G)$ is related to following property:

A set V of discrete valuations of K satisfies (Φ) for an absolutely almost simple K-group G if

So, finiteness of $\mathbf{gen}_K(G)$ is related to following property:

A set V of discrete valuations of K satisfies (Φ) for an absolutely almost simple K-group G if

(Φ) set of K-isomorphism classes of (inner) K-forms G' of G having good reduction at all $v \in V \setminus S$ is finite, for any finite $S \subset V$

So, finiteness of $\mathbf{gen}_K(G)$ is related to following property:

A set V of discrete valuations of K satisfies (Φ) for an absolutely almost simple K-group G if

(Φ) set of K-isomorphism classes of (inner) K-forms G' of G having good reduction at all $v \in V \setminus S$ is finite, for any finite $S \subset V$

Question.

When can a finitely generated field K be equipped with V that satisfies (Φ)?

So, finiteness of $\mathbf{gen}_K(G)$ is related to following property:

A set V of discrete valuations of K satisfies (Φ) for an absolutely almost simple K-group G if

(Φ) set of K-isomorphism classes of (inner) K-forms G' of G having good reduction at all $v \in V \setminus S$ is finite, for any finite $S \subset V$

Question.

When can a finitely generated field K be equipped with V that satisfies (Φ)?

Does a divisorial V satisfy (Φ)?

Additional challenges for arbitrary groups:

- It is not known how to classify forms by cohomological invariants.
- Even when such description is available (e.g. for type G_2), one needs to prove finiteness of unramified cohomology in degrees > 2, which is a difficult problem.

Additional challenges for arbitrary groups:

- It is not known how to classify forms by cohomological invariants.
- Even when such description is available (e.g. for type G_2), one needs to prove finiteness of unramified cohomology in degrees > 2, which is a difficult problem.

Additional challenges for arbitrary groups:

- It is not known how to classify forms by cohomological invariants.
- Even when such description is available (e.g. for type G_2), one needs to prove finiteness of unramified cohomology in degrees > 2, which is a difficult problem.

Additional challenges for arbitrary groups:

- It is not known how to classify forms by cohomological invariants.
- Even when such description is available (e.g. for type G_2), one needs to prove finiteness of unramified cohomology in degrees > 2, which is a difficult problem.

- Finiteness results for unramified Brauer groups imply that divisorial V does satisfy (Φ) for inner forms of type A_{n-1} for any finitely generated K such that $\operatorname{char} K \nmid n$.

Theorem 3

Let C be a smooth geometrically integral curve over a number field k, $K = k(C)$, and V divisorial set of places. Fix $n \geqslant 5$.

Theorem 3

Let C be a smooth geometrically integral curve over a number field k, $K = k(C)$, and V divisorial set of places. Fix $n \geqslant 5$.

Then *set of K-isomorphism classes of $\mathrm{Spin}_n(q)$ with good reduction at all $v \in V$ is finite.*

Theorem 3

Let C be a smooth geometrically integral curve over a number field k, $K = k(C)$, and V divisorial set of places. Fix $n \geqslant 5$.

Then *set of K-isomorphism classes of $\mathrm{Spin}_n(q)$ with good reduction at all $v \in V$ is finite.*

- Similar results for groups of types A_n, C_n, F_4 that split over a quadratic extension, and G_2.

Theorem 3

Let C be a smooth geometrically integral curve over a number field k, $K = k(C)$, and V divisorial set of places. Fix $n \geqslant 5$.

Then *set of K-isomorphism classes of $\mathrm{Spin}_n(q)$ with good reduction at all $v \in V$ is finite.*

- Similar results for groups of types A_n, C_n, F_4 that split over a quadratic extension, and G_2.

PROOF consists of two parts.

Theorem 3

Let C be a smooth geometrically integral curve over a number field k, $K = k(C)$, and V divisorial set of places. Fix $n \geqslant 5$.

Then *set of K-isomorphism classes of $\mathrm{Spin}_n(q)$ with good reduction at all $v \in V$ is finite.*

- Similar results for groups of types A_n, C_n, F_4 that split over a quadratic extension, and G_2.

PROOF consists of two parts.

1. Using Milnor's conjecture proved by Voevodsky, we reduce to finiteness of unramified cohomology $H^i(K, \mu_2)_V$, $\mu_2 = \{\pm 1\}$.
2. Prove finiteness of $H^i(K, \mu_2)_V$ for all $i \geqslant 1$.

Theorem 3

Let C be a smooth geometrically integral curve over a number field k, $K = k(C)$, and V divisorial set of places. Fix $n \geqslant 5$.

Then *set of K-isomorphism classes of $\mathrm{Spin}_n(q)$ with good reduction at all $v \in V$ is finite.*

- Similar results for groups of types A_n, C_n, F_4 that split over a quadratic extension, and G_2.

PROOF consists of two parts.

1. Using Milnor's conjecture proved by Voevodsky, we reduce to finiteness of unramified cohomology $H^i(K, \mu_2)_V$, $\mu_2 = \{\pm 1\}$.
2. Prove finiteness of $H^i(K, \mu_2)_V$ for all $i \geqslant 1$.

Theorem 3

Let C be a smooth geometrically integral curve over a number field k, $K = k(C)$, and V divisorial set of places. Fix $n \geqslant 5$.

Then *set of K-isomorphism classes of $\mathrm{Spin}_n(q)$ with good reduction at all $v \in V$ is finite.*

- Similar results for groups of types A_n, C_n, F_4 that split over a quadratic extension, and G_2.

PROOF consists of two parts.

1. Using Milnor's conjecture proved by Voevodsky, we reduce to finiteness of unramified cohomology $H^i(K, \mu_2)_V$, $\mu_2 = \{\pm 1\}$.
2. Prove finiteness of $H^i(K, \mu_2)_V$ for all $i \geqslant 1$.

Theorem 3

Let C be a smooth geometrically integral curve over a number field k, $K = k(C)$, and V divisorial set of places. Fix $n \geqslant 5$.

Then *set of K-isomorphism classes of $\mathrm{Spin}_n(q)$ with good reduction at all $v \in V$ is finite.*

- Similar results for groups of types A_n, C_n, F_4 that split over a quadratic extension, and G_2.

PROOF consists of two parts.

1. Using Milnor's conjecture proved by Voevodsky, we reduce to finiteness of unramified cohomology $H^i(K, \mu_2)_V$, $\mu_2 = \{\pm 1\}$.
2. Prove finiteness of $H^i(K, \mu_2)_V$ for all $i \geqslant 1$.

   Difficult case: $i = 3$.

Theorem 3

Let C be a smooth geometrically integral curve over a number field k, $K = k(C)$, and V divisorial set of places. Fix $n \geqslant 5$.

Then *set of K-isomorphism classes of $\mathrm{Spin}_n(q)$ with good reduction at all $v \in V$ is finite.*

- Similar results for groups of types A_n, C_n, F_4 that split over a quadratic extension, and G_2.

PROOF consists of two parts.

1. Using Milnor's conjecture proved by Voevodsky, we reduce to finiteness of unramified cohomology $H^i(K, \mu_2)_V$, $\mu_2 = \{\pm 1\}$.
2. Prove finiteness of $H^i(K, \mu_2)_V$ for all $i \geqslant 1$.

   Difficult case: $i = 3$. We adapt Jannsen's proof of Kato's local-global principle for H^3.

Finiteness of genus

Finiteness of genus

- Finiteness of $\mathbf{gen}_K(G)$ for inner forms of type A_n over any finitely generated field K.

Finiteness of genus

- Finiteness of $\mathbf{gen}_K(G)$ for inner forms of type A_n over any finitely generated field K.

Theorem 4

Let $K = k(C)$ where C is a smooth geometrically integral curve over a number field k, and $G = \mathrm{Spin}_n(q)$ where q is a quadratic form.

Finiteness of genus

- Finiteness of $\mathbf{gen}_K(G)$ for inner forms of type A_n over any finitely generated field K.

Theorem 4

Let $K = k(C)$ where C is a smooth geometrically integral curve over a number field k, and $G = \mathrm{Spin}_n(q)$ where q is a quadratic form. If either $n \geqslant 5$ is odd, or $n \geqslant 10$ is even and q is isotropic, then $\mathbf{gen}_K(G)$ is finite.

Finiteness of genus

- Finiteness of $\mathbf{gen}_K(G)$ for inner forms of type A_n over any finitely generated field K.

Theorem 4

Let $K = k(C)$ where C is a smooth geometrically integral curve over a number field k, and $G = \mathrm{Spin}_n(q)$ where q is a quadratic form. If either $n \geqslant 5$ is odd, or $n \geqslant 10$ is even and q is isotropic, then $\mathbf{gen}_K(G)$ is finite.

Theorem 5

Let G be a simple algebraic group of type G_2.

(1) *If $K = k(x)$, where k is a number field, then $|\mathbf{gen}_K(G)| = 1$;*

(2) *If $K = k(x_1, \ldots, x_r)$ or $k(C)$, where k is a number field, then $\mathbf{gen}_K(G)$ is finite.*

Global-to-local map

Global-to-local map

Theorem 6

Suppose V *satisfies* (I) *&* (Φ).

Global-to-local map

Theorem 6

Suppose V *satisfies* (I) *&* (Φ). *Then the natural map*

$$H^1(K, \overline{G}) \longrightarrow \prod_{v \in V} H^1(K_v, \overline{G})$$

for adjoint group $\overline{G}$ *is* proper.

Global-to-local map

Theorem 6

Suppose V satisfies (I) *&* (Φ). *Then the natural map*

$$H^1(K, \overline{G}) \longrightarrow \prod_{v \in V} H^1(K_v, \overline{G})$$

for adjoint group $\overline{G}$ is proper. *In particular, its kernel $Ш(\overline{G})$ is finite.*

Global-to-local map

Theorem 6

Suppose V satisfies (I) & (Φ). Then the natural map

$$H^1(K, \overline{G}) \longrightarrow \prod_{v \in V} H^1(K_v, \overline{G})$$

for adjoint group $\overline{G}$ is proper. *In particular, its kernel $Ш(\overline{G})$ is finite.*

True for:

Global-to-local map

Theorem 6

Suppose V *satisfies* (I) & (Φ). *Then the natural map*

$$H^1(K, \overline{G}) \longrightarrow \prod_{v \in V} H^1(K_v, \overline{G})$$

for adjoint group $\overline{G}$ *is* proper. *In particular, its kernel* $Ш(\overline{G})$ *is finite.*

True for:

- PSL_n over a finitely generated field K, $(n, \operatorname{char} K) = 1$;

Global-to-local map

Theorem 6

Suppose V *satisfies* (I) & (Φ). *Then the natural map*

$$H^1(K, \overline{G}) \longrightarrow \prod_{v \in V} H^1(K_v, \overline{G})$$

for adjoint group $\overline{G}$ *is* proper. *In particular, its kernel* $Ш(\overline{G})$ *is finite.*

True for:

- PSL_n over a finitely generated field K, $(n, \operatorname{char} K) = 1$;
- $\mathrm{SO}_n(q)$ over $K = k(C)$, k a number field;

Global-to-local map

Theorem 6

Suppose V *satisfies* (I) & (Φ). *Then the natural map*

$$H^1(K, \overline{G}) \longrightarrow \prod_{v \in V} H^1(K_v, \overline{G})$$

for adjoint group $\overline{G}$ *is* proper. *In particular, its kernel* $Ш(\overline{G})$ *is finite.*

True for:

- PSL_n over a finitely generated field K, $(n, \operatorname{char} K) = 1$;
- $\mathrm{SO}_n(q)$ over $K = k(C)$, k a number field;
- G of type G_2 over $K = k(C)$, k a number field.