Algebraic matroids and group configurations

Tobias Boege and Geva Yashfe

Department of Mathematics and Statistics
UiT The Arctic University of Norway

Oberseminar Groups and Geometry,
Bielefeld, 6 May 2026

Supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 101110545.

Funded by the European Union

Outline

Recognizing linear matroids

- Consider an F-vector space V.

Recognizing linear matroids

- Consider an F-vector space V.
- Elements $v_1, \ldots, v_n \in V$ define a linear matroid on $[n]$:
  - I is independent if and only if $(v_i : i \in I)$ is linearly independent over F,
  - The rank of a set K is the dimension of $\text{span}(v_i : i \in K)$ over F.

Recognizing linear matroids

- Consider an F-vector space V.
- Elements $v_1, \ldots, v_n \in V$ define a linear matroid on $[n]$:
  - I is independent if and only if $(v_i : i \in I)$ is linearly independent over F,
  - The rank of a set K is the dimension of $\text{span}(v_i : i \in K)$ over F.

Recognition problem

Is there an algorithm to which I can input a matroid and it tells me if it is F-linear?

Recognizing linear matroids

- Consider an F-vector space V.
- Elements $v_1, \ldots, v_n \in V$ define a linear matroid on $[n]$:
  - I is independent if and only if $(v_i : i \in I)$ is linearly independent over F,
  - The rank of a set K is the dimension of $\text{span}(v_i : i \in K)$ over F.

Recognition problem

Is there an algorithm to which I can input a matroid and it tells me if it is F-linear?

Universality theorem (MacLane (1936)?)

The recognition problem is just as hard as deciding if a system of Diophantine equations has a solution over F.

Simple linear matroids of rank 3: points and lines

- In a simple linear matroid of rank 3 any two vectors are independent.

Simple linear matroids of rank 3: points and lines

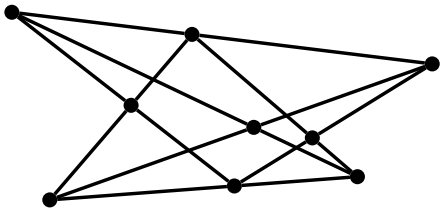
- In a simple linear matroid of rank 3 any two vectors are independent.
- Think of a vector as a point in a projective plane. Any two points span a line.

Simple linear matroids of rank 3: points and lines

- In a simple linear matroid of rank 3 any two vectors are independent.
- Think of a vector as a point in a projective plane. Any two points span a line.
- The matroid encodes which points are on which lines.

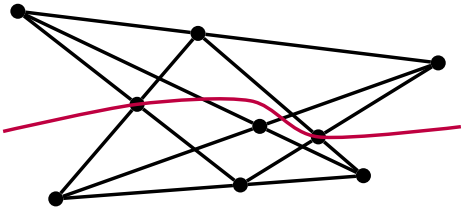
Simple linear matroids of rank 3: points and lines

- In a simple linear matroid of rank 3 any two vectors are independent.
- Think of a vector as a point in a projective plane. Any two points span a line.
- The matroid encodes which points are on which lines.



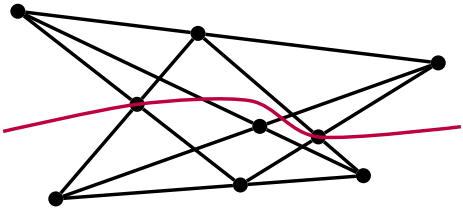
Simple linear matroids of rank 3: points and lines

- In a simple linear matroid of rank 3 any two vectors are independent.
- Think of a vector as a point in a projective plane. Any two points span a line.
- The matroid encodes which points are on which lines.



Simple linear matroids of rank 3: points and lines

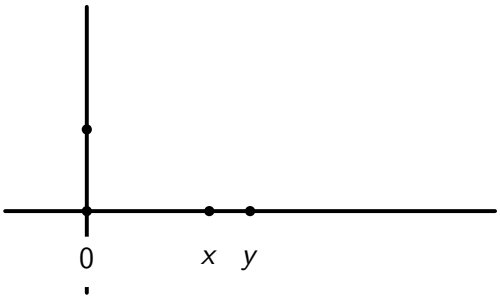
- In a simple linear matroid of rank 3 any two vectors are independent.
- Think of a vector as a point in a projective plane. Any two points span a line.
- The matroid encodes which points are on which lines.



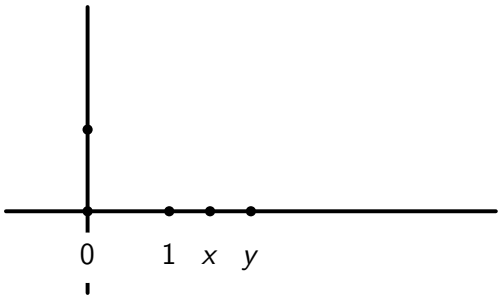
von Staudt (1857)

The existential theory of F reduces to constructing point-line configurations.

Von Staudt constructions

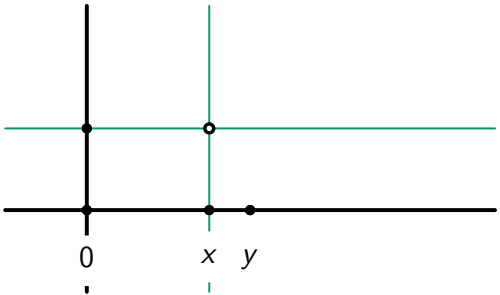


Addition

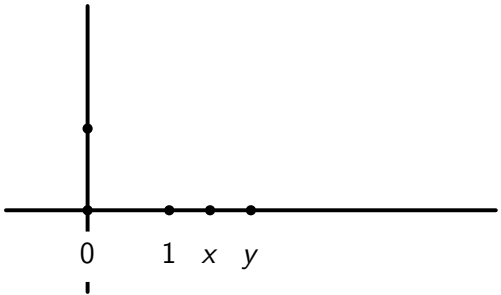


Multiplication

Von Staudt constructions

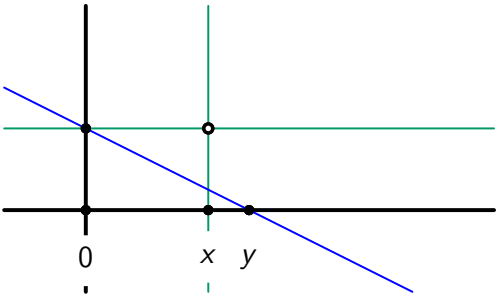


Addition

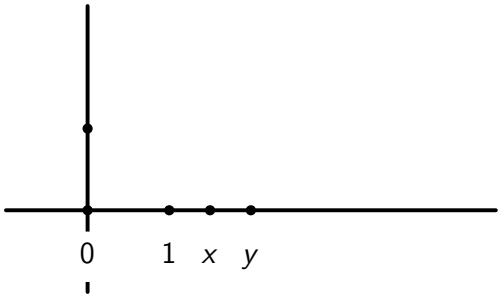


Multiplication

Von Staudt constructions

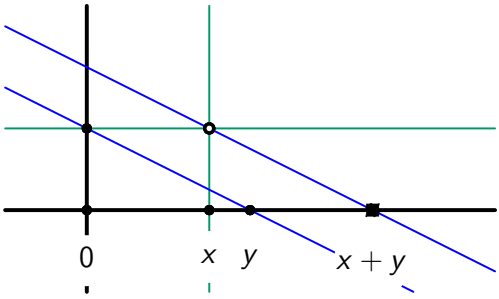


Addition

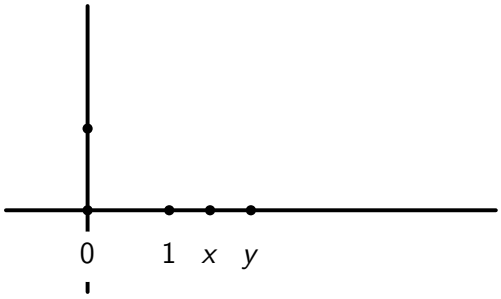


Multiplication

Von Staudt constructions

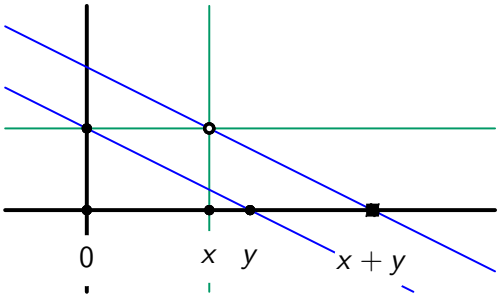


Addition

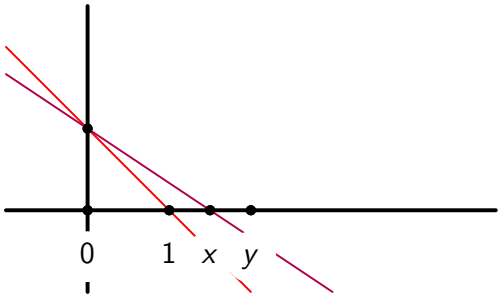


Multiplication

Von Staudt constructions

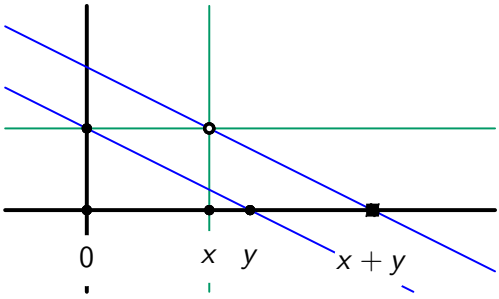


Addition

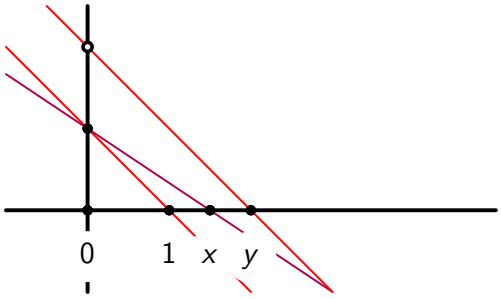


Multiplication

Von Staudt constructions

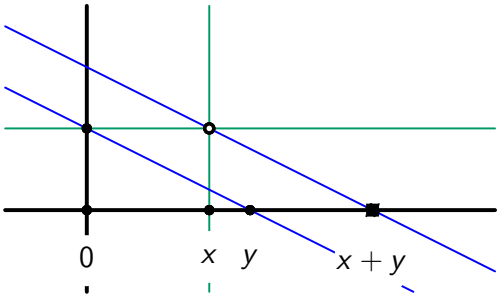


Addition

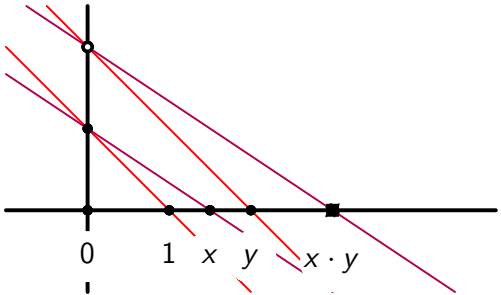


Multiplication

Von Staudt constructions

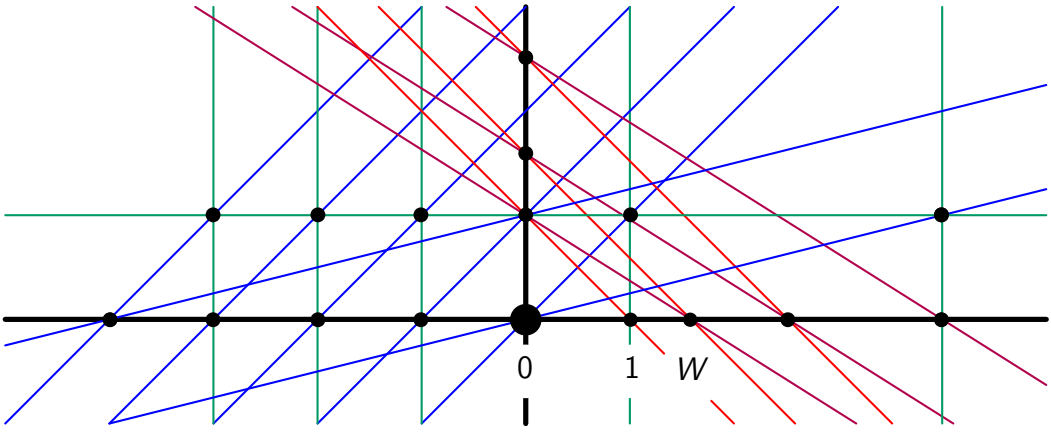


Addition

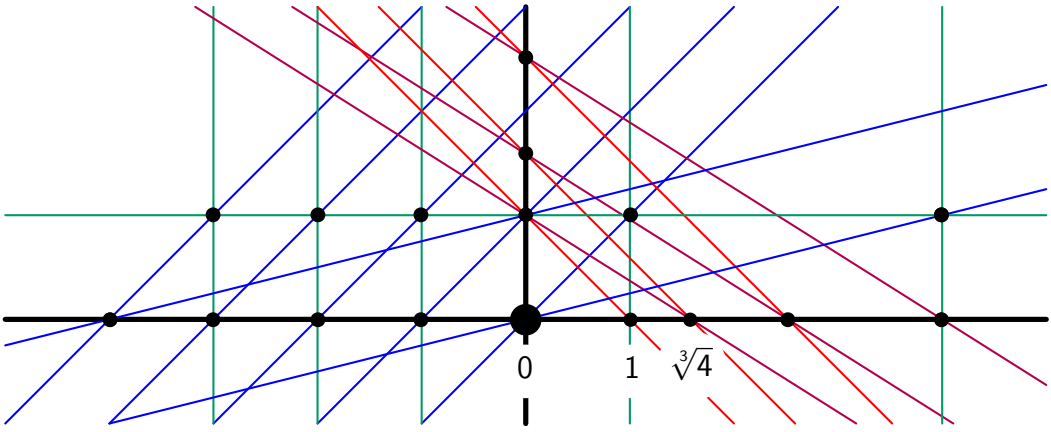


Multiplication

Where is Waldo?



Where is Waldo? On the cube root of 4!



Algebraic matroids

- Consider a field extension K/F.

Algebraic matroids

- Consider a field extension K/F.
- Elements $x_1, \ldots, x_n \in K$ define an algebraic matroid on $[n]$:
  - I is independent if and only if $\{x_i : i \in I\}$ is algebraically independent over F,
  - The rank of a set A is the transcendence degree of $F(x_i : i \in A)$ over F.

Algebraic matroids

- Consider a field extension K/F.
- Elements $x_1, \ldots, x_n \in K$ define an algebraic matroid on $[n]$:
  - I is independent if and only if $\{x_i : i \in I\}$ is algebraically independent over F,
  - The rank of a set A is the transcendence degree of $F(x_i : i \in A)$ over F.

Recognition problems

- AlgMat_F: Is M algebraic over a field F?

Algebraic matroids

- Consider a field extension K/F.
- Elements $x_1, \ldots, x_n \in K$ define an algebraic matroid on $[n]$:
  - I is independent if and only if $\{x_i : i \in I\}$ is algebraically independent over F,
  - The rank of a set A is the transcendence degree of $F(x_i : i \in A)$ over F.

Recognition problems

- AlgMat_F: Is M algebraic over a field F?
- AlgMat_p: Is M algebraic over some field of characteristic p?

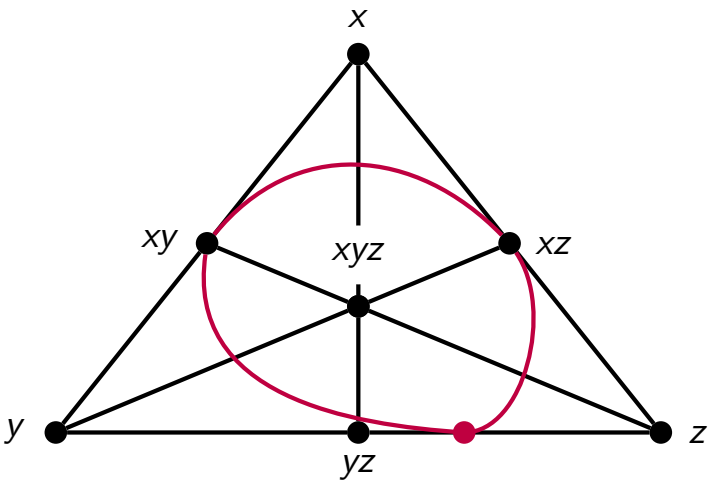
Algebraic matroids

- Consider a field extension K/F.
- Elements $x_1, \ldots, x_n \in K$ define an algebraic matroid on $[n]$:
  - I is independent if and only if $\{x_i : i \in I\}$ is algebraically independent over F,
  - The rank of a set A is the transcendence degree of $F(x_i : i \in A)$ over F.

Recognition problems

- AlgMat_F: Is M algebraic over a field F?
- AlgMat_p: Is M algebraic over some field of characteristic p?
- AlgMat: Is M algebraic over some field?

Non-Fano is algebraic over $\mathbb{F}_2$



Some results and connections

Piff (1969) & Ingleton (1971)

If M is linear over F then it is algebraic over F. If F is algebraically closed of characteristic zero, the converse holds, too.

Some results and connections

Piff (1969) & Ingleton (1971)

If M is linear over F then it is algebraic over F. If F is algebraically closed of characteristic zero, the converse holds, too.

Piff (1972) & Lindström (1989)

M is algebraic over some field F if and only if it is algebraic over the prime field of F.

☞ Thus $\mathsf{AlgMat}_F = \mathsf{AlgMat}_{F'} = \mathsf{AlgMat}_p$.

Some results and connections

Piff (1969) & Ingleton (1971)

If M is linear over F then it is algebraic over F. If F is algebraically closed of characteristic zero, the converse holds, too.

Piff (1972) & Lindström (1989)

M is algebraic over some field F if and only if it is algebraic over the prime field of F.

☞ Thus $\mathrm{AlgMat}_F = \mathrm{AlgMat}_{F'} = \mathrm{AlgMat}_p$.

Lindström (1985)

For each prime $p > 0$ there is a matroid M_p which is algebraic over a field F if and only if $\mathrm{char}\, F = p$.

☞ Can reduce AlgMat_p to AlgMat by transforming M to $M \oplus M_p$.

Recognizing algebraic matroids

Boege–Yashfe (2026+)

The problem AlgMat_p is undecidable for all $p > 0$. Hence, AlgMat is undecidable, too.

Recognizing algebraic matroids

Boege–Yashfe (2026+)

The problem AlgMat_p is undecidable for all $p > 0$. Hence, AlgMat is undecidable, too.

- Suppose K/F is a field extension and $x_1, \ldots, x_n \in K$. We can assume $F = \mathbb{F}_p$.

Recognizing algebraic matroids

Boege–Yashfe (2026+)

The problem AlgMat_p is undecidable for all $p > 0$. Hence, AlgMat is undecidable, too.

- Suppose K/F is a field extension and $x_1, \ldots, x_n \in K$. We can assume $F = \mathbb{F}_p$.
- They are the coordinate functions of an irreducible affine variety V over $\mathbb{F}_p$:

Recognizing algebraic matroids

Boege–Yashfe (2026+)

The problem AlgMat_p is undecidable for all $p > 0$. Hence, AlgMat is undecidable, too.

- Suppose K/F is a field extension and $x_1, \ldots, x_n \in K$. We can assume $F = \mathbb{F}_p$.
- They are the coordinate functions of an irreducible affine variety V over $\mathbb{F}_p$:
  - Consider the map $\phi\colon \mathbb{F}_p[t_1, \ldots, t_n] \to K$ sending $t_i \mapsto x_i$.

Recognizing algebraic matroids

Boege–Yashfe (2026+)

The problem AlgMat_p is undecidable for all $p > 0$. Hence, AlgMat is undecidable, too.

- Suppose K/F is a field extension and $x_1, \ldots, x_n \in K$. We can assume $F = \mathbb{F}_p$.
- They are the coordinate functions of an irreducible affine variety V over $\mathbb{F}_p$:
  - Consider the map $\phi\colon \mathbb{F}_p[t_1, \ldots, t_n] \to K$ sending $t_i \mapsto x_i$.
  - Then $\mathscr{I} = \ker \phi$ is prime and its zero locus is an irreducible variety.

Recognizing algebraic matroids

Boege–Yashfe (2026+)

The problem AlgMat_p is undecidable for all $p > 0$. Hence, AlgMat is undecidable, too.

- Suppose K/F is a field extension and $x_1, \ldots, x_n \in K$. We can assume $F = \mathbb{F}_p$.
- They are the coordinate functions of an irreducible affine variety V over $\mathbb{F}_p$:
  - Consider the map $\phi\colon \mathbb{F}_p[t_1, \ldots, t_n] \to K$ sending $t_i \mapsto x_i$.
  - Then $\mathscr{I} = \ker \phi$ is prime and its zero locus is an irreducible variety.
- The search space for algebraic representations is $\operatorname{Spec} \mathbb{F}_p[x_1, \ldots, x_n]$.

Recognizing algebraic matroids

Boege–Yashfe (2026+)

The problem AlgMat_p is undecidable for all $p > 0$. Hence, AlgMat is undecidable, too.

- Suppose K/F is a field extension and $x_1, \ldots, x_n \in K$. We can assume $F = \mathbb{F}_p$.
- They are the coordinate functions of an irreducible affine variety V over $\mathbb{F}_p$:
  - Consider the map $\phi\colon \mathbb{F}_p[t_1, \ldots, t_n] \to K$ sending $t_i \mapsto x_i$.
  - Then $\mathscr{I} = \ker \phi$ is prime and its zero locus is an irreducible variety.
- The search space for algebraic representations is $\operatorname{Spec} \mathbb{F}_p[x_1, \ldots, x_n]$.
- Unclear how to perform the search or conclude that there is no representation.

Recognizing algebraic matroids

Boege–Yashfe (2026+)

The problem AlgMat_p is undecidable for all $p > 0$. Hence, AlgMat is undecidable, too.

- Suppose K/F is a field extension and $x_1, \ldots, x_n \in K$. We can assume $F = \mathbb{F}_p$.
- They are the coordinate functions of an irreducible affine variety V over $\mathbb{F}_p$:
  - Consider the map $\phi\colon \mathbb{F}_p[t_1, \ldots, t_n] \to K$ sending $t_i \mapsto x_i$.
  - Then $\mathscr{I} = \ker \phi$ is prime and its zero locus is an irreducible variety.
- The search space for algebraic representations is $\operatorname{Spec} \mathbb{F}_p[x_1, \ldots, x_n]$.
- Unclear how to perform the search or conclude that there is no representation.
- Also unclear how to encode the execution of a universal Turing machine in this.

The Group Configuration Theorem

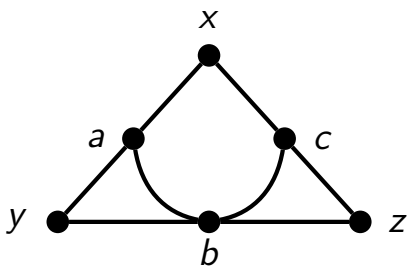
- Two tuples (x_i) and (x_i') in K/F are interalgebraic if $\mathrm{acl}(F(x_i)) = \mathrm{acl}(F(x_i'))$.

The Group Configuration Theorem

- Two tuples (x_i) and (x_i') in K/F are interalgebraic if $\mathrm{acl}(F(x_i)) = \mathrm{acl}(F(x_i'))$.

Hrushovski (1986)

Let K/F both be algebraically closed. If $x, y, z, a, b, c \in K$ are an algebraic realization of the below group configuration matroid over F

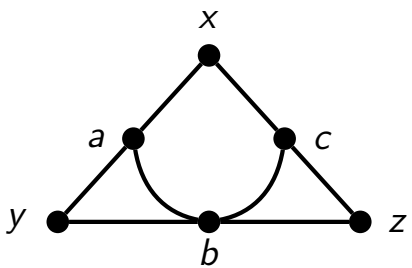


The Group Configuration Theorem

- Two tuples (x_i) and (x_i') in K/F are interalgebraic if $\mathrm{acl}(F(x_i)) = \mathrm{acl}(F(x_i'))$.

Hrushovski (1986)

Let K/F both be algebraically closed. If $x, y, z, a, b, c \in K$ are an algebraic realization of the below group configuration matroid over F then there exists a one-dimensional, connected algebraic group G defined over F

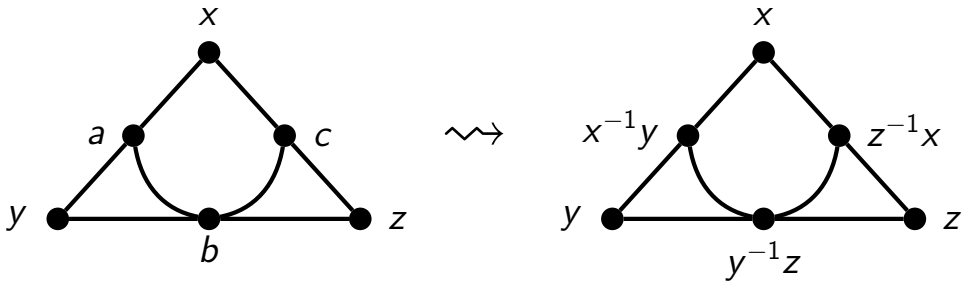


The Group Configuration Theorem

- Two tuples (x_i) and (x_i') in K/F are interalgebraic if $\mathrm{acl}(F(x_i)) = \mathrm{acl}(F(x_i'))$.

Hrushovski (1986)

Let K/F both be algebraically closed. If $x, y, z, a, b, c \in K$ are an algebraic realization of the below group configuration matroid over F then there exists a one-dimensional, connected algebraic group G defined over F and an interalgebraic realization of the form $x', y', z', a', b', c' \in G$ where $a' = x'^{-1}y'$, $b' = y'^{-1}z'$, and $c' = z'^{-1}x'$.



Endomorphism labeling

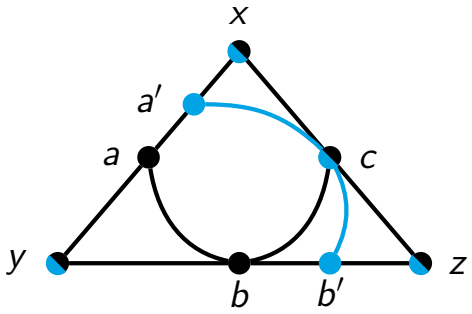
- The Group Configuration Theorem regularizes algebraic representations: instead of arbitrary polynomial equations we can assume multiplication in some group.

Endomorphism labeling

- The Group Configuration Theorem regularizes algebraic representations: instead of arbitrary polynomial equations we can assume multiplication in some group.

Evans & Hrushovski (1991)

Consider the augmented (double) group configuration below. There exist non-zero $\beta, \gamma \in \mathrm{End}_F(G)$ such that $\mathrm{acl}(b') = \mathrm{acl}(\beta(y) * \gamma(z))$.



Census of one-dimensional, connected algebraic groups

Theorem

The one-dimensional, connected algebraic groups in K defined over F are:

Census of one-dimensional, connected algebraic groups

Theorem

The one-dimensional, connected algebraic groups in K defined over F are:

- $\mathbb{G}_{\mathrm{a}}(K)$ the additive group of K, or

Census of one-dimensional, connected algebraic groups

Theorem

The one-dimensional, connected algebraic groups in K defined over F are:

- $\mathbb{G}_{\mathrm{a}}(K)$ the additive group of K, or
- $\mathbb{G}_{\mathrm{m}}(K)$ the multiplicative group of K, or

Census of one-dimensional, connected algebraic groups

Theorem

The one-dimensional, connected algebraic groups in K defined over F are:

- $\mathbb{G}_{\mathrm{a}}(K)$ the additive group of K, or
- $\mathbb{G}_{\mathrm{m}}(K)$ the multiplicative group of K, or
- $\mathbb{E}(K)$ the K-rational points of an elliptic curve.

Census of one-dimensional, connected algebraic groups

Theorem

The one-dimensional, connected algebraic groups in K defined over F are:

- $\mathbb{G}_{\mathsf{a}}(K)$ the additive group of K, or
- $\mathbb{G}_{\mathsf{m}}(K)$ the multiplicative group of K, or
- $\mathbb{E}(K)$ the K-rational points of an elliptic curve.

- All of them are abelian, $\mathrm{End}_F(G)$ are all rings satisfying the left Ore property.

Census of one-dimensional, connected algebraic groups

Theorem

The one-dimensional, connected algebraic groups in K defined over F are:

- $\mathbb{G}_{\mathsf{a}}(K)$ the additive group of K, or
- $\mathbb{G}_{\mathsf{m}}(K)$ the multiplicative group of K, or
- $\mathbb{E}(K)$ the K-rational points of an elliptic curve.

- All of them are abelian, $\mathrm{End}_F(G)$ are all rings satisfying the left Ore property.
- Thus, $\mathrm{End}_F(G)$ embeds into a canonical skew field of fractions $L_F(G)$.

Census of one-dimensional, connected algebraic groups

Theorem

The one-dimensional, connected algebraic groups in K defined over F are:

- $\mathbb{G}_{\mathsf{a}}(K)$ the additive group of K, or
- $\mathbb{G}_{\mathsf{m}}(K)$ the multiplicative group of K, or
- $\mathbb{E}(K)$ the K-rational points of an elliptic curve.

- All of them are abelian, $\mathrm{End}_F(G)$ are all rings satisfying the left Ore property.
- Thus, $\mathrm{End}_F(G)$ embeds into a canonical skew field of fractions $L_F(G)$.

Theorem

- $L_F(\mathbb{G}_{\mathsf{a}})$ is the skew field $F(\sigma)$ where $\sigma\colon F \to F$ is the Frobenius,

Census of one-dimensional, connected algebraic groups

Theorem

The one-dimensional, connected algebraic groups in K defined over F are:

- $\mathbb{G}_{\mathsf{a}}(K)$ the additive group of K, or
- $\mathbb{G}_{\mathsf{m}}(K)$ the multiplicative group of K, or
- $\mathbb{E}(K)$ the K-rational points of an elliptic curve.

- All of them are abelian, $\mathrm{End}_F(G)$ are all rings satisfying the left Ore property.
- Thus, $\mathrm{End}_F(G)$ embeds into a canonical skew field of fractions $L_F(G)$.

Theorem

- $L_F(\mathbb{G}_{\mathsf{a}})$ is the skew field $F(\sigma)$ where $\sigma\colon F \to F$ is the Frobenius,
- $L_F(\mathbb{G}_{\mathsf{m}}) = \mathbb{Q}$,

Census of one-dimensional, connected algebraic groups

Theorem

The one-dimensional, connected algebraic groups in K defined over F are:

- $\mathbb{G}_{\mathsf{a}}(K)$ the additive group of K, or
- $\mathbb{G}_{\mathsf{m}}(K)$ the multiplicative group of K, or
- $\mathbb{E}(K)$ the K-rational points of an elliptic curve.

- All of them are abelian, $\mathrm{End}_F(G)$ are all rings satisfying the left Ore property.
- Thus, $\mathrm{End}_F(G)$ embeds into a canonical skew field of fractions $L_F(G)$.

Theorem

- $L_F(\mathbb{G}_{\mathsf{a}})$ is the skew field $F(\sigma)$ where $\sigma\colon F \to F$ is the Frobenius,
- $L_F(\mathbb{G}_{\mathsf{m}}) = \mathbb{Q}$,
- $L_F(\mathbb{E}) \in \left\{ \mathbb{Q}(\sqrt{-d}),\ \left(\frac{a,b}{\mathbb{Q}}\right) \right\}$.

Coordinates

Evans & Hrushovski (1991)

Let G be a one-dimensional, connected algebraic group in K defined over F and $x, y, z \in G$ independent and generic.

Coordinates

Evans & Hrushovski (1991)

Let G be a one-dimensional, connected algebraic group in K defined over F and $x, y, z \in G$ independent and generic. The collection of fields

$$\left\{ \mathrm{acl}(\alpha(x) * \beta(y) * \gamma(z)) : \alpha, \beta, \gamma \in \mathrm{End}_F(G) \text{ not all zero} \right\}$$

is a projective plane.

Coordinates

Evans & Hrushovski (1991)

Let G be a one-dimensional, connected algebraic group in K defined over F and $x, y, z \in G$ independent and generic. The collection of fields

$$\left\{ \mathrm{acl}(\alpha(x) * \beta(y) * \gamma(z)) : \alpha, \beta, \gamma \in \mathrm{End}_F(G) \text{ not all zero} \right\}$$

is a projective plane. (Moreover, every projective plane in the full algebraic matroid of K/F is contained in a plane of this form.)

Coordinates

Evans & Hrushovski (1991)

Let G be a one-dimensional, connected algebraic group in K defined over F and $x, y, z \in G$ independent and generic. The collection of fields

$$\left\{ \mathrm{acl}(\alpha(x) * \beta(y) * \gamma(z)) : \alpha, \beta, \gamma \in \mathrm{End}_F(G) \text{ not all zero} \right\}$$

is a projective plane. (Moreover, every projective plane in the full algebraic matroid of K/F is contained in a plane of this form.)

- These projective planes are coordinatized by the skew fields $L_F(G)$.

Coordinates

Evans & Hrushovski (1991)

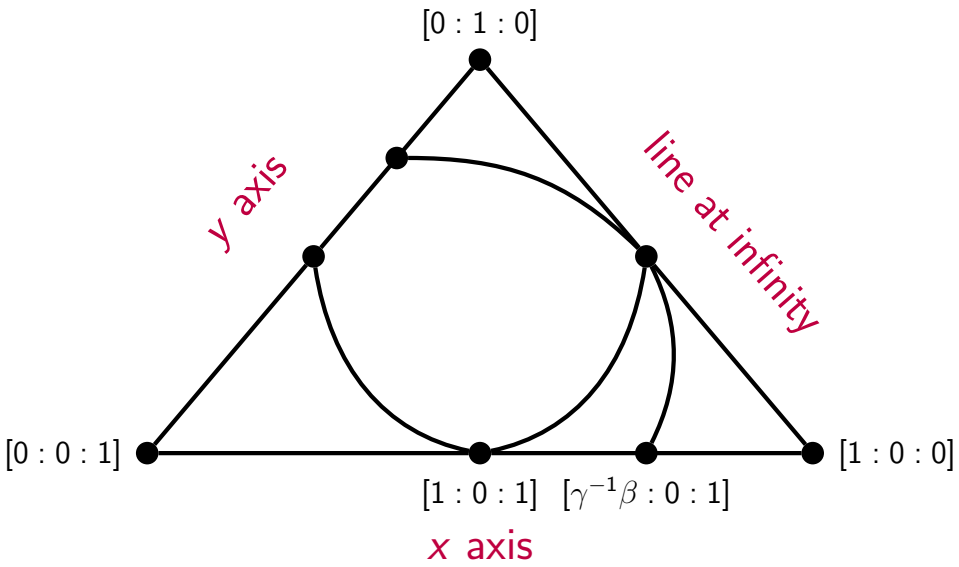
Let G be a one-dimensional, connected algebraic group in K defined over F and $x, y, z \in G$ independent and generic. The collection of fields

$$\left\{ \mathrm{acl}(\alpha(x) * \beta(y) * \gamma(z)) : \alpha, \beta, \gamma \in \mathrm{End}_F(G) \text{ not all zero} \right\}$$

is a projective plane. (Moreover, every projective plane in the full algebraic matroid of K/F is contained in a plane of this form.)

- These projective planes are coordinatized by the skew fields $L_F(G)$.
- The group configuration acts as a projective basis.

Group configuration as a projective basis



Playing with skew fields

- Von Staudt constructions become available through algebraic matroids.

Playing with skew fields

- Von Staudt constructions become available through algebraic matroids.
- Get access to the existential theory of a skew field but we do not know which.

Playing with skew fields

- Von Staudt constructions become available through algebraic matroids.
- Get access to the existential theory of a skew field but we do not know which.

Observation

The existential theory of $\overline{\mathbb{F}_p}(\sigma)$ reduces to AlgMat_p for all $p > 0$.

Playing with skew fields

- Von Staudt constructions become available through algebraic matroids.
- Get access to the existential theory of a skew field but we do not know which.

Observation

The existential theory of $\overline{\mathbb{F}_p}(\sigma)$ reduces to AlgMat_p for all $p > 0$.

- It is the only skew field of characteristic p!

Playing with skew fields

- Von Staudt constructions become available through algebraic matroids.
- Get access to the existential theory of a skew field but we do not know which.

Observation

The existential theory of $\overline{\mathbb{F}_p}(\sigma)$ reduces to AlgMat_p for all $p > 0$.

- It is the only skew field of characteristic p!

Observation

The existential theory of $\mathbb{Q}$ reduces to AlgMat_p for all $p > 0$.

Playing with skew fields

- Von Staudt constructions become available through algebraic matroids.
- Get access to the existential theory of a skew field but we do not know which.

Observation

The existential theory of $\overline{\mathbb{F}_p}(\sigma)$ reduces to AlgMat_p for all $p > 0$.

- It is the only skew field of characteristic p!

Observation

The existential theory of $\mathbb{Q}$ reduces to AlgMat_p for all $p > 0$.

- Pick a (supersingular) elliptic curve $\mathbb{E}$ and $a, b \in \mathbb{Z}_{<0}$ such that $L_{\overline{\mathbb{F}_p}}(\mathbb{E}) = \left(\frac{a,b}{\mathbb{Q}}\right)$.

Playing with skew fields

- Von Staudt constructions become available through algebraic matroids.
- Get access to the existential theory of a skew field but we do not know which.

Observation

The existential theory of $\overline{\mathbb{F}_p}(\sigma)$ reduces to AlgMat_p for all $p > 0$.

- It is the only skew field of characteristic p!

Observation

The existential theory of $\mathbb{Q}$ reduces to AlgMat_p for all $p > 0$.

- Pick a (supersingular) elliptic curve $\mathbb{E}$ and $a, b \in \mathbb{Z}_{<0}$ such that $L_{\overline{\mathbb{F}_p}}(\mathbb{E}) = \left(\frac{a,b}{\mathbb{Q}}\right)$.
- Any $x, y \in \left(\frac{a,b}{\mathbb{Q}}\right)$ with $x^2 = a, y^2 = b, xy = -yx$ yield a $\mathbb{Q}$-basis $\{1, x, y, xy\}$.

Playing with skew fields

- Von Staudt constructions become available through algebraic matroids.
- Get access to the existential theory of a skew field but we do not know which.

Observation

The existential theory of $\overline{\mathbb{F}_p}(\sigma)$ reduces to AlgMat_p for all $p > 0$.

- It is the only skew field of characteristic p!

Observation

The existential theory of $\mathbb{Q}$ reduces to AlgMat_p for all $p > 0$.

- Pick a (supersingular) elliptic curve $\mathbb{E}$ and $a, b \in \mathbb{Z}_{<0}$ such that $L_{\overline{\mathbb{F}_p}}(\mathbb{E}) = \left(\frac{a,b}{\mathbb{Q}}\right)$.
- Any $x, y \in \left(\frac{a,b}{\mathbb{Q}}\right)$ with $x^2 = a, y^2 = b, xy = -yx$ yield a $\mathbb{Q}$-basis $\{1, x, y, xy\}$.
- Then $w \in \mathbb{Q} \iff xw = wx \wedge yw = wy$ is an existential definition of $\mathbb{Q}$.

Undecidability in the affine group

- The affine group is a two-dimensional, connected algebraic group

$$\mathbb{A}\mathrm{ff}(K) = \mathbb{G}_{\mathrm{a}}(K) \rtimes \mathbb{G}_{\mathrm{m}}(K) = \left\{ \begin{pmatrix} s & a \\ 0 & 1 \end{pmatrix} : s \in K^{\times}, a \in K \right\}.$$

Undecidability in the affine group

- The affine group is a two-dimensional, connected algebraic group

$$\mathbb{A}\mathrm{ff}(K) = \mathbb{G}_{\mathrm{a}}(K) \rtimes \mathbb{G}_{\mathrm{m}}(K) = \left\{ \begin{pmatrix} s & a \\ 0 & 1 \end{pmatrix} : s \in K^{\times}, a \in K \right\}.$$

- Group Configuration Theorem works in rank two but requires work to get $\mathbb{A}\mathrm{ff}$.

Undecidability in the affine group

- The affine group is a two-dimensional, connected algebraic group

$$\mathbb{A}\mathrm{ff}(K) = \mathbb{G}_{\mathrm{a}}(K) \rtimes \mathbb{G}_{\mathrm{m}}(K) = \left\{ \begin{pmatrix} s & a \\ 0 & 1 \end{pmatrix} : s \in K^{\times}, a \in K \right\}.$$

- Group Configuration Theorem works in rank two but requires work to get $\mathbb{A}\mathrm{ff}$.

Helpful facts about $\mathbb{A}\mathrm{ff}$

- $\mathbb{G}_{\mathrm{a}}$ is the smallest non-trivial normal subgroup. It is $[\mathbb{A}\mathrm{ff}, \mathbb{A}\mathrm{ff}]$ and characteristic.

Undecidability in the affine group

- The affine group is a two-dimensional, connected algebraic group

$$\mathbb{A}\mathrm{ff}(K) = \mathbb{G}_{\mathrm{a}}(K) \rtimes \mathbb{G}_{\mathrm{m}}(K) = \left\{ \begin{pmatrix} s & a \\ 0 & 1 \end{pmatrix} : s \in K^{\times}, a \in K \right\}.$$

- Group Configuration Theorem works in rank two but requires work to get $\mathbb{A}\mathrm{ff}$.

Helpful facts about $\mathbb{A}\mathrm{ff}$

- $\mathbb{G}_{\mathrm{a}}$ is the smallest non-trivial normal subgroup. It is $[\mathbb{A}\mathrm{ff}, \mathbb{A}\mathrm{ff}]$ and characteristic.
- Any two complements of $\mathbb{G}_{\mathrm{a}}$ in $\mathbb{A}\mathrm{ff}$ are conjugate.

Undecidability in the affine group

- The affine group is a two-dimensional, connected algebraic group

$$\mathbb{A}\mathrm{ff}(K) = \mathbb{G}_{\mathrm{a}}(K) \rtimes \mathbb{G}_{\mathrm{m}}(K) = \left\{ \begin{pmatrix} s & a \\ 0 & 1 \end{pmatrix} : s \in K^{\times}, a \in K \right\}.$$

- Group Configuration Theorem works in rank two but requires work to get $\mathbb{A}\mathrm{ff}$.

Helpful facts about $\mathbb{A}\mathrm{ff}$

- $\mathbb{G}_{\mathrm{a}}$ is the smallest non-trivial normal subgroup. It is $[\mathbb{A}\mathrm{ff}, \mathbb{A}\mathrm{ff}]$ and characteristic.
- Any two complements of $\mathbb{G}_{\mathrm{a}}$ in $\mathbb{A}\mathrm{ff}$ are conjugate.

- $\mathbb{A}\mathrm{ff}$ is not abelian, so no more skew field or projective geometry.

Undecidability in the affine group

- The affine group is a two-dimensional, connected algebraic group

$$\mathbb{A}\mathrm{ff}(K) = \mathbb{G}_{\mathrm{a}}(K) \rtimes \mathbb{G}_{\mathrm{m}}(K) = \left\{ \begin{pmatrix} s & a \\ 0 & 1 \end{pmatrix} : s \in K^{\times}, a \in K \right\}.$$

- Group Configuration Theorem works in rank two but requires work to get $\mathbb{A}\mathrm{ff}$.

Helpful facts about $\mathbb{A}\mathrm{ff}$

- $\mathbb{G}_{\mathrm{a}}$ is the smallest non-trivial normal subgroup. It is $[\mathbb{A}\mathrm{ff}, \mathbb{A}\mathrm{ff}]$ and characteristic.
- Any two complements of $\mathbb{G}_{\mathrm{a}}$ in $\mathbb{A}\mathrm{ff}$ are conjugate.

- $\mathbb{A}\mathrm{ff}$ is not abelian, so no more skew field or projective geometry.
- Instead, there is a group of definable automorphisms through which the coordinate skew fields of $\mathbb{G}_{\mathrm{a}}$ and $\mathbb{G}_{\mathrm{m}}$ can interact.

Undecidability in the affine group

- Using von Staudt for $\mathbb{G}_m$ we can describe an automorphism of $\mathbb{A}$ff which:

Undecidability in the affine group

- Using von Staudt for $\mathbb{G}_{\mathsf{m}}$ we can describe an automorphism of $\mathbb{A}\mathrm{ff}$ which:
  - projects to $p \in \mathbb{Q} = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_{\mathsf{m}})$ acting as $s \mapsto s^p$ (the Frobenius), and

Undecidability in the affine group

- Using von Staudt for $\mathbb{G}_{\mathsf{m}}$ we can describe an automorphism of $\mathbb{A}\mathrm{ff}$ which:
  - projects to $p \in \mathbb{Q} = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_{\mathsf{m}})$ acting as $s \mapsto s^p$ (the Frobenius), and
  - thus restricts to $c\sigma \in \overline{\mathbb{F}_p}(\sigma) = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_{\mathsf{a}})$ for some $c \in \overline{\mathbb{F}_p}^{\times}$.

Undecidability in the affine group

- Using von Staudt for $\mathbb{G}_{\mathsf{m}}$ we can describe an automorphism of $\mathbb{A}\mathrm{ff}$ which:
  - projects to $p \in \mathbb{Q} = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_{\mathsf{m}})$ acting as $s \mapsto s^p$ (the Frobenius), and
  - thus restricts to $c\sigma \in \overline{\mathbb{F}_p}(\sigma) = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_{\mathsf{a}})$ for some $c \in \overline{\mathbb{F}_p}^{\times}$.

This smuggles Frobenius from $\mathbb{G}_{\mathsf{m}}$ via $\mathbb{A}\mathrm{ff}$ into $\mathbb{G}_{\mathsf{a}}$.

Undecidability in the affine group

- Using von Staudt for $\mathbb{G}_{\mathsf{m}}$ we can describe an automorphism of $\mathbb{A}\mathrm{ff}$ which:
  - projects to $p \in \mathbb{Q} = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_{\mathsf{m}})$ acting as $s \mapsto s^p$ (the Frobenius), and
  - thus restricts to $c\sigma \in \overline{\mathbb{F}_p}(\sigma) = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_{\mathsf{a}})$ for some $c \in \overline{\mathbb{F}_p}^{\times}$.

This smuggles Frobenius from $\mathbb{G}_{\mathsf{m}}$ via $\mathbb{A}\mathrm{ff}$ into $\mathbb{G}_{\mathsf{a}}$.

- The centralizer of $c\sigma$ in $\overline{\mathbb{F}_p}(\sigma)$ is $\mathbb{F}_p(c\sigma)$.

Undecidability in the affine group

- Using von Staudt for $\mathbb{G}_{\mathsf{m}}$ we can describe an automorphism of $\mathbb{A}\mathrm{ff}$ which:
  - projects to $p \in \mathbb{Q} = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_{\mathsf{m}})$ acting as $s \mapsto s^p$ (the Frobenius), and
  - thus restricts to $c\sigma \in \overline{\mathbb{F}_p}(\sigma) = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_{\mathsf{a}})$ for some $c \in \overline{\mathbb{F}_p}^{\times}$.

This smuggles Frobenius from $\mathbb{G}_{\mathsf{m}}$ via $\mathbb{A}\mathrm{ff}$ into $\mathbb{G}_{\mathsf{a}}$.

- The centralizer of $c\sigma$ in $\overline{\mathbb{F}_p}(\sigma)$ is $\mathbb{F}_p(c\sigma)$.
- We get an existential definition of the field $\mathbb{F}_p(t)$ with a distinguished generator t.

Undecidability in the affine group

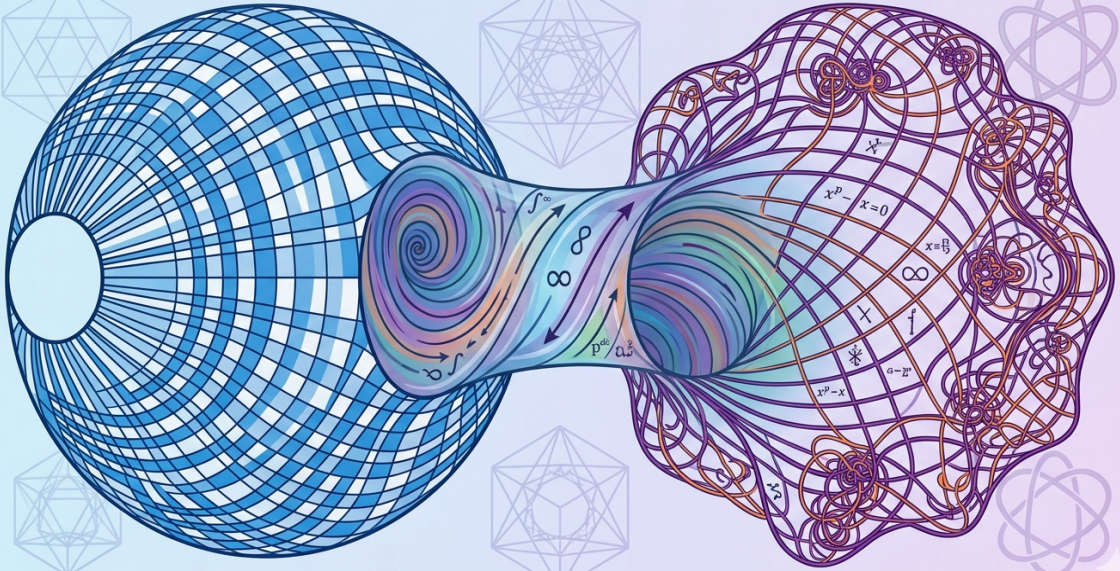
- Using von Staudt for $\mathbb{G}_\mathsf{m}$ we can describe an automorphism of $\mathbb{A}\mathrm{ff}$ which:
  - projects to $p \in \mathbb{Q} = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_\mathsf{m})$ acting as $s \mapsto s^p$ (the Frobenius), and
  - thus restricts to $c\sigma \in \overline{\mathbb{F}_p}(\sigma) = L_{\overline{\mathbb{F}_p}}(\mathbb{G}_\mathsf{a})$ for some $c \in \overline{\mathbb{F}_p}^\times$.

This smuggles Frobenius from $\mathbb{G}_\mathsf{m}$ via $\mathbb{A}\mathrm{ff}$ into $\mathbb{G}_\mathsf{a}$.

- The centralizer of $c\sigma$ in $\overline{\mathbb{F}_p}(\sigma)$ is $\mathbb{F}_p(c\sigma)$.
- We get an existential definition of the field $\mathbb{F}_p(t)$ with a distinguished generator t.

Pheidas (1991) & Videla (1994)

The existential theory of the field $\mathbb{F}_p(t)$ with named generator t is undecidable.



References I

[EH91] David M. Evans and Ehud Hrushovski. "Projective planes in algebraically closed fields". In: *Proc. Lond. Math. Soc. (3)* 62.1 (1991), pp. 1–24. DOI: 10.1112/plms/s3-62.1.1.

[Hru86] Ehud Hrushovski. "Contributions to stable model theory". PhD thesis. University of California, Berkeley, 1986.

[Ing71] Aubrey W. Ingleton. "Representation of matroids". In: *Combinatorial mathematics and its applications. Proceedings, Oxford, 1969*. Ed. by Dominic J. A. Welsh. Academic Press, 1971, pp. 149–167.

[Lin85] Bernt Lindström. "On the algebraic characteristic set for a class of matroids". In: *Proc. Am. Math. Soc.* 95 (1985), pp. 147–151. DOI: 10.2307/2045591.

[Lin89] Bernt Lindström. "Matroids algebraic over $F(t)$ are algebraic over F". In: *Combinatorica* 9.1 (1989), pp. 107–109. DOI: 10.1007/BF02122691.

[Mac36] Saunders MacLane. "Some interpretations of abstract linear dependence in terms of projective geometry". In: *Amer. J. Math.* 58.1 (1936), pp. 236–240.

[Phe91] Thanases Pheidas. "Hilbert's tenth problem for fields of rational functions over finite fields". In: *Invent. Math.* 103.1 (1991), pp. 1–8. DOI: 10.1007/BF01239506.

References II

[Pif69] Michael J. Piff. "The representability of matroids". Diploma thesis. University of Oxford, 1969.

[Pif72] Michael J. Piff. "Some problems in combinatorial theory". PhD thesis. University of Oxford, 1972.

[Sta57] Karl Georg Christian von Staudt. *Beiträge zur Geometrie der Lage. 2. Heft*. Bauer und Raspe Nürnberg, 1857.

[Vid94] Carlos R. Videla. "Hilbert's tenth problem for rational function fields in characteristic 2". In: *Proc. Am. Math. Soc.* 120.1 (1994), pp. 249–253. DOI: 10.2307/2160192.