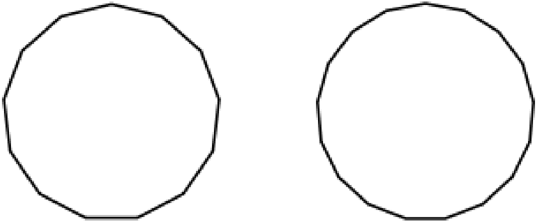
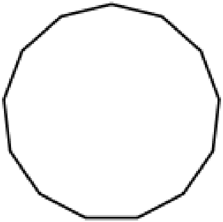
Introduction to anabelian geometry

July 2014

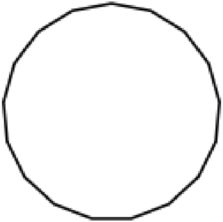
Is there a difference?



Is there a difference?



13



17

Construction of regular polygons

Gauss (1796): A regular n-gon is constructible with compass and straightedge iff $n = 2^m \cdot p$, where p is a Fermat prime, i.e., $p = 2^{2^n} + 1$; first such primes are $3, 5, 17, 257, 65537, \ldots$

Construction of regular polygons

Gauss (1796): A regular n-gon is constructible with compass and straightedge iff $n = 2^m \cdot p$, where p is a Fermat prime, i.e., $p = 2^{2^n} + 1$; first such primes are $3, 5, 17, 257, 65537, \dots$

F. Richelot (1832): Explicit construction of the 257-gon

Construction of regular polygons

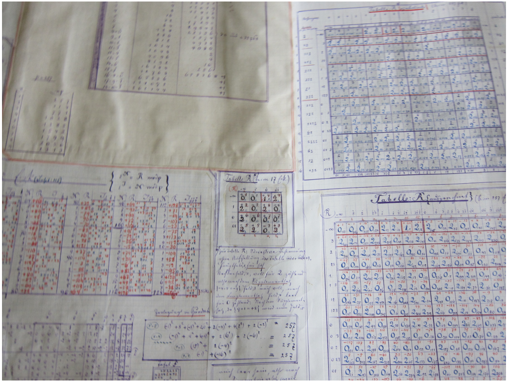
Gauss (1796): A regular n-gon is constructible with compass and straightedge iff $n = 2^m \cdot p$, where p is a Fermat prime, i.e., $p = 2^{2^n} + 1$; first such primes are $3, 5, 17, 257, 65537, \ldots$

F. Richelot (1832): Explicit construction of the 257-gon

J. Hermes (1894): Explicit construction of the 65537-gon, 10 years of work...

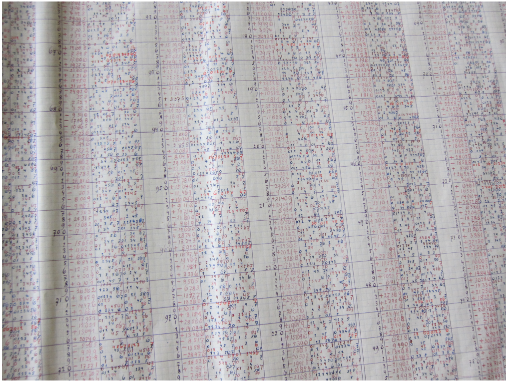
Construction of regular polygons

Construction of regular polygons



Construction of regular polygons

Construction of regular polygons



Galois groups

Let K be a field, e.g., $K = \mathbb{Q}$, and

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x]$$

a polynomial with coefficients in K. Let $L \subset \bar{K}$ be the smallest subfield of an algebraic closure of K containing all roots of f. The Galois group

$$\mathrm{Gal}(f) = \mathrm{Gal}(L/K) \subseteq \mathfrak{S}_n$$

is the group of automorphisms of L fixing K. It is a subgroup of the symmetric group exchanging the roots of f.

Galois groups

Let K be a field, e.g., $K = \mathbb{Q}$, and

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x]$$

a polynomial with coefficients in K. Let $L \subset \bar{K}$ be the smallest subfield of an algebraic closure of K containing all roots of f. The Galois group

$$\mathrm{Gal}(f) = \mathrm{Gal}(L/K) \subseteq \mathfrak{S}_n$$

is the group of automorphisms of L fixing K. It is a subgroup of the symmetric group exchanging the roots of f. It can be effectively computed, e.g.,

- $\mathrm{Gal}(x^5 - 5x + 5/2) = \mathfrak{S}_5$

Galois groups

Let K be a field, e.g., $K = \mathbb{Q}$, and

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x]$$

a polynomial with coefficients in K. Let $L \subset \bar{K}$ be the smallest subfield of an algebraic closure of K containing all roots of f. The Galois group

$$\mathrm{Gal}(f) = \mathrm{Gal}(L/K) \subseteq \mathfrak{S}_n$$

is the group of automorphisms of L fixing K. It is a subgroup of the symmetric group exchanging the roots of f. It can be effectively computed, e.g.,

- $\mathrm{Gal}(x^5 - 5x + 5/2) = \mathfrak{S}_5$
- $\mathrm{Gal}(x^{16} + x^{15} + \cdots + x + 1) = (\mathbb{Z}/17\mathbb{Z})^\times \simeq \mathbb{Z}/16\mathbb{Z}$, this is why the 17-gon is constructible with compass and straightedge

Computing the Galois group

Dedekind

Let $f \in \mathbb{Z}[x]$ be a monic polynomial and p a prime. If

$$f(x) \equiv f_1(x) \cdots f_r(x) \pmod{p}$$

then $\mathrm{Gal}(f)$ contains a permutation σ that is a product of r cycles of length $n_i := \deg(f_i)$.

Computing the Galois group

Let $f_1, f_2, f_3 \in \mathbb{Z}[x]$ be monic, of degree n, with

- f_1 irreducible (mod 2)
- $f_2 = (\text{linear}) \cdot (\text{irreducible})$ (mod 3)
- $f_3 = (\text{degree } 2) \cdot \begin{pmatrix} \text{product of one or two irreducible} \\ \text{polynomials of odd degree} \end{pmatrix}$ (mod 5)

Put

$$f := -15f_1 + 10f_2 + 6f_3.$$

Then $\mathrm{Gal}(f) = \mathfrak{S}_n$.

Computing the Galois group

Let $f_1, f_2, f_3 \in \mathbb{Z}[x]$ be monic, of degree n, with

- f_1 irreducible (mod 2)
- $f_2 = (\text{linear}) \cdot (\text{irreducible})$ (mod 3)
- $f_3 = (\text{degree } 2) \cdot \left(\begin{array}{l}\text{product of one or two irreducible} \\ \text{polynomials of odd degree}\end{array}\right)$ (mod 5)

Put

$$f := -15 f_1 + 10 f_2 + 6 f_3.$$

Then $\mathrm{Gal}(f) = \mathfrak{S}_n$.
We see that already few primes determine the Galois group.

Reciprocity

Problem

Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial. How does it behave when reduced modulo p?

Reciprocity

Problem

Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial. How does it behave when reduced modulo p?

Example

$$x^{q-1} + \cdots + x + 1 = \prod_{j=1}^{q-1} (x - \alpha_j) \pmod{p} \text{ iff } p = 1 \pmod{q}.$$

Reciprocity

Problem

Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial. How does it behave when reduced modulo p?

Example

$$x^{q-1} + \cdots + x + 1 = \prod_{j=1}^{q-1} (x - \alpha_j) \pmod{p} \text{ iff } p = 1 \pmod{q}.$$

Example

$$x^4 - 2 = \prod_{j=1}^{4} (x - \alpha_j) \pmod{p} \text{ iff } a_p \equiv 2 \pmod{3},$$

for an explicit modular form $\sum_{n \geq 1} a_n q^n$ of weight 2 and level 768.

Plan

- Fields and projective geometry

Plan

- Fields and projective geometry
- Milnor K-theory and Galois cohomology

Plan

- Fields and projective geometry
- Milnor K-theory and Galois cohomology
- Almost Abelian Anabelian geometry - Bogomolov's program

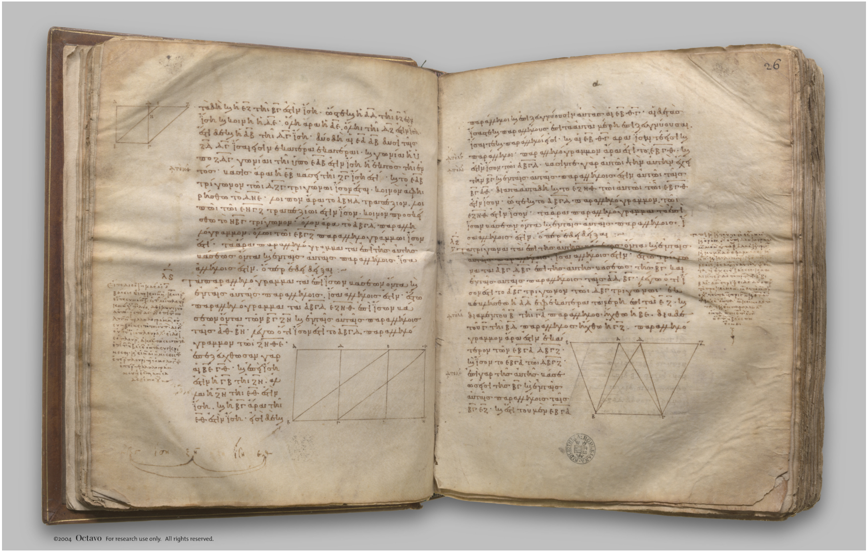
Plan

- Fields and projective geometry
- Milnor K-theory and Galois cohomology
- Almost Abelian Anabelian geometry - Bogomolov's program
- Proofs: main steps

Plan

- Fields and projective geometry
- Milnor K-theory and Galois cohomology
- Almost Abelian Anabelian geometry - Bogomolov's program
- Proofs: main steps
- Applications

Euclid (Elements, Book I)



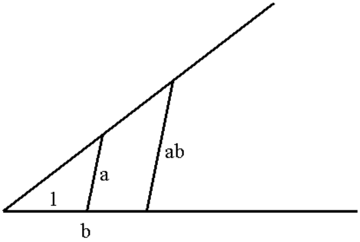
What is a field, geometrically?

Addition:

What is a field, geometrically?

Addition:

Multiplication:



More on projective geometry: axiomatization

- Steiner 1832: *Durch gehörige Aneignung der wenigen Grundbeziehungen macht man sich zum Herrn des ganzen Gegenstandes; es tritt Ordnung in das Chaos ein, und man sieht, wie alle Theile naturgemäss ineinander greifen, in schönster Ordnung sich in Reihen stellen ...*

More on projective geometry: axiomatization

- Steiner 1832: *Durch gehörige Aneignung der wenigen Grundbeziehungen macht man sich zum Herrn des ganzen Gegenstandes; es tritt Ordnung in das Chaos ein, und man sieht, wie alle Theile naturgemäss ineinander greifen, in schönster Ordnung sich in Reihen stellen ...*
- Staudt 1847: *Ich habe in dieser Schrift versucht, die Geometrie der Lage zu einer selbstständigen Wissenschaft zu machen, welche des Messens nicht bedarf.*

More on projective geometry: axiomatization

- Steiner 1832: *Durch gehörige Aneignung der wenigen Grundbeziehungen macht man sich zum Herrn des ganzen Gegenstandes; es tritt Ordnung in das Chaos ein, und man sieht, wie alle Theile naturgemäss ineinander greifen, in schönster Ordnung sich in Reihen stellen ...*
- Staudt 1847: *Ich habe in dieser Schrift versucht, die Geometrie der Lage zu einer selbstständigen Wissenschaft zu machen, welche des Messens nicht bedarf.*
- Klein, Pasch, Pieri, ...

More on projective geometry: axiomatization

- Steiner 1832: *Durch gehörige Aneignung der wenigen Grundbeziehungen macht man sich zum Herrn des ganzen Gegenstandes; es tritt Ordnung in das Chaos ein, und man sieht, wie alle Theile naturgemäss ineinander greifen, in schönster Ordnung sich in Reihen stellen ...*
- Staudt 1847: *Ich habe in dieser Schrift versucht, die Geometrie der Lage zu einer selbstständigen Wissenschaft zu machen, welche des Messens nicht bedarf.*
- Klein, Pasch, Pieri, ...
- Schur: proof of the fundamental theorem of projective geometry from incidence axioms, Desargues and Pappus axiom

More on projective geometry: axiomatization

- Steiner 1832: *Durch gehörige Aneignung der wenigen Grundbeziehungen macht man sich zum Herrn des ganzen Gegenstandes; es tritt Ordnung in das Chaos ein, und man sieht, wie alle Theile naturgemäss ineinander greifen, in schönster Ordnung sich in Reihen stellen ...*
- Staudt 1847: *Ich habe in dieser Schrift versucht, die Geometrie der Lage zu einer selbstständigen Wissenschaft zu machen, welche des Messens nicht bedarf.*
- Klein, Pasch, Pieri, ...
- Schur: proof of the fundamental theorem of projective geometry from incidence axioms, Desargues and Pappus axiom
- Hessenberg: Desargues follows from Pappus

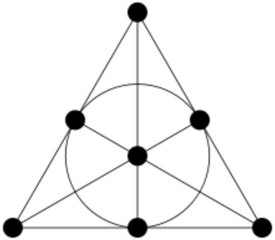
More on projective geometry: axiomatization

- Steiner 1832: *Durch gehörige Aneignung der wenigen Grundbeziehungen macht man sich zum Herrn des ganzen Gegenstandes; es tritt Ordnung in das Chaos ein, und man sieht, wie alle Theile naturgemäss ineinander greifen, in schönster Ordnung sich in Reihen stellen ...*
- Staudt 1847: *Ich habe in dieser Schrift versucht, die Geometrie der Lage zu einer selbstständigen Wissenschaft zu machen, welche des Messens nicht bedarf.*
- Klein, Pasch, Pieri, ...
- Schur: proof of the fundamental theorem of projective geometry from incidence axioms, Desargues and Pappus axiom
- Hessenberg: Desargues follows from Pappus
- Veblen 1910: *What we call general projective geometry is,* analytically, *the geometry associated with a general number field.*

More on projective geometry: axiomatization

- Steiner 1832: *Durch gehörige Aneignung der wenigen Grundbeziehungen macht man sich zum Herrn des ganzen Gegenstandes; es tritt Ordnung in das Chaos ein, und man sieht, wie alle Theile naturgemäss ineinander greifen, in schönster Ordnung sich in Reihen stellen ...*
- Staudt 1847: *Ich habe in dieser Schrift versucht, die Geometrie der Lage zu einer selbstständigen Wissenschaft zu machen, welche des Messens nicht bedarf.*
- Klein, Pasch, Pieri, ...
- Schur: proof of the fundamental theorem of projective geometry from incidence axioms, Desargues and Pappus axiom
- Hessenberg: Desargues follows from Pappus
- Veblen 1910: *What we call general projective geometry is,* analytically, *the geometry associated with a general number field.*
- Hilbert ... Klein: *When people run out of ideas they start axiomatizing.*

Fano plane



Universality theorems

Configuration spaces: moduli of finitely many points with specified alignments.

Universality theorems

Configuration spaces: moduli of finitely many points with specified alignments.

Mnëv 1988

Any scheme over $\mathbb{Z}$ arises as a configuration space of points in $\mathbb{P}^2$.

Universality theorems

Configuration spaces: moduli of finitely many points with specified alignments.

Mnëv 1988

Any scheme over $\mathbb{Z}$ arises as a configuration space of points in $\mathbb{P}^2$.

- Lafforgue 2002: singularities of certain strata in some moduli spaces arising in the Geometric Langlands Program, e.g., compactifications of $\mathrm{PGL}_r^{n+1}/\mathrm{PGL}_r$.

Universality theorems

Configuration spaces: moduli of finitely many points with specified alignments.

Mnëv 1988

Any scheme over $\mathbb{Z}$ arises as a configuration space of points in $\mathbb{P}^2$.

- Lafforgue 2002: singularities of certain strata in some moduli spaces arising in the Geometric Langlands Program, e.g., compactifications of $\mathrm{PGL}_r^{n+1}/\mathrm{PGL}_r$.
- Vakil: Murphy's law - badly behaved moduli spaces, e.g., Hilbert schemes of smooth curves in projective space, surfaces in $\mathbb{P}^4$, etc.

Undecidability in Euclidean geometry

Harvey Friedman

There is a shortage of elementary decision problems known to be recursively unsolvable. Here we give an example from Euclidean geometry that is "almost linear" and potentially meaningful in high school.

We work entirely in the Euclidean plane, $\mathbb{R}^2$. A line is a line in $\mathbb{R}^2$ which extends infinitely in both directions. A rational line is a line with two distinct points whose coordinates are rational.

Let $L_1, ..., L_k$ and $L'_1, ..., L'_r$ be lines. We say that $L_1, ..., L_k$ is equivalent to $L'_1, ..., L'_r$ if and only if $k = r$, and for all $1 \leq i_1, ..., i_p \leq k$, $L_{i_1}, ..., L_{i_p}$ have a common point if and only if $L'_{i_1}, ..., L'_{i_p}$ have a common point.

Undecidability in Euclidean geometry

Theorem (H. Friedman, May 2009)

The following problem is not algorithmically solvable: Is a given finite sequence of rational lines equivalent to a finite sequence of rational lines whose intersection points are integral and include $(0,0),(0,1)$?

Universality theorems

```
to Harvey Friedman <friedman@math.ohio-state.edu>
cc Karl Rubin <krubin@math.uci.edu>,
Yuri Tschinkel <tschinkel@cims.nyu.edu>
date Tue, May 5, 2009 at 8:28 AM
```

Harvey,

This is great, and interests me (and I'm sure interests Karl Rubin) a lot, since it might connect with our recent work. Do you have the analogous theorem when you replace H10P over $\mathbb{Z}$ by H10P over the ring of integers of a number field K, and simultaneously "rational" and "integral" by "rational over K" and "in the ring of integers of K"?

Barry

Projective geometry: axiomatization

Definition

A projective structure is a pair $(S, \mathfrak{L})$ where S is a (nonempty) set (of points) and $\mathfrak{L}$ a collection of subsets $\mathfrak{l} \subset S$ (lines) such that

P1 there exist an $s \in S$ and an $\mathfrak{l} \in \mathfrak{L}$ such that $s \notin \mathfrak{l}$;

P2 for every $\mathfrak{l} \in \mathfrak{L}$ there exist at least three distinct $s, s', s'' \in \mathfrak{l}$;

P3 for every pair of distinct $s, s' \in S$ there exists exactly one

$$\mathfrak{l} = \mathfrak{l}(s, s') \in \mathfrak{L}$$

such that $s, s' \in \mathfrak{l}$;

P4 for every quadruple of pairwise distinct $s, s', t, t' \in S$ one has

$$\mathfrak{l}(s, s') \cap \mathfrak{l}(t, t') \neq \emptyset \ \Rightarrow \ \mathfrak{l}(s, t) \cap \mathfrak{l}(s', t') \neq \emptyset.$$

Axioms

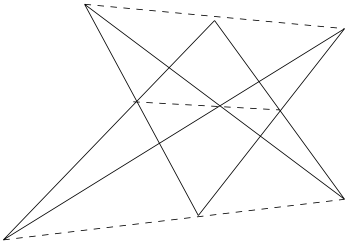
A morphism of projective structures $\rho : (S, \mathfrak{L}) \to (S', \mathfrak{L}')$ is a map of sets $\rho : S \to S'$ preserving lines, i.e., $\rho(\mathfrak{l}) \in \mathfrak{L}'$, for all $\mathfrak{l} \in \mathfrak{L}$.

Axioms

A morphism of projective structures $\rho : (S, \mathfrak{L}) \rightarrow (S', \mathfrak{L}')$ is a map of sets $\rho : S \rightarrow S'$ preserving lines, i.e., $\rho(\mathfrak{l}) \in \mathfrak{L}'$, for all $\mathfrak{l} \in \mathfrak{L}$.

A projective structure $(S, \mathfrak{L})$ satisfies *Pappus' axiom* if

PA for all 2-dimensional subspaces and every configuration of six points and lines in these subspaces as below



the intersections are collinear.

Fundamental theorem

Reconstruction

Let $(S, \mathfrak{L})$ be a projective structure of dimension $n \geq 2$ which satisfies Pappus' axiom. Then there exists a vector space V over a field k and an isomorphism

$$\sigma : \mathbb{P}_k(V) \xrightarrow{\sim} S.$$

Moreover, for any two such triples (V, k, σ) and (V', k', σ') there is an isomorphism

$$V/k \xrightarrow{\sim} V'/k'$$

compatible with σ, σ' and unique up to homothety $v \mapsto \lambda v$, $\lambda \in k^\times$.

Main example

Let k be a field and $\mathbb{P}^n$ the usual projective space over k of dimension $n \geq 2$. Then $\mathbb{P}^n(k)$ carries a projective structure: lines are the usual projective lines $\mathbb{P}^1(k) \subset \mathbb{P}^n(k)$.

Main example

Let k be a field and $\mathbb{P}^n$ the usual projective space over k of dimension $n \geq 2$. Then $\mathbb{P}^n(k)$ carries a projective structure: lines are the usual projective lines $\mathbb{P}^1(k) \subset \mathbb{P}^n(k)$.

Let K/k be an extension of fields. Then

$$S := \mathbb{P}_k(K) = (K \setminus 0)/k^\times$$

carries a natural (possibly, infinite-dimensional) projective structure.

Main example

Let k be a field and $\mathbb{P}^n$ the usual projective space over k of dimension $n \geq 2$. Then $\mathbb{P}^n(k)$ carries a projective structure: lines are the usual projective lines $\mathbb{P}^1(k) \subset \mathbb{P}^n(k)$.

Let K/k be an extension of fields. Then

$$S := \mathbb{P}_k(K) = (K \setminus 0)/k^\times$$

carries a natural (possibly, infinite-dimensional) projective structure.
Multiplication in $K^\times/k^\times$ preserves this structure.

Main theorem

Reconstructing fields

Let K/k and K'/k' be field extensions of degree ≥ 3 and

$$\bar{\psi} : S = \mathbb{P}_k(K) \to \mathbb{P}_{k'}(K') = S'$$

a bijection of sets which is an isomorphism of abelian groups and of projective structures. Then

$$k \simeq k' \quad \text{and} \quad K \simeq K'.$$

Pregeometries and geometries

Pregeometries and geometries

A combinatorial pregeometry (finitary matroid) is a pair $(\mathcal{P}, cl)$ where $\mathcal{P}$ is a set and

$$cl\ :\ \mathrm{Subsets}(\mathcal{P}) \to \mathrm{Subsets}(\mathcal{P}),$$

such that for all $a, b \in \mathcal{P}$ and all $Y, Z \subseteq \mathcal{P}$ one has:

- $Y \subseteq cl(Y)$,
- if $Y \subseteq Z$, then $cl(Y) \subseteq cl(Z)$,
- $cl(cl(Y)) = cl(Y)$,
- if $a \in cl(Y)$, then there is a finite subset $Y' \subset Y$ such that $a \in cl(Y')$ (finite character),
- (exchange condition) if $a \in cl(Y \cup \{b\}) \setminus cl(Y)$, then $b \in cl(Y \cup \{a\})$.

Pregeometries and geometries

A combinatorial pregeometry (finitary matroid) is a pair $(\mathcal{P}, cl)$ where $\mathcal{P}$ is a set and

$$cl : \mathrm{Subsets}(\mathcal{P}) \to \mathrm{Subsets}(\mathcal{P}),$$

such that for all $a, b \in \mathcal{P}$ and all $Y, Z \subseteq \mathcal{P}$ one has:

- $Y \subseteq cl(Y)$,
- if $Y \subseteq Z$, then $cl(Y) \subseteq cl(Z)$,
- $cl(cl(Y)) = cl(Y)$,
- if $a \in cl(Y)$, then there is a finite subset $Y' \subset Y$ such that $a \in cl(Y')$ (finite character),
- (exchange condition) if $a \in cl(Y \cup \{b\}) \setminus cl(Y)$, then $b \in cl(Y \cup \{a\})$.

A geometry is a pregeometry such that $cl(a) = a$, for all $a \in \mathcal{P}$, and $cl(\emptyset) = \emptyset$.

Examples

1. $\mathcal{P} = V/k$, a vector space over a field k and $cl(Y)$ the k-span of $Y \subset \mathcal{P}$

Examples

1. $\mathcal{P} = V/k$, a vector space over a field k and $cl(Y)$ the k-span of $Y \subset \mathcal{P}$
2. $\mathcal{P} = \mathbb{P}_k(V)$, the usual projective space over a k

Examples

1. $\mathcal{P} = V/k$, a vector space over a field k and $cl(Y)$ the k-span of $Y \subset \mathcal{P}$
2. $\mathcal{P} = \mathbb{P}_k(V)$, the usual projective space over a k
3. $\mathcal{P} = \mathcal{P}_k(K)$, a field K containing an algebraically closed subfield k and $cl(Y)$ - the normal closure of $k(Y)$ in K;

Examples

1. $\mathcal{P} = V/k$, a vector space over a field k and $cl(Y)$ the k-span of $Y \subset \mathcal{P}$
2. $\mathcal{P} = \mathbb{P}_k(V)$, the usual projective space over a k
3. $\mathcal{P} = \mathcal{P}_k(K)$, a field K containing an algebraically closed subfield k and $cl(Y)$ - the normal closure of $k(Y)$ in K; a geometry is obtained after factoring by $x \sim y$ iff $cl(x) = cl(y)$.

Combinatorial geometries of field extensions

Evans–Hrushovski 1991 / Gismatullin 2008

Let k and k' be algebraically closed fields, K/k and K'/k' field extensions of transcendence degree ≥ 5 over k, resp. k'. Then, every isomorphism of combinatorial geometries

$$\mathcal{P}_k(K) \to \mathcal{P}_{k'}(K')$$

is induced by an isomorphism of separable closures

$$\bar{K} \to \bar{K}'.$$

K-theory

Let $\mathrm{K}_i^M(K)$ be i-th Milnor K-group of a field K. Recall that

$$\mathrm{K}_1^M(K) = K^\times$$

and that there is a canonical surjective homomorphism

$$\sigma_K : \mathrm{K}_1^M(K) \otimes \mathrm{K}_1^M(K) \to \mathrm{K}_2^M(K)$$

whose kernel is generated by symbols $(x, 1-x)$, for $x \in K^\times \setminus 1$.

K-theory

Let $\mathrm{K}_i^M(K)$ be i-th Milnor K-group of a field K. Recall that

$$\mathrm{K}_1^M(K) = K^\times$$

and that there is a canonical surjective homomorphism

$$\sigma_K \,:\, \mathrm{K}_1^M(K) \otimes \mathrm{K}_1^M(K) \to \mathrm{K}_2^M(K)$$

whose kernel is generated by symbols $(x, 1-x)$, for $x \in K^\times \setminus 1$.
Let

$$\bar{\mathrm{K}}_i^M(K) := \mathrm{K}_i^M(K)/\text{infinitely divisible}, \quad i = 1, 2.$$

Group cohomology

Let

$$\mathrm{H}^i(G, M)$$

be the i-cohomology group of a finite or profinite group G, with coefficients in a G-module M. Recall:

- $\mathrm{H}^0(G, M) = M^G$, the submodule of G-invariants;

Group cohomology

Let

$$\mathrm{H}^i(G, M)$$

be the *i*-cohomology group of a finite or profinite group G, with coefficients in a G-module M. Recall:

- $\mathrm{H}^0(G, M) = M^G$, the submodule of G-invariants;
- $\mathrm{H}^1(G, M) = \mathrm{Hom}(G, M)$, provided M has trivial G-action;

Group cohomology

Let

$$\mathrm{H}^i(G, M)$$

be the i-cohomology group of a finite or profinite group G, with coefficients in a G-module M. Recall:

- $\mathrm{H}^0(G, M) = M^G$, the submodule of G-invariants;
- $\mathrm{H}^1(G, M) = \mathrm{Hom}(G, M)$, provided M has trivial G-action;
- $\mathrm{H}^2(G, M)$ classifies central extensions

$$1 \to M \to \tilde{G} \to G \to 1,$$

Group cohomology

Let

$$\mathrm{H}^i(G, M)$$

be the i-cohomology group of a finite or profinite group G, with coefficients in a G-module M. Recall:

- $\mathrm{H}^0(G, M) = M^G$, the submodule of G-invariants;
- $\mathrm{H}^1(G, M) = \mathrm{Hom}(G, M)$, provided M has trivial G-action;
- $\mathrm{H}^2(G, M)$ classifies central extensions

$$1 \to M \to \tilde{G} \to G \to 1,$$

For $M = \mathbb{Q}/\mathbb{Z}$ this group is called the Schur multiplier.

Group cohomology

Let

$$\mathrm{H}^i(G, M)$$

be the i-cohomology group of a finite or profinite group G, with coefficients in a G-module M. Recall:

- $\mathrm{H}^0(G, M) = M^G$, the submodule of G-invariants;
- $\mathrm{H}^1(G, M) = \mathrm{Hom}(G, M)$, provided M has trivial G-action;
- $\mathrm{H}^2(G, M)$ classifies central extensions

$$1 \to M \to \tilde{G} \to G \to 1,$$

For $M = \mathbb{Q}/\mathbb{Z}$ this group is called the Schur multiplier.

- if $M = \mathbb{Z}/\ell^n$ and $\mathfrak{S}_\ell(G) \subset G$ is the ℓ-Sylow subgroup then

$$\mathrm{H}^i(G, M) \hookrightarrow \mathrm{H}^i(\mathfrak{S}_\ell(G), M), \qquad \text{for all} \qquad i \geq 0$$

Group cohomology

We work with constant coefficients $M = \mathbb{Z}/\ell^n$, for some prime ℓ, trivial G-action, and write

$$\mathrm{H}^*(G) = \mathrm{H}^*(G, \mathbb{Z}/\ell^n).$$

Group cohomology

We work with constant coefficients $M = \mathbb{Z}/\ell^n$, for some prime ℓ, trivial G-action, and write

$$\mathrm{H}^*(G) = \mathrm{H}^*(G, \mathbb{Z}/\ell^n).$$

Example

$$\mathrm{H}^*((\mathbb{Z}/2)^r, \mathbb{F}_2) = \mathbb{F}_2[x_1, \dots, x_r], \quad \deg(x_j) = 1$$

Group cohomology

We work with constant coefficients $M = \mathbb{Z}/\ell^n$, for some prime ℓ, trivial G-action, and write

$$\mathrm{H}^*(G) = \mathrm{H}^*(G, \mathbb{Z}/\ell^n).$$

Example

$$\mathrm{H}^*((\mathbb{Z}/2)^r, \mathbb{F}_2) = \mathbb{F}_2[x_1, \ldots, x_r], \quad \deg(x_j) = 1$$

$$\mathrm{H}^*((\mathbb{Z}/\ell)^r, \mathbb{F}_\ell) = \wedge^*(x_1, \ldots, x_r) \otimes \mathbb{F}_\ell[y_1, \ldots, y_r],$$
$$\deg(x_j) = 1, \deg(y_j) = 2.$$

Galois cohomology

Let $K = k(X)$ be a function field over $k = \bar{\mathbb{F}}_p$, with $p \neq \ell$. Fix an isomorphism

$$\mu_{\ell^n} \simeq \mathbb{Z}/\ell^n.$$

- Kummer theory: $\mathrm{H}^1(G_K) = \mathrm{Hom}(G_K, \mathbb{Z}/\ell^n) = \mathrm{K}_1^{\mathrm{M}}(K)/\ell^n$

Galois cohomology

Let $K = k(X)$ be a function field over $k = \bar{\mathbb{F}}_p$, with $p \neq \ell$. Fix an isomorphism

$$\mu_{\ell^n} \simeq \mathbb{Z}/\ell^n.$$

- Kummer theory: $\mathrm{H}^1(G_K) = \mathrm{Hom}(G_K, \mathbb{Z}/\ell^n) = \mathrm{K}_1^{\mathrm{M}}(K)/\ell^n$
- Merkuriev-Suslin: $\mathrm{H}^2(G_K) = \mathrm{K}_2^{\mathrm{M}}(K)/\ell^n$

Galois cohomology

Let $K = k(X)$ be a function field over $k = \bar{\mathbb{F}}_p$, with $p \neq \ell$. Fix an isomorphism

$$\mu_{\ell^n} \simeq \mathbb{Z}/\ell^n.$$

- Kummer theory: $\mathrm{H}^1(G_K) = \mathrm{Hom}(G_K, \mathbb{Z}/\ell^n) = \mathrm{K}_1^{\mathrm{M}}(K)/\ell^n$
- Merkuriev-Suslin: $\mathrm{H}^2(G_K) = \mathrm{K}_2^{\mathrm{M}}(K)/\ell^n = \mathrm{Br}(K)[\ell^n]$

Galois cohomology

Let $K = k(X)$ be a function field over $k = \bar{\mathbb{F}}_p$, with $p \neq \ell$. Fix an isomorphism

$$\mu_{\ell^n} \simeq \mathbb{Z}/\ell^n.$$

- Kummer theory: $\mathrm{H}^1(G_K) = \mathrm{Hom}(G_K, \mathbb{Z}/\ell^n) = \mathrm{K}_1^{\mathrm{M}}(K)/\ell^n$
- Merkuriev-Suslin: $\mathrm{H}^2(G_K) = \mathrm{K}_2^{\mathrm{M}}(K)/\ell^n = \mathrm{Br}(K)[\ell^n]$
- Voevodsky, Rost, Weibel: $\mathrm{H}^n(G_K) = \mathrm{K}_n^{\mathrm{M}}(K)/\ell^n$

Reconstructing fields

Let K and L be function fields of transcendence degree ≥ 2 over algebraically closed fields k and l. Assume there exist isomorphisms

$$\bar{\psi}_i : \bar{\mathrm{K}}_i^M(K) \to \bar{\mathrm{K}}_i^M(L), \quad i = 1, 2,$$

of abelian groups with a commutative diagram

$$\begin{array}{ccc} \bar{\mathrm{K}}_1^M(K) \otimes \bar{\mathrm{K}}_1^M(K) & \xrightarrow{\bar{\psi}_1 \otimes \bar{\psi}_1} & \bar{K}_1^M(L) \otimes \bar{\mathrm{K}}_1^M(L) \\ \downarrow \sigma_K & & \downarrow \sigma_L \\ \bar{\mathrm{K}}_2^M(K) & \xrightarrow[\bar{\psi}_2]{} & \bar{\mathrm{K}}_2^M(L). \end{array}$$

Reconstructing fields

Let K and L be function fields of transcendence degree ≥ 2 over algebraically closed fields k and l. Assume there exist isomorphisms

$$\bar{\psi}_i : \bar{\mathrm{K}}_i^M(K) \to \bar{\mathrm{K}}_i^M(L), \quad i = 1, 2,$$

of abelian groups with a commutative diagram

$$\begin{array}{ccc}
\bar{\mathrm{K}}_1^M(K) \otimes \bar{\mathrm{K}}_1^M(K) & \xrightarrow{\bar{\psi}_1 \otimes \bar{\psi}_1} & \bar{K}_1^M(L) \otimes \bar{\mathrm{K}}_1^M(L) \\
\downarrow \sigma_K & & \downarrow \sigma_L \\
\bar{\mathrm{K}}_2^M(K) & \xrightarrow[\bar{\psi}_2]{} & \bar{\mathrm{K}}_2^M(L).
\end{array}$$

Bogomolov-T. 2008

Then there exists a (compatible) isomorphism of fields

$$\psi : K \to L.$$

Sketch of proof

The ground field: Infinitely divisible elements

An element $f \in K^\times = \mathrm{K}_1^M(K)$ is infinitely divisible if and only if $f \in k^\times$. In particular,

$$\bar{\mathrm{K}}_1^M(K) = K^\times / k^\times.$$

Sketch of proof

1-dimensional subfields

Given a nonconstant $f_1 \in K^\times/k^\times$, we have

$$\mathrm{Ker}_2(f_1) = E^\times/k^\times,$$

where $E = \overline{k(f_1)}^K$ is the normal closure in K of the 1-dimensional field generated by f_1 and

$$\mathrm{Ker}_2(f) := \{\, g \in K^\times/k^\times = \bar{\mathrm{K}}_1^M(K) \mid (f,g) = 0 \in \bar{\mathrm{K}}_2^M(K) \,\}.$$

Sketch of proof

Reconstructing lines: Functional equations

Projective lines are intersections of well-chosen infinite-dimensional projective subspaces $\mathbb{P}(E_1), \mathbb{P}(E_2)$, where $E_1, E_2 \subset K$ are 1-dimensional subfields.

Sketch of proof

Reconstructing lines: Functional equations

Projective lines are intersections of well-chosen infinite-dimensional projective subspaces $\mathbb{P}(E_1), \mathbb{P}(E_2)$, where $E_1, E_2 \subset K$ are 1-dimensional subfields. Precisely, assume that $x, y \in K^\times$ are algebraically independent.

Sketch of proof

Reconstructing lines: Functional equations

Projective lines are intersections of well-chosen infinite-dimensional projective subspaces $\mathbb{P}(E_1), \mathbb{P}(E_2)$, where $E_1, E_2 \subset K$ are 1-dimensional subfields. Precisely, assume that $x, y \in K^\times$ are algebraically independent. Let $p \in \overline{k(x)}^\times$, $q \in \overline{k(y)}^\times$ be such that x, y, p, q are multiplicatively independent in $K^\times/k^\times$.

Sketch of proof

Reconstructing lines: Functional equations

Projective lines are intersections of well-chosen infinite-dimensional projective subspaces $\mathbb{P}(E_1), \mathbb{P}(E_2)$, where $E_1, E_2 \subset K$ are 1-dimensional subfields. Precisely, assume that $x, y \in K^\times$ are algebraically independent. Let $p \in \overline{k(x)}^\times$, $q \in \overline{k(y)}^\times$ be such that x, y, p, q are multiplicatively independent in $K^\times/k^\times$. Assume that there is a nonconstant

$$\Pi \in \overline{k(x/y)}^\times \cdot y \cap \overline{k(p/q)}^\times \cdot q.$$

Assume moreover that this Π arises from infinitely many, modulo scalars, elements p, q as above.

Sketch of proof

Reconstructing lines: Functional equations

Projective lines are intersections of well-chosen infinite-dimensional projective subspaces $\mathbb{P}(E_1), \mathbb{P}(E_2)$, where $E_1, E_2 \subset K$ are 1-dimensional subfields. Precisely, assume that $x, y \in K^\times$ are algebraically independent. Let $p \in \overline{k(x)}^\times$, $q \in \overline{k(y)}^\times$ be such that x, y, p, q are multiplicatively independent in $K^\times/k^\times$. Assume that there is a nonconstant

$$\Pi \in \overline{k(x/y)}^\times \cdot y \cap \overline{k(p/q)}^\times \cdot q.$$

Assume moreover that this Π arises from infinitely many, modulo scalars, elements p, q as above. Then, modulo $k^\times$,

$$\Pi = \Pi_{\kappa,\delta}(x, y) := (x^\delta - \kappa y^\delta)^\delta, \qquad (1)$$

with $\kappa \in k^\times$ and $\delta = \pm 1$.

Sketch of proof

Reconstructing lines: Functional equations

The corresponding p and q are given by

$$\begin{aligned} p_{\kappa_x,1}(x) &= x+\kappa_x, & q_{\kappa_y,1}(y) &= y+\kappa_y \\ p_{\kappa_x,-1}(x) &= (x^{-1}+\kappa_x)^{-1}, & q_{\kappa_x,-1}(y) &= (y^{-1}+\kappa_y)^{-1} \end{aligned}$$

with

$$\kappa_x\kappa_y = \kappa.$$

Anabelian geometry

Grothendieck's Anabelian program

The Galois group of a function field determines the field.

Anabelian geometry

Grothendieck's Anabelian program

The Galois group of a function field determines the field.

Two group operations, $+$ and $\cdot$, are encoded in one group.

Anabelian geometry

Grothendieck's Anabelian program

The Galois group of a function field determines the field.

Two group operations, $+$ and $\cdot$, are encoded in one group.

Let K be a field with absolute Galois group $G_K := \mathrm{Gal}(\bar{K}/K)$.

Let $\mathcal{G}_K$ be the pro-ℓ-completion of G_K, for $\ell \neq \mathrm{char}(K)$ a prime.

Anabelian geometry

Grothendieck's Anabelian program

The Galois group of a function field determines the field.

Two group operations, $+$ and $\cdot$, are encoded in one group.

Let K be a field with absolute Galois group $G_K := \mathrm{Gal}(\bar{K}/K)$.

Let $\mathcal{G}_K$ be the pro-ℓ-completion of G_K, for $\ell \neq \mathrm{char}(K)$ a prime.

Uchida, Tamagawa, Mochizuki, Pop, Königsmann, Zaidi ...:
reconstruction of function fields from the full G_K or $\mathcal{G}_K$.

Almost abelian anabelian geometry

Let

$$\mathcal{G}_K^a := \mathcal{G}_K/[\mathcal{G}_K, \mathcal{G}_K], \quad \mathcal{G}_K^c := \mathcal{G}_K/[\mathcal{G}_K, [\mathcal{G}_K, \mathcal{G}_K]]$$

be the abelianization, resp. its canonical central extension.

Almost abelian anabelian geometry

Let

$$\mathcal{G}_K^a := \mathcal{G}_K/[\mathcal{G}_K, \mathcal{G}_K], \quad \mathcal{G}_K^c := \mathcal{G}_K/[\mathcal{G}_K, [\mathcal{G}_K, \mathcal{G}_K]]$$

be the abelianization, resp. its canonical central extension. The group $\mathcal{G}_K^a$ is a torsion-free $\mathbb{Z}_\ell$-module of infinite rank.

Almost abelian anabelian geometry

Let

$$\mathcal{G}_K^a := \mathcal{G}_K/[\mathcal{G}_K, \mathcal{G}_K], \quad \mathcal{G}_K^c := \mathcal{G}_K/[\mathcal{G}_K, [\mathcal{G}_K, \mathcal{G}_K]]$$

be the abelianization, resp. its canonical central extension. The group $\mathcal{G}_K^a$ is a torsion-free $\mathbb{Z}_\ell$-module of infinite rank.

Let Σ_K be the set of all topologically noncyclic subgroups of $\mathcal{G}_K^a$ that lift to abelian subgroups of $\mathcal{G}_K^c$.

Almost abelian anabelian geometry

Let

$$\mathcal{G}_K^a := \mathcal{G}_K/[\mathcal{G}_K, \mathcal{G}_K], \quad \mathcal{G}_K^c := \mathcal{G}_K/[\mathcal{G}_K, [\mathcal{G}_K, \mathcal{G}_K]]$$

be the abelianization, resp. its canonical central extension. The group $\mathcal{G}_K^a$ is a torsion-free $\mathbb{Z}_\ell$-module of infinite rank.

Let Σ_K be the set of all topologically noncyclic subgroups of $\mathcal{G}_K^a$ that lift to abelian subgroups of $\mathcal{G}_K^c$.

Bogomolov's program

The pair $(\mathcal{G}_K^a, \Sigma_K)$ determines K.

Almost abelian anabelian geometry

Theorem (Bogomolov-T.) $\dim = 2$ **in 2004 /** $\dim \geq 2$ **in 2009**

Let K and L be function fields over algebraic closures of finite fields k, l of characteristic $\neq \ell$. Assume that the transcendence degree of K over k is ≥ 2 and that there exists an isomorphism

$$\psi : \mathcal{G}^a_K \simeq \mathcal{G}^a_L$$

inducing a bijection of sets

$$\Sigma_K = \Sigma_L.$$

Then, for some $c \in \mathbb{Z}_\ell^\times$, $c\psi$ is induced by an isomorphism of purely inseparable closures of K and L.

Sketch of proof: Kummer theory

The abelianized Galois group $\mathcal{G}_K^a$ is dual to $\hat{K}^\times$, the pro-ℓ-completion of $K^\times$, and one obtains an isomorphism

$$\hat{K}^\times \simeq \hat{L}^\times.$$

Sketch of proof: Kummer theory

The abelianized Galois group $\mathcal{G}_K^a$ is dual to $\hat{K}^\times$, the pro-ℓ-completion of $K^\times$, and one obtains an isomorphism

$$\hat{K}^\times \simeq \hat{L}^\times.$$

In our setup, we can interpret $\mathcal{G}_K^a$ as homomorphisms

$$K^\times/k^\times \to \mathbb{Z}_\ell(1),$$

arising from

$$\mathcal{G}_K^a/\ell^n \ni \gamma_n \mapsto \left(f \mapsto \gamma(\sqrt[\ell^n]{f})/\sqrt[\ell^n]{f}\right).$$

Sketch of proof: Kummer theory

The abelianized Galois group $\mathcal{G}_K^a$ is dual to $\hat{K}^\times$, the pro-ℓ-completion of $K^\times$, and one obtains an isomorphism

$$\hat{K}^\times \simeq \hat{L}^\times.$$

In our setup, we can interpret $\mathcal{G}_K^a$ as homomorphisms

$$K^\times / k^\times \to \mathbb{Z}_\ell(1),$$

arising from

$$\mathcal{G}_K^a / \ell^n \ni \gamma_n \mapsto \left(f \mapsto \gamma(\sqrt[\ell^n]{f}) / \sqrt[\ell^n]{f} \right).$$

Thus, $\mathcal{G}_K^a$ is dual to $K^\times / k^\times = \bar{\mathrm{K}}_1(K)$.

Sketch of proof: K_2

Consider the exact sequence

$$1 \to \mathcal{Z}_K \to \mathcal{G}_K^c \to \mathcal{G}_K^a \to 1.$$

We have a natural map

$$\wedge^2(\mathcal{G}_K^a) \to \mathcal{Z}_K, \qquad (\gamma, \gamma') \mapsto [\tilde{\gamma}, \tilde{\gamma}'].$$

Put $\quad \mathrm{R}(\mathcal{G}_K^c) := \mathrm{Ker}(\wedge^2(\mathcal{G}_K^a) \to \mathcal{Z}_K) \quad$ and let $\quad \mathrm{R}_\wedge(\mathcal{G}_K^c) \subseteq \mathrm{R}(\mathcal{G}_K^c)$

be the subgroup generated by $\langle \gamma, \gamma' \rangle$, where γ, γ' is a commuting pair.

Bogomolov

Let $k = \bar{\mathbb{F}}_p$ and $K = k(X)$. Then $\mathrm{H}^2_{nr}(K)$ is dual to $\mathrm{R}(\mathcal{G}_K^c)/\mathrm{R}_\wedge(\mathcal{G}_K^c)$.

Sketch of proof: K_2

Consider the exact sequence

$$1 \to \mathcal{Z}_K \to \mathcal{G}_K^c \to \mathcal{G}_K^a \to 1.$$

We have a natural map

$$\wedge^2(\mathcal{G}_K^a) \to \mathcal{Z}_K, \qquad (\gamma, \gamma') \mapsto [\tilde{\gamma}, \tilde{\gamma}'].$$

Put $\quad \mathrm{R}(\mathcal{G}_K^c) := \mathrm{Ker}(\wedge^2(\mathcal{G}_K^a) \to \mathcal{Z}_K) \quad$ and let $\quad \mathrm{R}_\wedge(\mathcal{G}_K^c) \subseteq \mathrm{R}(\mathcal{G}_K^c)$

be the subgroup generated by $\langle \gamma, \gamma' \rangle$, where γ, γ' is a commuting pair.

Bogomolov

Let $k = \bar{\mathbb{F}}_p$ and $K = k(X)$. Then $\mathrm{H}^2_{nr}(K)$ is dual to $\mathrm{R}(\mathcal{G}_K^c)/\mathrm{R}_\wedge(\mathcal{G}_K^c)$.

To summarize, Σ_K carries information about $\mathrm{K}_2(K)$.

Valuations

A key ingredient of the proof is the reconstruction of valuations.

Valuations

A key ingredient of the proof is the reconstruction of valuations.

A value group, Γ, is a totally ordered (torsion-free) abelian group.

Valuations

A key ingredient of the proof is the reconstruction of valuations.

A value group, Γ, is a totally ordered (torsion-free) abelian group. A (nonarchimedean) valuation on a field K is a pair $\nu = (\nu, \Gamma_\nu)$ consisting of a value group Γ_ν and a map

$$\nu \,:\, K \to \Gamma_{\nu,\infty} = \Gamma_\nu \cup \infty$$

such that

- $\nu \,:\, K^\times \to \Gamma_\nu$ is a surjective homomorphism;
- $\nu(\kappa + \kappa') \geq \min(\nu(\kappa), \nu(\kappa'))$ for all $\kappa, \kappa' \in K$;
- $\nu(0) = \infty$.

Valuations

A key ingredient of the proof is the reconstruction of valuations.

A value group, Γ, is a totally ordered (torsion-free) abelian group. A (nonarchimedean) valuation on a field K is a pair $\nu = (\nu, \Gamma_\nu)$ consisting of a value group Γ_ν and a map

$$\nu : K \to \Gamma_{\nu,\infty} = \Gamma_\nu \cup \infty$$

such that

- $\nu : K^\times \to \Gamma_\nu$ is a surjective homomorphism;
- $\nu(\kappa + \kappa') \geq \min(\nu(\kappa), \nu(\kappa'))$ for all $\kappa, \kappa' \in K$;
- $\nu(0) = \infty$.

Note that $\bar{\mathbb{F}}_p$ admits only the trivial valuation.

Valuations

Denote by K_ν, $\mathfrak{o}_\nu, \mathfrak{m}_\nu$ and $\mathbf{K}_\nu := \mathfrak{o}_\nu/\mathfrak{m}_\nu$ the completion of K with respect to ν, the ring of ν-integers in K, the maximal ideal of $\mathfrak{o}_\nu$ and the residue field.

Valuations

Denote by K_ν, $\mathfrak{o}_\nu, \mathfrak{m}_\nu$ and $\mathbf{K}_\nu := \mathfrak{o}_\nu/\mathfrak{m}_\nu$ the completion of K with respect to ν, the ring of ν-integers in K, the maximal ideal of $\mathfrak{o}_\nu$ and the residue field. We have the following diagram

$$\begin{array}{ccccccccc}
 & & 1 & \longrightarrow & \mathfrak{o}_\nu^\times & \longrightarrow & K^\times & \longrightarrow & \Gamma_\nu \longrightarrow 1 \\
 & & & & \| & & & & \\
1 & \longrightarrow & (1+\mathfrak{m}_\nu)^\times & \longrightarrow & \mathfrak{o}_\nu^\times & \longrightarrow & \mathbf{K}_\nu^\times & \longrightarrow & 1
\end{array}$$

Weil groups

Let $K = \bar{\mathbb{F}}_p(X)$ be a function field and R a (topological) ring such that the order of every torsion element is coprimeto p. Define the abelian Weil group:

$$\mathrm{W}^a_K(R) := \mathrm{Hom}(K^\times/k^\times, R).$$

Weil groups

Let $K = \bar{\mathbb{F}}_p(X)$ be a function field and R a (topological) ring such that the order of every torsion element is coprimeto p. Define the abelian Weil group:

$$\mathrm{W}^a_K(R) := \mathrm{Hom}(K^\times/k^\times, R).$$

Main example:

$$\mathrm{W}^a_K(\mathbb{Z}_\ell) = \mathcal{G}^a_K.$$

Weil groups

Let $K = \bar{\mathbb{F}}_p(X)$ be a function field and R a (topological) ring such that the order of every torsion element is coprimeto p. Define the abelian Weil group:

$$\mathrm{W}^a_K(R) := \mathrm{Hom}(K^\times/k^\times, R).$$

Main example:

$$\mathrm{W}^a_K(\mathbb{Z}_\ell) = \mathcal{G}^a_K.$$

Other interesting cases: $R = \mathbb{Z}$ or $R = \mathbb{Z}/\ell$.

Weil groups

Let $K = \bar{\mathbb{F}}_p(X)$ be a function field and R a (topological) ring such that the order of every torsion element is coprimeto p. Define the abelian Weil group:

$$\mathrm{W}^a_K(R) := \mathrm{Hom}(K^\times/k^\times, R).$$

Main example:

$$\mathrm{W}^a_K(\mathbb{Z}_\ell) = \mathcal{G}^a_K.$$

Other interesting cases: $R = \mathbb{Z}$ or $R = \mathbb{Z}/\ell$. Define

$$\begin{aligned} \mathrm{D}^a_\nu(R) &= \{\mu \in \mathrm{W}^a_K(R) \,|\, \mu \text{ trivial on } (1+\mathfrak{m}_\nu)^\times\}, \\ \mathrm{I}^a_\nu(R) &= \{\iota \in \mathrm{W}^a_K(R) \,|\, \iota \text{ trivial on } \mathfrak{o}^\times_\nu\}. \end{aligned}$$

Weil groups

Let $K = \bar{\mathbb{F}}_p(X)$ be a function field and R a (topological) ring such that the order of every torsion element is coprimeto p. Define the abelian Weil group:

$$\mathrm{W}^a_K(R) := \mathrm{Hom}(K^\times/k^\times, R).$$

Main example:

$$\mathrm{W}^a_K(\mathbb{Z}_\ell) = \mathcal{G}^a_K.$$

Other interesting cases: $R = \mathbb{Z}$ or $R = \mathbb{Z}/\ell$. Define

$$\begin{aligned} \mathrm{D}^a_\nu(R) &= \{\mu \in \mathrm{W}^a_K(R) \,|\, \mu \text{ trivial on } (1+\mathfrak{m}_\nu)^\times\}, \\ \mathrm{I}^a_\nu(R) &= \{\iota \in \mathrm{W}^a_K(R) \,|\, \iota \text{ trivial on } \mathfrak{o}_\nu^\times\}. \end{aligned}$$

For $R = \mathbb{Z}_\ell$ these are the usual decomposition and inertia subgroups corresponding to ν.

Valuations

Any homomorphism $\chi : \Gamma_\nu \to R$ gives rise to a homomorphism

$$\chi \circ \nu \, : \, K^\times \to R,$$

thus to an element of $\mathrm{W}_K^a(R)$, an inertia element of ν.

Valuations

Any homomorphism $\chi : \Gamma_\nu \to R$ gives rise to a homomorphism

$$\chi \circ \nu \,:\, K^\times \to R,$$

thus to an element of $\mathrm{W}^a_K(R)$, an inertia element of ν. It is a flag map on K with values in R, i.e., every finite-dimensional $\mathbb{F}_p$-subspace $V \subset K$ has a flag $V = V_1 \supset V_2 \ldots$ such that ν is constant on $V_j \setminus V_{j+1}$.

Valuations

Any homomorphism $\chi : \Gamma_\nu \to R$ gives rise to a homomorphism

$$\chi \circ \nu \, : \, K^\times \to R,$$

thus to an element of $\mathrm{W}^a_K(R)$, an inertia element of ν. It is a flag map on K with values in R, i.e., every finite-dimensional $\mathbb{F}_p$-subspace $V \subset K$ has a flag $V = V_1 \supset V_2 \ldots$ such that ν is constant on $V_j \setminus V_{j+1}$.

Conversely, every flag map on K with values in R gives rise to a unique valuation ν and a homomorphism $\chi : \Gamma_\nu \to R$ as above.

Commuting pairs

Let K be a function field over $k = \bar{\mathbb{F}}_p$. We say that noncyclic subgroup $\sigma \subset \mathrm{W}^a_K(R)$ is a c-subgroup if its image in $\mathrm{W}^a_E(R)$ is cyclic, for every one-dimensional $E \subset K$.

Commuting pairs

Let K be a function field over $k = \bar{\mathbb{F}}_p$. We say that noncyclic subgroup $\sigma \subset \mathrm{W}^a_K(R)$ is a c-subgroup if its image in $\mathrm{W}^a_E(R)$ is cyclic, for every one-dimensional $E \subset K$. These form a fan $\Sigma_K(R)$.

Theorem

Let $R = \hat{\mathbb{Z}}, \mathbb{Z}, \mathbb{Z}/\ell^n$, or $\mathbb{Z}_\ell$. Then

- every c-subgroup σ has R-rank $\leq \mathrm{trdeg}_k(K)$;
- for every c-subgroup σ there exists a valuation $\nu \in \mathcal{V}_K$ such that
  - σ is trivial on $(1 + \mathfrak{m}_\nu)^\times \subset K^\times$
  - there exists a maximal subgroup $\sigma' \subseteq \sigma$ of R-corank at most one such that

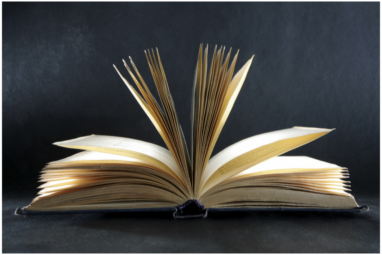
$$\sigma' \subseteq \mathrm{Hom}(\Gamma_\nu, R) \subset \mathrm{Hom}(K^\times, R) = \mathrm{W}^a_K(R).$$

Commuting pairs

The group σ' is, in fact, the inertia subgroups $\mathrm{I}^a_\nu(R)$ corresponding to ν. The union of all σ containing an inertia subgroup $\mathrm{I}^a_\nu(R)$ is the corresponding decomposition group $\mathrm{D}^a_\nu(R)$.

Commuting pairs

The group σ' is, in fact, the inertia subgroups $\mathrm{I}^a_\nu(R)$ corresponding to ν. The union of all σ containing an inertia subgroup $\mathrm{I}^a_\nu(R)$ is the corresponding decomposition group $\mathrm{D}^a_\nu(R)$.



Projective geometry of the Weil group

Key fact

Let $\gamma, \gamma' \in \sigma \subset \mathrm{W}^a_K(R)$ be nonproportional elements contained in a c-subgroup $\sigma \in \Sigma_K(R)$. Then, for any nonconstant $f \in K^\times$ the restrictions of γ, γ' to the projective line $\mathbb{P}_{\mathbb{F}_p}(\mathbb{F}_p \oplus f\mathbb{F}_p)$ are proportional (modulo addition of constants).

Projective geometry of the Weil group

Key fact

Let $\gamma, \gamma' \in \sigma \subset \mathrm{W}^a_K(R)$ be nonproportional elements contained in a c-subgroup $\sigma \in \Sigma_K(R)$. Then, for any nonconstant $f \in K^\times$ the restrictions of γ, γ' to the projective line $\mathbb{P}_{\mathbb{F}_p}(\mathbb{F}_p \oplus f\mathbb{F}_p)$ are proportional (modulo addition of constants).

Consider the map

$$\begin{array}{ccc} K^\times/k^\times = \mathbb{P}_k(K) & \to & \mathbb{A}^2(R) \\ f & \mapsto & (\gamma(f), \gamma'(f)) \end{array}$$

Projective geometry of the Weil group

Key fact

Let $\gamma, \gamma' \in \sigma \subset \mathrm{W}^a_K(R)$ be nonproportional elements contained in a c-subgroup $\sigma \in \Sigma_K(R)$. Then, for any nonconstant $f \in K^\times$ the restrictions of γ, γ' to the projective line $\mathbb{P}_{\mathbb{F}_p}(\mathbb{F}_p \oplus f\mathbb{F}_p)$ are proportional (modulo addition of constants).

Consider the map

$$\begin{array}{rcc} K^\times/k^\times = \mathbb{P}_k(K) & \to & \mathbb{A}^2(R) \\ f & \mapsto & (\gamma(f), \gamma'(f)) \end{array}$$

This maps every projective line into an affine line, a collineation.

Projective geometry of the Weil group

Key fact

Let $\gamma, \gamma' \in \sigma \subset \mathrm{W}^a_K(R)$ be nonproportional elements contained in a c-subgroup $\sigma \in \Sigma_K(R)$. Then, for any nonconstant $f \in K^\times$ the restrictions of γ, γ' to the projective line $\mathbb{P}_{\mathbb{F}_p}(\mathbb{F}_p \oplus f\mathbb{F}_p)$ are proportional (modulo addition of constants).

Consider the map

$$\begin{array}{ccc} K^\times/k^\times = \mathbb{P}_k(K) & \to & \mathbb{A}^2(R) \\ f & \mapsto & (\gamma(f), \gamma'(f)) \end{array}$$

This maps every projective line into an affine line, a collineation.

Images of planes

The image of every $\mathbb{P}^2(\mathbb{F}_p)$ in $\mathbb{A}^2(R)$ is contained in a union of an affine line and a point.

Projective geometry of the Weil group

Lemma

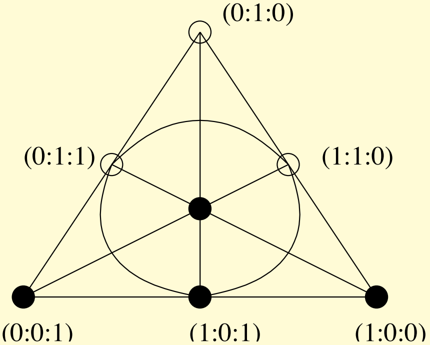
A map $\alpha : \mathbb{P}_k(K) \to R$ is a flag map iff the restiction to every $\mathbb{P}^1 \subset \mathbb{P}_k(K)$ is a flag map, i.e., constant on the complement of one point.

Projective geometry of the Weil group

Lemma

A map $\alpha : \mathbb{P}_k(K) \to R$ is a flag map iff the restiction to every $\mathbb{P}^1 \subset \mathbb{P}_k(K)$ is a flag map, i.e., constant on the complement of one point.

Counterexample: the Fano plane



Geometry of collineations

Given a map

$$\phi_{\gamma,\gamma'} : \mathbb{P}^2(\mathbb{F}_q) \to \{\bullet, \circ, \star\} \subset \mathbb{A}^2(\mathbb{F}_2)$$

such that every $\mathfrak{l} \subset \mathbb{P}^2(\mathbb{F}_q)$ is contained in an "affine line" (any subset of two points) one of the following

$$\gamma, \gamma', \gamma + \gamma'$$

is a flag map.

Geometry of collineations

Given a map

$$\phi_{\gamma,\gamma'} : \mathbb{P}^2(\mathbb{F}_q) \to \{\bullet, \circ, \star\} \subset \mathbb{A}^2(\mathbb{F}_2)$$

such that every $\mathfrak{l} \subset \mathbb{P}^2(\mathbb{F}_q)$ is contained in an "affine line" (any subset of two points) one of the following

$$\gamma, \gamma', \gamma + \gamma'$$

is a flag map.

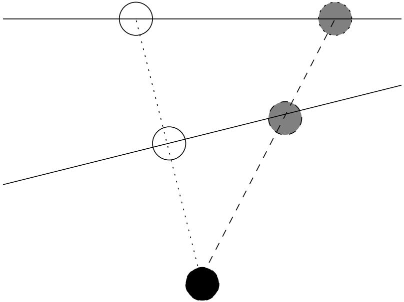
Geometry of collineations

Step 1. We can assume that $\mathbb{P}^2(\mathbb{F}_q)$ has lines of all three types and that every line has at least two points of each type.

Geometry of collineations

Step 1. We can assume that $\mathbb{P}^2(\mathbb{F}_q)$ has lines of all three types and that every line has at least two points of each type.

Step 2. Every point of type $\bullet$ induces a projective equivalence on lines of type $\mathfrak{l}(\circ, \star)$, preserving the "colors" of points.



Geometry of collineations

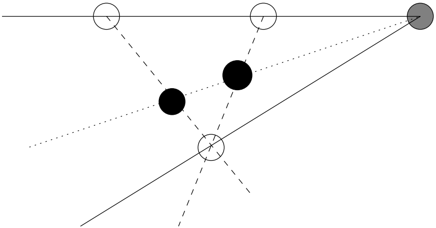
Step 3. There exist related points: $\bullet, \bullet' \subset \mathfrak{l}$, i.e, there exists a $\bullet'' \notin \mathfrak{l}$ such that the lines $\mathfrak{l}(\bullet, \bullet'')$ and $\mathfrak{l}(\bullet', \bullet'')$ are of the same type.

Geometry of collineations

Step 3. There exist related points: $\bullet, \bullet' \subset \mathfrak{l}$, i.e, there exists a $\bullet'' \notin \mathfrak{l}$ such that the lines $\mathfrak{l}(\bullet, \bullet'')$ and $\mathfrak{l}(\bullet', \bullet'')$ are of the same type.

Step 4. There exists a projective transformation on $\mathfrak{l}$, with exactly one fixed point, preserving the "colors" and transitive on the complement to the fixed point:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$



Geometry of collineations

This forces one of $\gamma, \gamma', \gamma + \gamma''$ to be a flag map on the whole $\mathbb{P}^2(\mathbb{F}_q)$, and in the end on all of $\mathbb{P}(K)$.

Projective geometry of the Weil group

Proposition

Every $\sigma \in \Sigma_K(R)$ contains an inertia element $\iota = \iota_\nu$ for some valuation ν of K.

Projective geometry of the Weil group

Proposition

Every $\sigma \in \Sigma_K(R)$ contains an inertia element $\iota = \iota_\nu$ for some valuation ν of K. The elements "commuting" with ι form $\mathrm{D}^a_\nu(R)$.

Projective geometry of the Weil group

Proposition

Every $\sigma \in \Sigma_K(R)$ contains an inertia element $\iota = \iota_\nu$ for some valuation ν of K. The elements "commuting" with ι form $\mathrm{D}^a_\nu(R)$.

In the reconstruction of function fields from their ℓ-Galois groups, i.e., when $R = \mathbb{Z}_\ell$, an isomorphism pairs

$$(\mathcal{G}^a_K, \Sigma_K) \simeq (\mathcal{G}^a_L, \Sigma_L)$$

allows to identify the intricate relations between valuations, and in the end the projective structures of $\mathbb{P}_k(K)$ and $\mathbb{P}_l(L)$; thus a field isomorphism.

Reconstruction of function fields

As seen above, we need to reconstruct:

- $K^\times/k^\times$ from $\hat{K}^\times$
- projective lines $\mathfrak{l} \subset \mathbb{P}(K)$, or multiplicative groups of 1-dimensional subfields.

Reconstruction of function fields

As seen above, we need to reconstruct:

- $K^\times/k^\times$ from $\hat{K}^\times$
- projective lines $\mathfrak{l} \subset \mathbb{P}(K)$, or multiplicative groups of 1-dimensional subfields.

What we see are inertia and decomposition groups of valuations on K.

Reconstruction of function fields

As seen above, we need to reconstruct:

- $K^\times/k^\times$ from $\hat{K}^\times$
- projective lines $\mathfrak{l} \subset \mathbb{P}(K)$, or multiplicative groups of 1-dimensional subfields.

What we see are inertia and decomposition groups of valuations on K.

Assume for simplicity that $K = k(X)$, where X is a surface. We see divisorial valuations, i.e., curves on some model of K (a blowup of X).

Reconstruction of function fields

Characterizing curves of genus ≥ 1

Let $E = k(C)$ be the function field of a curve. Then $\mathrm{g}(C) \geq 1$ iff there exists a nontrivial homomorphism from $\mathcal{G}_E^a$ onto an abelian ℓ-group that maps all inertia elements in $\mathcal{G}_E^a$ to zero.

Indeed, every higher-genus curve over $\bar{\mathbb{F}}_p$ has unramified covering of degree ℓ.

Reconstruction of function fields

Characterizing curves of genus ≥ 1

Let $E = k(C)$ be the function field of a curve. Then $\mathrm{g}(C) \geq 1$ iff there exists a nontrivial homomorphism from $\mathcal{G}^a_E$ onto an abelian ℓ-group that maps all inertia elements in $\mathcal{G}^a_E$ to zero.

Indeed, every higher-genus curve over $\bar{\mathbb{F}}_p$ has unramified covering of degree ℓ. It follows that from an isomorphism

$$(\mathcal{G}^a_K, \Sigma_K) \to (\mathcal{G}^a_L, \Sigma_L)$$

we can match higher-genus curves on models X and Y of K, resp. L. Note that different models of the same field differ only in rational curves.

Reconstruction of function field

Let

$$\mathcal{T}_\ell(X) := \varprojlim \mathrm{Tor}_1(\mathbb{Z}/\ell^n, \mathrm{Pic}^0(X)\{\ell\}).$$

Reconstruction of function field

Let

$$\mathcal{T}_\ell(X) := \varprojlim \mathrm{Tor}_1(\mathbb{Z}/\ell^n, \mathrm{Pic}^0(X)\{\ell\}).$$

We have

$$0 \to K^\times/k^\times \to \mathrm{Div}(X) \to \mathrm{Pic}(X) \to 0$$

which gives rise to the diagram

$$\begin{array}{ccccccc} 0 & \to & K^\times/k^\times \otimes \mathbb{Z}_\ell & \xrightarrow{\rho_{X,\ell}} & \mathrm{Div}^0(X)_\ell & \overset{\mathrm{pic}_\ell}{\twoheadrightarrow} & \mathrm{Pic}^0(X)\{\ell\} \\ & & \downarrow & & \downarrow & & \downarrow \\ \mathcal{T}_\ell(X) & \hookrightarrow & \hat{K}^\times & \xrightarrow{\hat{\rho}_X} & \widehat{\mathrm{Div}^0}(X) & \xrightarrow{\hat{\mathrm{pic}}} & 0. \end{array}$$

Reconstruction of function fields

We have two notions of support for $\hat{f} = \sum_m a_m(f) D_m \in \hat{K}^\times$:

$$\begin{aligned} \mathrm{supp}_K(\hat{f}) &:= \{\nu \in \mathcal{DV}_K \mid [\hat{f}, \mathcal{I}_\nu^a] \neq 0\} \\ \mathrm{supp}_X(\hat{f}) &:= \{D_m \subset X \mid a_m(f) \neq 0\} \end{aligned}$$

Reconstruction of function fields

We have two notions of support for $\hat{f} = \sum_m a_m(f) D_m \in \hat{K}^\times$:

$$\begin{aligned} \mathrm{supp}_K(\hat{f}) &:= \{\nu \in \mathcal{DV}_K \mid [\hat{f}, \mathcal{I}_\nu^a] \neq 0\} \\ \mathrm{supp}_X(\hat{f}) &:= \{D_m \subset X \mid a_m(f) \neq 0\} \end{aligned}$$

If X contains only finitely many rational curves, then there is an intrinsic notion of finite support: finite support on $\nu \in \mathcal{DV}_K$ corresponding to curves of genus ≥ 1. This allows to reconstruct "honest" functions f inside $\hat{K}^\times$. ...

Main points of the proof

Rational curves play a crucial role in anabelian geometry.

- 1-dimensional subfields

Main points of the proof

Rational curves play a crucial role in anabelian geometry.

- 1-dimensional subfields
- uniruled divisors complicate the identification of

$$K^\times \otimes \mathbb{Z}_{(\ell)}^\times \subset \hat{K}^\times.$$

Unramified cohomology

Let ν be a divisorial valuation of K. We have a natural homomorphism

$$\partial_\nu : \mathrm{H}^i(G_K) \to \mathrm{H}^{i-1}(G_{\mathbf{K}_\nu}),$$

where $\mathbf{K}_\nu$ is the residue field at ν. After Bloch-Ogus (1974) and Colliot-Thélène-Ojanguren (1989), unramified cohomology is

$$\mathrm{H}^i_{nr}(G_K) := \bigcap_\nu \mathrm{Ker}(\partial_\nu) \subset \mathrm{H}^i(G_K).$$

By definition, this is a birational invariant and we may write $\mathrm{H}^*_{nr}(X)$; it vanishes for rational varieties.

Universal spaces for unramified cohomology

Let $k = \bar{\mathbb{F}}_p$, $\ell \neq p$. Let $K = k(X)$ be the function field of an algebraic variety of dimension ≥ 2 and G_K its absolute Galois group.

Bogomolov-T. 2012

If $\alpha \in \mathrm{H}^i_{nr}(G_K, \mathbb{Z}/\ell^n)$ then there exist

- a surjective homomorphism $G_K \to G^a$ onto finite abelian ℓ-group,
- projective G^a-representations $\mathbb{P}(V_j)$ over k,
- an explicit open G^a-stable subset

$$\mathbb{P}^\circ \subset \mathbb{P} := \prod_j \mathbb{P}(V_j),$$

- and a rational map $\varrho : X \to \mathbb{P}^\circ / G^a$

such that α is induced from $\mathbb{P}^\circ / G^a$.

"Section conjecture"

Bogomolov-T. 2011

Assume that K, L are function fields over algebraic closures of finite fields k, l, respectively. Assume that

$$\psi_1 : K^\times/k^\times \to L^\times/l^\times$$

is a noninjective homomorphism such that

(a) for any one-dimensional subfield $E \subset K$, there exists a one-dimensional subfield $F \subset L$ with

$$\psi_1(E^\times/k^\times) \subseteq F^\times/l^\times,$$

(b) $\psi_1(K^\times/k^\times)$ contains at least two algebraically independent elements of $L^\times/l^\times$.

“Section conjecture”

Bogomolov-T. 2011

Then

1. there is a valuation ν of K such that ψ_1 is trivial on
$$(1+\mathfrak{m}_\nu)^\times/k^\times \subset \mathfrak{o}_\nu^\times/k^\times;$$
2. the restriction of ψ_1 to
$$\mathbf{K}_\nu^\times/k^\times = \mathfrak{o}_\nu^\times/k^\times(1+\mathfrak{m}_\nu)^\times \to L^\times/l^\times$$
is injective and satisfies (a).