Algebraic Groups and Field Extensions

Sebastiano Tronto

2020-04-01

Algebraic Varieties

K any field, $\overline{K}$ algebraic closure.

- Affine varieties: $V \subseteq \overline{K}^n$ zero set of system of polynomial equations
- Projective varieties: $V \subseteq \mathbb{P}^n_{\overline{K}}$ zero set of homogeneous polynomials
- Algebraic varieties: more general class, includes affine and projective
- Topology: Zariski topology (closed sets are sub-varieties)
- Morphisms: locally defined by ratios of polynomials
- "Defined over K" if the polynomials involved have coefficients in K

Algebraic Varieties - Examples

- Affine space $\overline{K}^n$ and projective space $\mathbb{P}^n_{\overline{K}}$ (empty set of equations)
- Linear subspaces (lines, hyperplanes...)
- Compact Riemann surfaces
- Complex submanifolds of $\mathbb{CP}^n$ (Chow's theorem)

The functor of points

$V \subseteq \overline{K}^n$ algebraic variety over K

- For any field extension $L \supseteq K$ we can consider

$$V(L) = \{(x_1, \ldots, x_n) \in V \mid x_1, \ldots, x_n \in L\}$$

- If $F \supseteq L$ then $V(F) \supseteq V(L)$
- A morphism of K-varieties $\varphi : V \to W$ induces maps $V(L) \to W(L)$

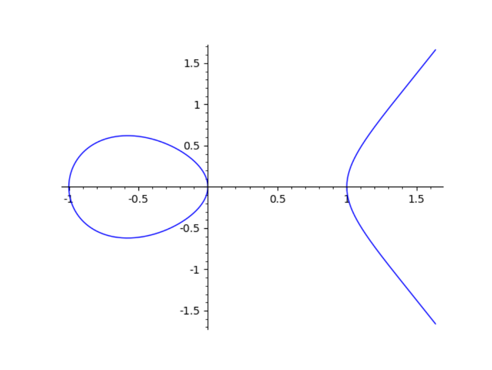
Example

$K = \mathbb{R}$
V: affine variety in $\mathbb{C}^1$ defined by $x^2 + 1 = 0$
$V(\mathbb{R}) = \emptyset$ and $V(\mathbb{C}) = \{i, -i\}$

The functor of points

Example

$K = \mathbb{Q}$, $\overline{K} = \overline{\mathbb{Q}}$
E: elliptic curve in $\mathbb{P}^2_{\mathbb{Q}}$ defined by $y^2z = x^3 - xz^2$
$E(\mathbb{Q}) = \{(0:1:0), (0:0:1), (1:0:1), (-1:0:1)\}$
$E(\mathbb{R})$:



Groups

Definition (1)

A group is a set G with:

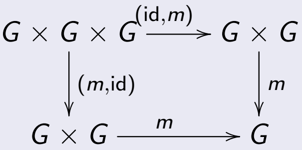
- An operation $\cdot : G \times G \to G$ such that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- An $e \in G$ such that $a \cdot e = e \cdot a = a$ for any $a \in G$;
- For each $a \in G$, an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition (2)

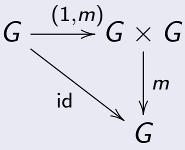
A group is a set G with maps

$$m : G \times G \to G \qquad e : \{\emptyset\} \to G \qquad i : G \to G$$

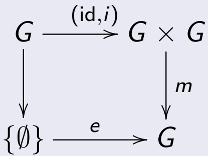
such that the following diagrams commute



$$m(a, m(b, c)) = m(m(a, b), c)$$



$$m(e(\emptyset), a) = a$$



$$m(a, i(a)) = e(\emptyset)$$


DEFINITION 1
DEFINITION 2
imgflip.com

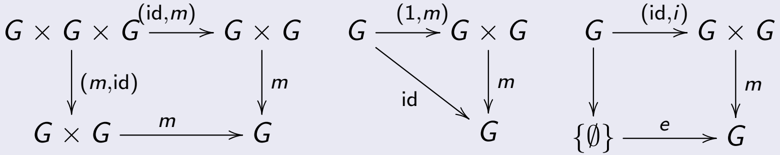
Groups in other categories

Definition

A topological group is a topological space G together continuous maps

$$m : G \times G \to G \qquad e : \{\emptyset\} \to G \qquad i : G \to G$$

such that the following diagrams commute



Groups in other categories

Definition

A Lie group is a smooth manifold G with smooth maps

$$m : G \times G \to G \qquad e : \{\emptyset\} \to G \qquad i : G \to G$$

such that the following diagrams commute

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{(\mathrm{id},m)} & G \times G \\ \downarrow{\scriptstyle (m,\mathrm{id})} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{(1,m)} & G \times G \\ & {\scriptstyle \mathrm{id}} \searrow & \downarrow{\scriptstyle m} \\ & & G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{(\mathrm{id},i)} & G \times G \\ \downarrow & & \downarrow{\scriptstyle m} \\ \{\emptyset\} & \xrightarrow{e} & G \end{array}$$

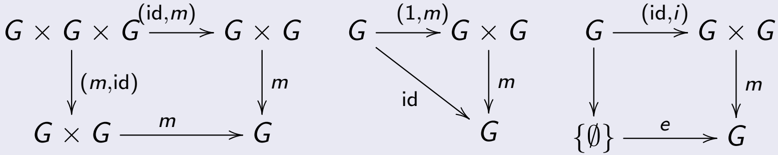
Algebraic Groups

Definition

An algebraic group is an algebraic variety G with morphisms

$$m : G \times G \to G \qquad e : \{\emptyset\} \to G \qquad i : G \to G$$

such that the following diagrams commute



Examples of algebraic groups

Example

The general linear group of degree 2

$$\mathrm{GL}_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \overline{K}^4 \mid ad - bc \neq 0 \right\}$$

can be rewritten as

$$\mathrm{GL}_2 = \left\{ (a, b, c, d, t) \in \overline{K}^5 \mid (ad - bc)t = 1 \right\}$$

It is an (affine) algebraic group with the usual matrix multiplication.

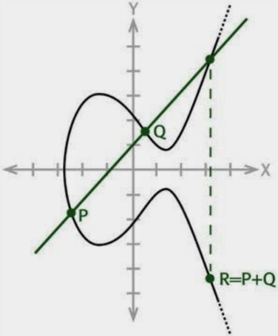
Examples of algebraic groups

Example

An elliptic curve over K is a projective curve defined by

$$y^2z = x^3 + axz^2 + bz^3 \qquad (a, b \in K, \quad 4a^3 \neq -27b^2)$$

It is a (projective) algebraic group:



The "group functor" of points

G algebraic group over K, $L \supseteq K$ field extension

- $G(L)$ is a set
- we have maps

$$m_L : G(L) \times G(L) \to G(L), \quad e_L : \{\emptyset\} \to G(L), \quad i_L : G(L) \to G(L)$$

  and the usual diagram commute
- Then $G(L)$ is a group

We can think of an algebraic group over K as a family of groups parametrized by the field extensions of K.

Field extensions from algebraic groups

K field, $\overline{K}$ algebraic closure, G algebraic group over K

- If G is **affine** and $P = (x_1, \dots, x_n) \in G(\overline{K})$, we define

$$K(P) := K(x_1, \dots, x_n)$$

- If G is projective and $P = (x_0 : \cdots : x_n) \in G(\overline{K})$, assuming $x_0 \neq 0$

$$K(P) := K\left(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}\right)$$

- In both cases $K(P)$ is an algebraic extension of K

Field extensions from algebraic groups

More abstract definition:

- There is an action of $\mathrm{Gal}(\overline{K} \mid K)$ on $G(\overline{K})$
- Call $H_P = \{g \in \mathrm{Gal}(\overline{K} \mid K) \mid g(P) = P\}$
- $\overline{K}^{H_P} = \{z \in \overline{K} \mid h(z) = z \quad \forall\, h \in H_P\}$
- Define $K(P) := \overline{K}^{H_P}$

Torsion fields

G commutative algebraic group over K, char $K = 0$

- For $n > 1$ consider $G[n] = \{P \in G(\overline{K}) \mid nP = 0\} \cong (\mathbb{Z}/n\mathbb{Z})^b$
- $K(G[n])$ is called *n-torsion field* of G
- The action of $\mathrm{Gal}(\overline{K} \mid K)$ on $G[n]$ gives a Galois representation

$$\rho_n : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_b(\mathbb{Z}/n\mathbb{Z})$$

whose image is isomorphic to $\mathrm{Gal}(K(G[n]) \mid K)$

Torsion fields

Example

If $G = \mathbb{G}_m = \overline{K}^\times$ then $n = 1$ and $G[n] = \{\zeta \in \overline{K}^\times \mid \zeta^n = 1\}$.
$K(\mathbb{G}_m[n])$ is the n-th cyclotomic extension of K.

Example

If G is an elliptic curve then $n = 2$.
If K is a number field and G has no CM, Serre's Open Image tells us that the image of ρ_n in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ has index bounded independently of n.

Kummer theory

G, K and n as before, fix $P_0 \in G(K)$ not torsion

- Consider $n^{-1}P_0 = \{Q \in G(\overline{K}) \mid nQ = P_0\}$
- We call $K(n^{-1}P_0)$ the *n-division field* of P_0
- Fixing $Q_0 \in n^{-1}P_0$ we get a bijection

$$\begin{aligned} n^{-1}P_0 &\to G[n] \\ Q &\mapsto Q - Q_0 \end{aligned}$$

so $K(n^{-1}P_0) \supseteq K(G[n])$

Kummer theory

- We have a "representation"

$$\begin{aligned} \kappa_n : \mathrm{Gal}(\overline{K} \mid K(G[n])) &\to G[n] \cong (\mathbb{Z}/n\mathbb{Z})^b \\ g &\mapsto g(Q_0) - Q_0 \end{aligned}$$

  whose image is $\mathrm{Gal}(\overline{K} \mid K(G[n]))$
- The Kummer extension $K(n^{-1}P_0) \mid K(G[n])$ is "easy" to study (abelian), but relies on understanding $K(G[n])$.

Kummer theory

Example

If $G = \mathbb{G}_m$ and $P_0 \in K^\times$, then $n^{-1}P_0$ is the set of all n-th roots of P_0 in $\overline{K}$, i.e. the roots of $x^n - P_0$.
$K(n^{-1}P_0) \mid K(G[n])$ is a Kummer extension in the classical sense:

$$K(\sqrt[n]{P_0}, \zeta_n) \mid K(\zeta_n)$$

A question

G commutative algebraic group over K, char $K = 0$, $n > 1$, $L = K(G[n])$

Question

Are there points $P_0 \in G(K)$ such that

- There is no $Q \in G(K)$ with $nQ = P_0$, but $\quad (P_0 \notin nG(K))$
- There is $Q \in G(L)$ with $nQ = P_0$? $\quad (P_0 \in nG(L))$

An exact sequence

Let $\Gamma := \mathrm{Gal}(L \mid K)$. The exact sequence of Γ-modules

$$0 \to G(L)[n] \to G(L) \xrightarrow{\cdot n} nG(L) \to 0$$

induces a long exact sequence in group cohomology

$$0 \to H^0(\Gamma, G(L)[n]) \to H^0(\Gamma, G(L)) \to H^0(\Gamma, nG(L)) \to H^1(\Gamma, G(L)[n]) \to \cdots$$

which we can rewrite as

$$0 \to G(K)[n] \to G(K) \xrightarrow{\cdot n} G(K) \cap nG(L) \xrightarrow{\delta} H^1(\Gamma, G[n]) \to \cdots$$

An exact sequence

Using the fact that $G(K)/G(K)[n] \cong nG(K)$ we have

$$0 \to nG(K) \to G(K) \cap nG(L) \xrightarrow{\delta} H^1(\Gamma, G[n]) \to \cdots$$

and we conclude that

$$\frac{G(K) \cap nG(L)}{nG(K)} \hookrightarrow H^1(\mathrm{Gal}(L \mid K), G[n])$$

A partial answer

Partial answer

If $H^1(\mathrm{Gal}(L \mid K), G[n]) = 0$ then "Question" has negative answer.

A counterexample

Let $K = \mathbb{Q}$, $n = p$ a prime and G an elliptic curve.

Theorem (Lawson, Wuthrich (2015))

If $p \notin \{3, 5, 11\}$ then $H^1(\mathrm{Gal}(K(G[n]) \mid K), G[n])) = 0$.

A counterexample

The elliptic curve over $\mathbb{Q}$

$$E: \qquad y^2 + y = x^3 - 216x - 1861 \qquad\qquad \text{(Cremona 17739g1)}$$

Has $\mathbb{Q}(E[3]) = L := \mathbb{Q}[x]/(x^3 + 54x - 18)$. There is a point

$$P_0 = \left(\frac{23769}{400}, \frac{3529853}{8000}\right) \in E(\mathbb{Q})$$

such that

- There is no $Q \in E(K)$ with $3Q = P_0$, but
- There is $Q \in E(L)$ with $nQ = P_0$.

Thank you for your attention!