GALOIS THEORY AND PROJECTIVE GEOMETRY

FEDOR BOGOMOLOV AND YURI TSCHINKEL

Abstract. We explore connections between birational anabelian geometry and abstract projective geometry. One of the applications is a proof of a version of the birational section conjecture.

1. Introduction

A major open problem today is to identify classes of fields characterized by their absolute Galois groups. There exist genuinely different fields with isomorphic Galois groups, e.g., \( \mathbb{F}_p \) and \( \mathbb{C}((t)) \). However, Neukirch and Uchida showed that Galois groups of maximal solvable extensions of number fields or function fields of curves over finite fields determine the corresponding field, up-to isomorphism [23, 31].

This result is the first instance of birational anabelian geometry which aims to show that Galois groups of certain fields, e.g., function fields of algebraic varieties, determine the field, in a functorial way. The term anabelian was proposed by Grothendieck in [15] where he introduced a class of anabelian varieties, functorially characterized by their étale fundamental groups; with prime examples being hyperbolic curves and varieties successively fibered into hyperbolic curves. For representative results, see [21, 33, 32, 30], as well as [16, 22, 26, 25, 20].

However, absolute Galois groups are simply too large. It turns out that there are intermediate groups, whose description involves some projective geometry, most importantly, geometry of lines and points in the projective plane. These groups are just minimally different from abelian groups; they encode the geometry of simple configurations. On the other hand, their structure is already sufficiently rich so that the corresponding objects in the theory of fields allow to capture all invariants and individual properties of large fields, i.e., function fields of transcendence degree at least two over algebraically closed ground fields. This insight of the first author [3, 5, 4], was developed in [6, 7, 8]. One of our main
results is that function fields $K = k(X)$ over $k = \overline{F}_p$ are determined by
\[ \mathcal{G}_K^c := \mathcal{G}_K / [\mathcal{G}_K, [\mathcal{G}_K, \mathcal{G}_K]], \]
where $\mathcal{G}_K$ is the maximal pro-$\ell$-quotient of the absolute Galois group $G_K$ of $K$, and $\mathcal{G}_K^c$ is the canonical central extension of its abelianization $\mathcal{G}_K^a$ (see also [27]).

In [9] we survey the development of the main ideas merging into this almost abelian anabelian geometry program. Here we prove a new result, a version of the birational section conjecture (see Section 4). In Sections 5 and 6 we discuss cohomological properties of Galois groups closely related to the Bloch–Kato conjecture, proved by Voevodsky, Rost, and Weibel, and focus on connections to anabelian geometry.

Acknowledgments. The first author was partially supported by NSF grants DMS-0701578, DMS-1001662, and by the AG Laboratory GU-HSE grant RF government ag. 11 11.G34.31.0023. The second author was partially supported by NSF grants DMS-0739380 and 0901777.

2. Projective geometry and K-theory

The introduction of the projective plane essentially trivialized plane geometry and provided simple proofs for many results concerning configurations of lines and points, considered difficult before that. More importantly, the axiomatization efforts in late 19th and early 20th century revealed that abstract projective structures capture coordinates, a “triumph of modern mathematical thought” [34, p. v]. The axioms can be found in many books, including Emil Artin’s lecture notes from a course he gave at the Courant Institute in the Fall of 1954 [2, Chapters VI and VII]. The classical result mentioned above is that an abstract projective space (subject to Pappus’ axiom) is a projectivization of a vector space over a field. This can be strengthened as follows:

**Theorem 1.** Let $K/k$ be an extension of fields. Then $K^\times/k^\times$ is simultaneously an abelian group and a projective space. Conversely, an abelian group with a compatible projective structure corresponds to a field extension.

*Proof.* See [9, Section 1].
In **Algebraic geometry**, projective spaces are the most basic objects. Over nonclosed fields $K$, they admit nontrivial forms, called Brauer-Severi varieties. These forms are classified by the Brauer group $\text{Br}(K)$, which admits a Galois-cohomological incarnation:

$$\text{Br}(K) = H^2(G_K, \mathbb{G}_m).$$

The theory of Brauer groups and the local-global principle for Brauer-Severi varieties over number fields are cornerstones of arithmetic geometry. Much less is known over more complicated ground fields, e.g., function fields of surfaces. Brauer groups, in turn, are closely related to Milnor’s $K_2$-groups, and more generally $K$-theory, which emerged in algebra in the study of matrix groups.

We recall the definition of Milnor $K$-groups. Let $K$ be a field. Then

$$K^M_1(K) = K^\times$$

and the higher $K$-groups are spanned by symbols:

$$K^M_n(K) = (K^\times)^n / \langle \cdots x \otimes (1 - x) \cdots \rangle,$$

the relations being symbols containing $x \otimes (1 - x)$. For $i = 1, 2$, Milnor $K$-groups of fields coincide with those defined by Quillen, and we will often omit the superscript.

Throughout, we work with function fields of algebraic varieties over algebraically closed ground fields; by convention, the dimension of the field is its transcendence degree over the ground field.

**Theorem 2.** [8] Assume that $K$ and $L$ are function fields of algebraic varieties of dimension $\geq 2$, over algebraically closed fields $k$ and $l$, and that there exist compatible isomorphisms of abelian groups

$$K_1(K) \xrightarrow{\psi_1} K_1(L) \quad \text{and} \quad K_2(K) \xrightarrow{\psi_2} K_2(L).$$

Then there exists an isomorphism of fields

$$\psi : K \to L$$

such that the induced map on $K^\times$ coincides with $\psi_1^{\pm 1}$.

The proof exploits the fact that $K_2(K)$ encodes the canonical projective structure on $\mathbb{P}_k(K) = K^\times / k^\times$. It is based on the following observations:

- The multiplicative groups $k^\times$ and $l^\times$ are characterized as *infinitely-divisible* elements in $K_1(K)$, resp. $K_1(L)$. This leads to an isomorphism of abelian groups (denoted by the same symbol):

$$\mathbb{P}_k(K) \xrightarrow{\psi_1} \mathbb{P}_l(L).$$
rational functions \( f_1, f_2 \in K^\times \) are algebraically dependent in \( K \) if and only if their symbol \( (f_1, f_2) \) is \textit{infinitely-divisible} in \( K_2(K) \). This allows to characterize \( \mathbb{P}_k(E) \subset \mathbb{P}_k(K) \), for one-dimensional \( E \subset K \) and we obtain a \textit{fan} of infinite-dimensional projective subspaces in \( \mathbb{P}_k(K) \). The compatibility of \( \psi_1 \) with \( \psi_2 \) implies that the corresponding structures on \( \mathbb{P}_k(K) \) and \( \mathbb{P}_l(L) \) coincide.

By Theorem \( \text{H} \) it remains to show that \( \psi_1 \) (or \( 1/\psi_1 \)) maps projective lines \( \mathbb{P}^1 \subset \mathbb{P}_k(K) \) to projective lines in \( \mathbb{P}_l(L) \). It turns out that projective lines can be intrinsically characterized as \textit{intersections} of well-chosen infinite-dimensional \( \mathbb{P}_k(E_1) \) and \( \mathbb{P}_k(E_2) \), for 1-dimensional subfields \( E_1, E_2 \subset K \) (see [8, Theorem 22] or [9, Proposition 9]).

The theorem proved in [8] is stronger, it addresses the case when \( \psi_1 \) is an \textit{injective} homomorphism.

3. \textbf{Projective geometry and Galois groups}

Let \( K \) be a function field over \( k = \overline{\mathbb{F}}_p \). In Section 2 we considered the abelian group / projective space \( \mathbb{P}_k(K) \) and its relationship to the \( K \)-theory of the field \( K \). Here we focus on a \textit{dual} picture.

Let \( R \) be a topological commutative ring such that the order of all torsion elements \( r \in R \) is coprime to \( p \). Define

\[
W^a_K(R) := \text{Hom}(K^\times/k^\times, R) = \text{Hom}(K^\times, R),
\]

the \( R \)-module of continuous homomorphisms, where \( \mathbb{P}_k(K) = K^\times/k^\times \) is endowed with discrete topology. We call \( W^a_K(R) \) the \textit{abelian Weil group} of \( K \) with values in \( R \).

The abelian Weil group carries a collection of distinguished subgroups, corresponding to various \textit{valuations}. Recall that a valuation is a surjective homomorphism

\[
\nu : K^\times \to \Gamma
\]

onto an ordered abelian group, subject to a nonarchimedean triangle inequality

\[
\nu(f + g) \geq \min(\nu(f), \nu(g)).
\]

Let \( \mathcal{V}_K \) be the set of all nontrivial valuations of \( K \), for \( \nu \in \mathcal{V}_K \) let \( \mathfrak{o}_\nu \) be the valuation ring, \( \mathfrak{m}_\nu \subset \mathfrak{o}_\nu \) its maximal ideal, and \( K_\nu \) the corresponding function field. We have the following fundamental diagram:
Every valuation of $k = \mathbb{F}_p$ is trivial, and valuation theory over function fields $K = k(X)$ is particularly geometric: all $\nu \in \mathcal{V}_K$ are trivial on $k^\times$ and define $\Gamma_\nu$-valued functions on $\mathbb{P}_k(K)$. Throughout, we restrict our attention to such ground fields. In this context, nontrivial valuations on $k(t)$ are in bijection with points $p \in \mathbb{P}^1$, they measure the order of a function at $p$. There are many more valuations on higher-dimensional varieties.

We call
\[
\Gamma_\nu^a(R) := \{ \gamma \in W_K^a(R) \mid \gamma \text{ is trivial on } \mathfrak{o}_K^\times \} \subseteq W_K^a(R)
\]
the abelian inertia group and
\[
D_\nu^a(R) := \{ \gamma \in W_K^a(R) \mid \gamma \text{ is trivial on } (1 + m_\nu)^\times \} \subseteq W_K^a(R)
\]
the abelian decomposition group, we have
\[
D_\nu^a(R)/\Gamma_\nu^a(R) = W_{K_\nu}^a(R).
\]

**Example 3.** Let $G_K$ be the absolute Galois group of a field $K$, $G_K^a$ its abelianization, and $G_K^a[\ell]$ the $\ell$-completion of $G_K^a$. By Kummer theory,
\[
G_K^a = W_{K_\ell}^a(\mathbb{Z}_\ell).
\]
Moreover, $\Gamma_\nu^a(\mathbb{Z}_\ell)$ and $D_\nu^a(\mathbb{Z}_\ell)$ are the standard abelian inertia and decomposition subgroups corresponding to $\nu$.

A valuation $\nu$ defines a simple geometry on the projective space $\mathbb{P}_k(K)$; equation (3.2) implies that each finite dimensional subspace $\mathbb{P}^n \subset \mathbb{P}_k(K)$ admits a flag
\[
(3.3) \quad \mathbb{P}_1 \subset \mathbb{P}_2 \subset ...
\]
of projective subspaces, such that
\[
\nu : \mathbb{P}_k(K) \to \Gamma_\nu
\]
is constant on $\mathbb{P}_j \setminus \mathbb{P}_{j-1}$, for all $j$, and this flag structure is preserved under multiplicative shifts by any $f \in K^\times/k^\times$.

Let $\mathbb{P}$ be a projective space over $k$, e.g., $\mathbb{P} = \mathbb{P}_k(K)$. We say that a map $\iota : \mathbb{P} \to R$ to an arbitrary ring $R$ is a flag map if every finite-dimensional $\mathbb{P}^n \subset \mathbb{P}$ admits a flag as in (3.3) such that $\iota$ is constant on each $\mathbb{P}_j \setminus \mathbb{P}_{j-1}$; a
subset $S \subset \mathbb{P}$ will be called a **flag subset** if its set-theoretic characteristic function is a flag map.

**Example 4.** A nonempty flag subset of $\mathbb{P}^1(k)$ is either a point, the complement to a point, or all of $\mathbb{P}^1(k)$. Nonempty proper flag subsets of $\mathbb{P}^2(k)$ are one of the following:
- a point $p$, a line $l$, $l^o := l \setminus p$,
- $\mathbb{P}^2 \setminus p$, $\mathbb{P}^2 \setminus l$, $\mathbb{P}^2 \setminus l^o$.

**Proposition 5.** [6, Section 2] Let $\mathbb{P}$ be a projective space over $k = \overline{\mathbb{F}}_p$. A map $\iota : \mathbb{P} \to R$ is a flag map if and only if its restriction to every $\mathbb{P}^1 \subset \mathbb{P}$ is a flag map, i.e., is constant on the complement to one point.

By [6, Section 6.3], flag maps are closely related to valuations: given a flag homomorphism $\iota : \mathbb{P}_k(K) \to R$ there exists a unique $\nu \in V_K$ and a homomorphism $\chi : \Gamma_\nu \to R$ such that
\[
(3.4) \quad \iota = \chi \circ \nu.
\]
This means that $\iota \in I^o_\nu(R)$.

We now describe the theory of **commuting pairs** developed in [6]: We say that nonproportional $\gamma, \gamma' \in W^a_k(R)$ form a $c$-pair if for every normally closed one-dimensional subfield $E \subset K$ the image of the subgroup $R\gamma \oplus R\gamma'$ in $W^a_E(R)$ is cyclic; a $c$-subgroup is a noncyclic subgroup $\sigma \subset W^a_k(R)$ whose image in $W^a_E(R)$ is cyclic, for all $E$ as above. We define the **centralizer** $Z_\gamma \subset W^a_k(R)$ of an element $\gamma \in W^a_k(R)$ as the subgroup of all elements forming a $c$-pair with $\gamma$.

The main result of [6] says:

**Theorem 6.** Assume that $R$ is one of the following:
- $\mathbb{Z}$, $\hat{\mathbb{Z}}$, $\mathbb{Z}/\ell^n$, $\mathbb{Z}_\ell$.

Then
- every $c$-subgroup $\sigma$ has $R$-rank $\leq \text{tr} \deg_k(K)$;
- for every $c$-subgroup $\sigma$ there exists a valuation $\nu \in V_K$ such that
  - $\sigma$ is trivial on $(1 + m_\nu)^x \subset K^x$
  - there exists a maximal subgroup $\sigma' \subset \sigma$ of $R$-corank at most one such that
    \[
    \sigma' \subset \text{Hom}(\Gamma_\nu, R) \subset \text{Hom}(K^x, R) = W^a_K(R).
    \]
The groups $σ'$ are, in fact, inertia subgroups $I_a(ν)$ corresponding to $ν$. The union of all $σ$ containing an inertia subgroup $I_a(ν)$ is the corresponding decomposition group $D_a(ν)(R)$. If $I_a(ν)(R)$ is cyclic, generated by $ι$, then $D_a(ν)(R) = Z_ι$, the centralizer of $ι$.

The proof of Theorem 6 is based on the following geometric observation, linking the abelian Weil group with affine/projective geometry: Let $γ, γ' \in W_K^a(R)$ be nonproportional elements forming a c-pair and let

$$\mathbb{P}_k(K) \xrightarrow{\phi} R^2$$

$$f \mapsto (γ(f), γ'(f))$$

be the induced map to the affine plane $\mathbb{A}^2(R)$. If follows that

(*) the image of every $P_1 \subset P_k(K)$ satisfies a linear relation, i.e., is contained in an affine line in $\mathbb{A}^2(R)$.

Classically, this is called a collineation. A simple model is a map

$$\mathbb{P}^2(F_p) \xrightarrow{φ} \mathbb{A}^2(F_2),$$

where $p > 2$ is a prime and where the target is a set with 4 elements. It turns out that when the map $φ$ satisfies condition (*) then the target contains only 3 points. Furthermore, on every line $P_1 \subset P_2$ the map is constant on the complement of one point! This in turn implies that there is a stratification

$$p \subset I \subset P^2,$$

where $p$ is a point and $I = P^1$ and $r, r' \in F_2$, $(r, r') \neq (0, 0)$, such that $ι : rγ + r'γ'$ is constant on $I \setminus p$, and $P^2 \setminus I$, i.e., $ι$ is a flag map on $P^2$. (This last property fails for $p = 2$.) Nevertheless, one can extract the following general fact:

• if $γ, γ'$ satisfy (*) then there exists a nontrivial $R$-linear combination $ι := rγ + r'γ'$ such that

$$ι : \mathbb{P}_k(K) \to R$$

is a flag map, i.e., $ι \in I_a^p(R)$, for some $ν \in V_K$.

The proof is based on a lemma from projective geometry:

**Lemma 7.** Let $\mathbb{P}^2(k) = S_1 \sqcup_{j \in J} S_j$ be a set-theoretic decomposition into at least three nonempty subsets such that for every $\mathbb{P}^1(k) \subset \mathbb{P}^2(k)$ we have

$$\mathbb{P}^1(k) \subseteq S_1 \sqcup S_j, \text{ for some } j \in J, \text{ or } \mathbb{P}^1 \subseteq \sqcup_{j \in J} S_j$$

Then one of the $S_j$ is a flag subspace of $\mathbb{P}^2(k)$.
These considerations lead to the following characterization of multiplicative groups of valuation rings, one of the main results of [6]:

**Proposition 8.** Let $\mathfrak{o}^\times \subset K^\times/k^\times$ be a subgroup such that its intersection with any projective plane $\mathbb{P}^2 \subset \mathbb{P}_k(K) = K^\times/k^\times$ is a flag subspace, i.e., its set-theoretic characteristic function is a flag function. Then there exists a $\nu \in \mathcal{V}_K$ such that $\mathfrak{o}^\times = \mathfrak{o}^\times_{\nu}/k^\times$.

We now turn to more classical objects, namely Galois groups of fields. Let $G_K$ be the absolute Galois group of a field $K$, $G^a_K$ its abelianization and $G^c_K = G_K/[G_K, [G_K, G]]$ its canonical central extension. Let $K$ be a function field of transcendence degree $\geq 2$ over $k = \bar{\mathbb{F}}_p$. Fix a prime $\ell \neq p$ and replace $G^a_K$ and $G^c_K$ by their maximal pro-$\ell$-quotients $G^a_K = \text{Hom}(K^\times/k^\times, \mathbb{Z}_\ell) = W^a_K(\mathbb{Z}_\ell)$, and $G^c_K$.

Note that $G^a_K$ is a torsion-free $\mathbb{Z}_\ell$-module of infinite rank.

A *commuting pair* is a pair of nonproportional $\gamma, \gamma' \in G^a_K$ which lift to commuting elements in $G^c_K$ (this property does not depend on the choice of the lift). The main result of the theory of commuting pairs in [6] says that if

(\text{**}) $\gamma, \gamma' \in G^a_K$ form a commuting pair then the $\mathbb{Z}_\ell$-linear span of $\gamma, \gamma' \in G^a_K$ contains an inertia element of some valuation $\nu$ of $K$.

A key observation is that Property (\text{**}) implies (\text{*}), for each $\mathbb{P}_k^2 \subset \mathbb{P}_k(K)$, which leads to a flag structure on $\mathbb{P}_k(K)$, which in turn gives rise to a valuation. For a related result on reconstruction of valuations see [14].

Commuting pairs are part of an intricate *fan* $\Sigma_K$ on $G^a_K$, which is defined as the set of all topologically noncyclic subgroups of $G^a_K$ which lift to commuting subgroups of $G^c_K$. We have:

- $\text{rk}_{\mathbb{Z}_\ell}(\sigma) \leq \text{tr deg}_k(K)$, for all $\sigma \in \Sigma_K$;
- every $\sigma \in \Sigma_K$ contains a subgroup of corank one which is the inertia subgroup of some valuation of $K$.

Intersections of subgroups in $\Sigma_K$ reflect subtle dependencies among valuations of $K$. Let $I^a_{\nu} := I^a_{\nu}(\mathbb{Z}_\ell) \subset G^a_K$ be the subgroup of inertia elements with respect to $\nu \in \mathcal{V}_K$ and $D^a_{\nu} = D^a_{\nu}(\mathbb{Z}_\ell)$ the corresponding *decomposition group*. In our context, $D^a_{\nu}$ is also the group of all elements $\gamma \in G^a_K$ forming a commuting pair with every $\iota \in I^a_{\nu}$. As noted above, the
definitions of inertia and decomposition groups given here are equivalent to the classical definitions in Galois theory. We have

$$G^a_{K\nu} = D^a_{\nu}/I^a_{\nu},$$

the Galois group of the residue field $K_\nu$ of $\nu$, and $\Sigma_{K\nu}$ is the set of projections of subgroups of $\sigma \in \Sigma_K$ which are contained in $D^a_{\nu}$. When $X$ is a surface, $K = k(X)$, and $\nu$ a divisorial valuation of $K$, we have $T^a_{\nu} \cong \mathbb{Z}_\ell$ and $D^a_{\nu}$ is a large group spanned by subgroups $\sigma$ of rank two consisting of all element commuting with the topological generator $\delta_\nu$ of $T^a_{\nu}$.

To summarize, the Galois group $G^a_{K}$ encodes information about affine and projective structures on $G^a_{K}$, in close parallel to what we saw in the context of K-theory in Section 2. These structures are so individual that they allow to recover the field, via the reconstruction of the projective structure on $\mathbb{P}_k(K)$:

**Theorem 9.** [7, 10] Let $K$ and $L$ be function fields of transcendence degree $\geq 2$ over $k = \overline{\mathbb{F}}_p$ and $\ell \neq p$ a prime. Let

$$\psi^* : G^a_{L} \to G^a_{K}$$

be an isomorphism of abelian pro-$\ell$-groups inducing a bijection of sets

$$\Sigma_L = \Sigma_K.$$

Then there exists an isomorphism of perfect closures

$$\overline{\psi} : \overline{K} \to \overline{L},$$

unique modulo rescaling by a constant in $\mathbb{Z}_\ell^\times$.

4. **Z-version of the Galois group**

In this section, we introduce a functorial version of the reconstruction/recognition theories presented in Sections 2 and 3. This version allows to recover not only field isomorphisms from data of K-theoretic or Galois-theoretic type, but also sections, i.e., rational points on varieties over higher-dimensional function fields.

We work in the following setup: let $X$ be an algebraic variety over $k = \overline{\mathbb{F}}_p$, with function field $K = k(X)$. We use the notation:

- for $x, y \in K^\times$ we let $l(x, y) \subset \mathbb{P}_k(K)$ be the projective line through the images of $x$ and $y$ in $K^\times/k^\times$;
for planes $\mathbb{P}^2(1, x, y) \subset \mathbb{P}_k(K)$ (the span of lines $l(1, x), l(1, y)$) we set $\mathbb{P}^2(1, x, y)^o := \mathbb{P}^2(1, x, y) \setminus \{1\}$.

We will say that $\bar{x}, \bar{y} \in K^\times/k^\times$ are algebraically dependent, and write $\bar{x} \approx \bar{y}$, if this holds for any of their lifts $x, y$ to $K^\times$.

Define the abelian Weil group

$$W_K^\alpha := \text{Hom}(K^\times/k^\times, \mathbb{Z}) = \text{Hom}(K^\times, \mathbb{Z}),$$

with discrete topology. Since $K^\times/k^\times$ is a free abelian group, $W_K^\alpha$ is a torsion-free, infinite rank $\mathbb{Z}$-module. The functor

$$K \mapsto W_K^\alpha$$

is contravariant; it is a $\mathbb{Z}$-version of $G_K^\alpha$, since it can be regarded as a $\mathbb{Z}$-sublattice of

$$G_K^\alpha = \text{Hom}(K^\times/k^\times, \mathbb{Z}_\ell), \quad \ell \neq p.$$  

We proceed to explore a functorial version of Theorem 9 for $(W_K^\alpha, \Sigma_K)$, where $\Sigma_K$ is the corresponding fan, i.e., the set of $c$-subgroups $\sigma \subset W_K^\alpha$.

We work with the following diagram

$$K \xrightarrow{\psi} L$$

$$\xrightarrow{\psi_1} \mathbb{L}^\times/k^\times \xrightarrow{\psi} \mathbb{L}^\times/l^\times$$

$$W_K^\alpha \xrightarrow{\psi^*} W_L^\alpha$$

where $K$ and $L$ are function fields over algebraically closed ground fields $k$ and $l$. We are interested in situations when $\psi_1$ maps subgroups of the form $E^\times/k^\times$, where $E \subset K$ is a subfield with $\text{tr deg}_k(E) = 1$, into similar subgroups in $L^\times/l^\times$. The dual homomorphisms

$$(4.1) \quad \psi^* : W_L^\alpha \to W_K^\alpha$$

to such $\tilde{\psi}_1$ respect the fans, in the following sense: for all $\sigma \in \Sigma_L$ either $\psi^*(\sigma) \in \Sigma_K$ or $\psi^*(\sigma)$ is cyclic.

**Example 10.** The following examples of homomorphisms $\psi^*$ as in Equation (4.1) arise from geometry:

1. If $X \to Y$ is a dominant map of varieties over $k$ then $k(Y) = L \subset K = k(X)$ and the induced homomorphism

$$\psi^* : W_K^\alpha \to W_L^\alpha$$
respects the fans.

(2) Let \( \pi : X \to Y \) be a dominant map of varieties over \( k \) and \( s : Y \to X \) a section of \( \pi \). There exists a valuation \( \nu \in \mathcal{V}_K \) with center \( s(Y) \) such that

\[
L^\times \subset o_\nu^\times \subset K^\times
\]

and the natural projection

\[
\rho_\nu : o_\nu^\times \to K_\nu^\times
\]

onto the multiplicative group of the residue field induces an isomorphism

\[
L^\times \simeq K_\nu^\times
\]

which extends to an isomorphism of fields

\[
L \simeq K_\nu.
\]

Let \( \tilde{\rho}_\nu : K^\times \to L^\times \) be any multiplicative extension of \( \rho_\nu \) to \( K^\times \). Such \( \tilde{\rho}_\nu \) map multiplicative subgroups of the form \( k(x)^\times \) to similar subgroups of \( L^\times \), i.e., the dual map

\[
W^a_L \to W^a_K
\]

preserves the fans.

(3) More generally, let \( \nu \in \mathcal{V}_K \) be a valuation, with valuation ring \( o_\nu \), maximal ideal \( m_\nu \) and residue field \( K_\nu \). Combining the exact sequences

\[
1 \to o_\nu^\times \to K^\times \overset{\nu}{\to} \Gamma_\nu \to 1
\]

\[
1 \to (1 + m_\nu)^\times \to o_\nu^\times \overset{\rho_\nu}{\to} K_\nu^\times \to 1
\]

we have an exact sequence

\[
1 \to K_\nu^\times \to (1 + m_\nu)^\times \backslash K^\times \to \Gamma_\nu \to 1.
\]

Let \( K_\nu = k(Y) \), for some algebraic variety \( Y \) over \( k \), and let \( L \) be any function field containing \( K_\nu = k(Y) \). Assume that there is a diagram
\[ \begin{array}{c}
o^\times_{\nu}/k^\times \\ \downarrow \rho_{\nu} \\
K^\times_{\nu}/k^\times \phi \\
\downarrow \psi_1 \\
L^\times/k^\times
d\end{array} \]

where \( \phi \) is injective and \( \psi_1 \) is an extension of \( \phi \). Such extensions exist provided we are given a splitting of \( \nu : K^\times \to \Gamma_{\nu} \). In this case, we will say that \( \psi_1 \) is defined by a valuation. The dual map to such \( \psi_1 \) respects the fans. Theorem [11] shows a converse result: any \( \psi_1 \) respecting one-dimensional subfields can be obtained via this construction.

We proceed to describe the restriction of \( \psi_1 \) to projective subspaces of \( \mathbb{P}_k(K) \), when \( \psi_1 \) is obtained from this geometric construction; in particular, \( \psi_1 \) is not injective. In this case, for any \( E = k(x) \subset K \) the restriction of \( \psi_1 \) to \( E^\times/k^\times \) is either

- injective, or
- its restriction to \( I(1, x) \) is constant on the complement of one point, i.e., it factors through a valuation homomorphism.

On planes \( \mathbb{P}^2(1, x, y) \) there are more possibilities: an inertia element

\[ \iota = \iota_{\nu} \in W^a_K = \text{Hom}(K^\times/k^\times, \mathbb{Z}) \]

restricts to any \( \mathbb{P}^2 = \mathbb{P}^2_k(1, x, y) \) as a flag map, in particular, it takes at most three values. This leads to the following cases:

(a) \( \iota \) is constant on \( \mathbb{P}^2(1, x, y) \); then \( \mathbb{P}^2(1, x, y) \subset o^\times_{\nu}/k^\times \) since the corresponding linear space does not intersect the maximal ideal \( m_{\nu} \) and contains 1. The projection

\[ \rho_{\nu} : \mathbb{P}^2(1, x, y) \to K^\times_{\nu}/k^\times \]

is injective. If \( x, y \) are algebraically independent the values of \( \psi_1 \) on \( \mathbb{P}^2(1, x, y) \) are algebraically independent in \( K^\times_{\nu} \).

(b) \( \iota \) takes two values and (after an appropriate multiplicative shift) is constant on \( \mathbb{P}^2(1, x, y) \setminus \{ x \} \); in this case \( \psi_1 \) on \( \mathbb{P}^2(1, x, y) \setminus \{ x \} \) is a composition of a projection from \( x \) onto \( I(1, y) \) and an embedding of \( I(1, y) \hookrightarrow K^\times_{\nu}/k^\times \) with the map \( x \mapsto \iota(x) \).

(c) \( \iota \) takes two values and is constant on the complement of a projective line, say \( I(x, y) \); then \( \psi_1 \equiv 1 \) on the complement to \( I(x, y) \). Note that \( 1/x \cdot I(x, y) \subset o^\times_{\nu} \) and hence embeds into \( K^\times_{\nu}/k^\times \).
The proof of Theorem 11 below relies on a reconstruction of these and similar flag structures from fan data, more precisely, it involves a construction of a special multiplicative subset $\mathfrak{o}^\times \subset K^\times /k^\times$ which will be equal to $\mathfrak{o}^\times _\nu /k^\times$, for some valuation $\nu \in V_K$.

**Theorem 11.** Assume that $K, L$ are function fields over algebraic closures of finite fields $k, l$, respectively. Assume that

(a) $\psi_1 : K^\times /k^\times \to L^\times /l^\times$ is a homomorphism such that 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 $L^\times /l^\times$.

If $\psi_1$ is not injective then

(1) there is a $\nu \in V_K$ such that $\psi_1$ is trivial on $(1+m_\nu)^\times /k^\times \subset \mathfrak{o}^\times _\nu /k^\times$;

(2) the restriction of $\psi_1$ to $(4.2)$

$K^\times _\nu /k^\times = \mathfrak{o}^\times _\nu /k^\times (1+m_\nu)^\times \to L^\times /l^\times$

is injective and satisfies (a).

If $\psi_1$ is injective, then there exists a subfield $F \subset L$, a field isomorphism $\phi : K \sim F \subset L$, and an integer $m \in \mathbb{Z}$, coprime to $p$, such that $\psi_1$ coincides with the homomorphism induced by $\phi^m$.

The case of injective $\psi_1$ has been treated in [8]. The remainder of this section is devoted to the proof of Theorem 11 in the case when $\psi_1$ is not injective.

An immediate application of Condition (a) is: if $f \approx f'$, i.e., $f, f'$ are algebraically dependent then $\psi_1(f) \approx \psi_1(f')$. The converse does not hold, in general, and we are lead to introduce the following decomposition:

$(4.3)$ $\mathbb{P}_k(K) = S_1 \sqcup_f S_f$, 

(d) $\iota$ takes three values.
where
\[ S_1 := \psi_1^{-1}(1) \]
and, for \( f \notin S_1 \),
\[ S_f := \{ f' \in \mathbb{P}_k(K) \mid S_1 \psi_1(f') \approx \psi_1(f) \} \subset \mathbb{P}_k(K) \]
are equivalence classes of elements whose images are algebraically dependent. We record some properties of this decomposition:

**Lemma 12.**

1. For all \( f \), the set \( S_1 \cup S_f \) is closed under multiplication,
   \[ f', f'' \in S_1 \cup S_f \Rightarrow f' \cdot f'' \in S_1 \cup S_f. \]
2. Every projective line \( l(1, f) \subset \mathbb{P}_k(K) \), with \( \psi_1(f) \neq 1 \), is contained in \( S_1 \cup S_f \).
3. Assume that \( f, g \) are such that \( \psi_1(f), \psi_1(g) \) are nonconstant and distinct. If \( \psi_1(f) \approx \psi_1(g) \) then \( l(f, g) \in S_1 \cup S_f \). Otherwise, \( l(f, g) \cap S_1 = \emptyset \).
4. Let \( \Pi \subset \mathbb{P}_k(K) \) be a projective subspace such that there exist \( x, y, z \in \Pi \) with distinct images and such that \( \psi_1(x/z) \neq \psi_1(y/z) \).
   Then, for any \( h \in K^*/k^* \), the projective subspace \( \Pi' := h \cdot \Pi \) satisfies the same property.

**Proof.** The first property is evident. Condition (a) of Theorem [11] implies that for every \( f \in K^*/k^* \) we have
\[ \psi_1(l(1, f)) \subset \mathbb{P}_l(F), \quad F = l(\psi_1(f)), \]
this implies the second property.

Considering the shift \( l(f, g) = f \cdot l(1, g/f) \) we see that
\[ \psi_1(l(f, g)) \subset \psi_1(f) \cdot \psi_1(l(1, g/f)) \subset \psi_1(f) \cdot \mathbb{P}_l(F), \]
where \( F = l(\psi_1(g/f)) \). If \( \psi_1(f) \approx \psi_1(g/f) \) then \( \psi_1(l(f, g)) \subset S_1 \cup S_f \).
Otherwise, \( \psi_1(l(f, g)) \) is disjoint from \( 1 \).

To prove the last property is suffices to remark that \( \psi_1(\Pi') \) contains \( \psi_1(hx), \psi_1(hy), \psi_1(hz) \), and \( \psi_1(hx/hz) \neq \psi_1(hy/hz) \). \( \square \)

**Lemma 13.** Let \( \Pi = \mathbb{P}^2 \subset \mathbb{P}_k(K) \) be a projective plane satisfying condition (4) of Lemma [12] and such that the restriction of \( \psi_1 \) to \( \Pi \) is not injective. Then

1. there exists a line \( l \subset \Pi \) such that \( \psi_1 \) is constant on \( \Pi \setminus l \) or
2. there exists a \( g \subset \Pi \) such that
   - \( \psi_1 \) is constant on every punctured line \( l(g, f) \setminus g \).
- \( \psi_1(g) \neq \psi_1(f) \), for every \( f \neq g \);
- \( \psi_1(f) \approx \psi_1(f') \) for all \( f, f' \neq g \).

**Proof.** After an appropriate shift and relabeling, and using Lemma \[12\] we may assume that \( \Pi = \mathbb{P}^2(1, x, y) \) and that \( \psi_1^{-1}(1) \) contains a nontrivial element \( z \in \mathbb{P}^2(1, x, y) \), i.e., \( z \in S_1 \). Let

\[
\mathbb{P}^2(1, x, y) = S_1 \cup_{f \in F} S_f
\]

be the decomposition induced by \([13]\).

**Step 1.** Neither of the sets \( S_1 \) nor \( S_f \) contains a line. Indeed, assume that there is a projective line \( l \subseteq S_1 \) and let \( g \in \mathbb{P}^2(1, x, y) \setminus S_1 \). Every \( f' \in \mathbb{P}^2(1, x, y) \) lies on a line through \( g \) and \( l(f', g) \) which intersects \( l \), and thus \( S_1 \), i.e., all \( f' \) lie in \( S_1 \cup S_g \), by Lemma \([12]\). Assume that \( l \subseteq S_f \). Every \( g \in \mathbb{P}^2(1, x, y) \setminus S_1 \) lies on a line of the form \( l(1, g) \), which intersects \( l \subseteq S_f \). It follows that \( g \in S_f \), contradicting our assumption that \( \psi_1(\mathbb{P}^2(1, x, y)) \) contains at least two algebraically independent elements.

**Step 2.** Split \( F = F' \sqcup F'' \) into nonempty subsets, arbitrarily, and let

\[
\mathbb{P}^2(1, x, y) = S_1 \cup S' \cup S'', \quad S' := \sqcup_{f \in F} S_f, \quad S' := \sqcup_{f'' \in F} S_f''
\]

be the induced decomposition. By Lemma \([12]\) every \( l \) is in either \( S_1 \cup S' \), \( S_1 \cup S'' \), or \( S' \cup S'' \).

By Lemma \([7]\), one of these subsets is a flag subset of \( \mathbb{P}^2(1, x, y) \).

**Step 3.** Assume that \( S_1 \) is a flag subset. Since it contains at least two elements and does not contain a projective line, by Step 1, we have:

- \( S_1 = \mathbb{P}^2 \setminus l \), for some line \( l \), and we are in Case (1), or
- \( S_1 = l(1, z)^\circ = l(1, z) \setminus g \), for some \( g \in S' \) (up to relabeling).

Choose a \( g'' \in S'' \), so that \( \psi_1(g'') \neq \psi_1(g) \), and let \( l \) be a line through \( g'' \), \( l \neq l(g, g'') \). Then \( l \) intersects \( l(1, z)^\circ = S_1 \), which implies that the complement \( l \setminus (l \cap l(1, z)^\circ) \subseteq S'' \). It follows that \( S'' \) contains the complement of \( l(1, z) \cap l(g, g'') \). Considering projective lines through \( l \) and elements in \( S'' \) and applying Lemma \([12]\) we find that \( S'' \supseteq \mathbb{P}^2(1, x, y) \setminus l(1, z) \). Since \( g \notin S'' \), we have equality. Thus all elements in \( \mathbb{P}^2(1, x, y) \setminus g \) have algebraically dependent images. If \( \psi_1 \) were not constant on a line \( l \) through \( g \), with \( l \neq l(1, z) \), let \( f_1, f_2 \in l \) be elements with \( \psi_1(f_1) \neq \psi_1(f_2) \). Lemma \([12]\) implies that \( g \in S_{f_1} \), contradicting our assumption that \( \psi_1(g) \neq \psi_1(f_1) \). Thus we are in Case (2).
Step 4. Assume that $S'$ is a flag subset and $S_1$ is not. We have the following cases:

- $S' = \{g\}$. Then $S' = S_g$ and $I(1, g)^{\circ} := I(1, g) \setminus g \subseteq S_1$. Assume that there exist $f_1, f_2 \in \mathbb{P}^2(1, x, y) \setminus I(1, g)$ with $\psi_1(f_1) \neq \psi_1(f_2)$. If $f_2 \notin I(g, f_1)$ then $\psi_1(f_1) \approx \psi_1(f_2)$, as $I(f_1, f_2)$ intersects $I(1, g)^{\circ}$. If there exists at least one $f_2 \notin I(g, f_1)$ with nonconstant $\psi_1(f_2)$, then by the argument above, all elements on the complement to $I(1, g)$ are algebraically dependent, on every line $l$ through $g$, $\psi_1$ is constant on $l \setminus g$, and we are in Case (2). If $\psi_1$ is identically 1 on $\mathbb{P}^2(1, x, y) \setminus I(g, f_1)$ then $\psi_1 \neq 1$ on $I(g, f_1)$ (otherwise $S_1$ would contain a projective line). Thus $S_1$ is a flag subset, contradiction.

- $S' = I^c = I \setminus g$, for some line $l$ and $g \in I$. Since $S_1$ has at least two elements, there is a $z' \in (\mathbb{P}^2 \setminus l) \cap S_1$. Lemma [12] implies that $\psi_1$ equals 1 on $I(z', g') \setminus g'$, for all $g' \in S' = I^c$. Similarly, $\psi_1$ equals 1 on $I(g, z') := I(g, z') \setminus g$, as every point on this punctured line lies on a line passing through $S_1$ and intersecting $S'$. Thus $S_1 \supseteq \mathbb{P}^2(1, x, y) \setminus I$ and since $S_1$ does not contain a line, these sets must be equal. It follows that we are in Case (1).

- Assume that $S' = \mathbb{P}^2(1, x, y) \setminus I$ and we are not in the previous case. Then $I$ contains at least two points in $S_1$ and the complement $S'' = I \setminus (I \cap S_1)$ also has at least two points, $f''_1, f''_2$. Thus $S'' = S_{f''}$ for some $f''$, by Lemma [12]. Since we were choosing the splitting $\mathcal{F} = \mathcal{F}' \sqcup \mathcal{F}''$ arbitrarily, we conclude that $S' = S_{f'}$ for some $f'$.

The same argument as in Step 3 implies that $\psi_1$ is constant on $I(g', f''_i) \setminus f''_i$ for any $g' \in S'$. Hence $\psi_1$ is constant on $\mathbb{P}^2(1, x, y) \setminus I$ and we are in Case (1).

\[\square\]

Lemma 14. Let

\[u := \cup I(1, x) \subseteq K^\times/k^\times = \mathbb{P}_k(K)\]

be union over all lines such that $\psi_1$ is injective on $I(1, x)$. Assume that there exist nonconstant $x, y \in u$ such that $\psi_1(x) \neq \psi_1(y)$. Then

\[o^\times := u \cdot u \subset \mathbb{P}_k(K)\]

is a multiplicative subset.

Proof. First of all, if $x \in u$ then $x^{-1} \in u$, since $I(1, x) = x \cdot I(1, x^{-1})$. 


It suffices to show that \( u \cdot o^x = o^x \), i.e., for all \( x, y, z \in u \) one has \( xyz = tw \), for some \( t, w \in u \).

Assume first that \( \psi_1(x) \not\approx \psi_1(y) \) and consider \( \mathbb{P}^2(1, x, y^{-1}) \). A shift of this plane contains the line \( \ell(1, xy) \). If \( xy \not\in u \) then \( \psi_1 \) is not injective on this plane and we may apply Lemma 13. We are not in Case (1) and not in Case (2), since \( \psi_1 \) injects \( \ell(1, x) \) and \( \ell(1, y^{-1}) \), contradiction. Thus \( \psi_1 \) is injective on \( \mathbb{P}^2(1, x, y^{-1}) \) and \( xy = t \), for some \( t \in u \), which proves the claim.

Now assume that \( \psi_1(x), \psi_1(y), \psi_1(z) \in F^x / l^x \), for some 1-dimensional \( F \subset L \). By assumption, there exists a \( w \in K^x / k^x \) such that \( \psi_1(w) \) is algebraically independent of \( F^x / l^x \) and such that \( \ell(1, w) \) injects. By the previous argument, \( \psi_1 \) is injective on the lines \( \ell(1, xw) \) and \( \ell(1, w^{-1}y) \), so that \( xw, w^{-1}y \in u \). By our assumptions, \( \psi_1 \) is injective on \( \ell(1, z) \). Now we repeat the previous argument for \( xw \) and \( z \): there is a \( t \in u \) such that \( xw \cdot z = t \). \( \square \)

**Proposition 15.** Let

\[
\psi_1 : K^x / k^x \to L^x / l^x
\]

be a homomorphism satisfying the assumptions of Theorem 14 and such that \( u \subset \mathbb{P}_x(K) \) contains \( x, y \) with \( \psi_1(x) \not\approx \psi_1(y) \). Let \( o^x = u \cdot u \subset K^x / k^x \) be the subset defined above. Then

\[
\nu : K^x / k^x \to K^x / o^x
\]

is a valuation homomorphism, i.e., there exists an ordered abelian group \( \Gamma_\nu \) with \( K^x / o^x \simeq \Gamma_\nu \) and \( \nu \) is the valuation map.

**Proof.** By Lemma 14 we know that \( o^x \) is multiplicative. We claim that the restriction of \( \nu \) to every \( \mathbb{P}^1 \subset \mathbb{P}_x(K) \) is a flag map. Indeed, we have \( \mathbb{P}^1 = x \cdot \ell(1, y) \), for some \( x, y \in K^x / k^x \). On every line \( \ell(1, y) \subset u \), the value of \( \nu \) is 1, and on every line \( \ell(1, x) \not\subset u \), the value of \( \nu \) is constant on the complement to one point.

By Proposition 5, this implies that \( \nu \) is a flag map, i.e., defines a valuation on \( K^x / k^x \) with values on \( \Gamma_\nu := K^x / o^x \). \( \square \)

To complete the proof of Theorem 14 we need to treat homomorphisms \( \psi_1 \) such that for most one-dimensional \( E \subset K \), the image \( \psi_1(E^x / k^x) \) is cyclic, or even trivial. We have two cases:

(A) there exists a line \( \ell = (1, x) \) such that \( \psi_1 \) is not a flag map on this line.
(B) \( \psi_1 \) is a flag map on every line \( l \subset \mathbb{P}_k(K) \).

In Case (A), let \( u' \) be the union of lines \( l(1, x) \) such that \( \psi_1 \) is not a flag map on \( l(1, x) \), i.e., is not constant on the line minus a point. By the arguments in Lemma 13, Lemma 14, and Proposition 15, there exists a unique 1-dimensional normally closed subfield \( F \subset L \) such that \( \psi_1(u') \subseteq F^\times/l^\times \). Define

\[
\mathfrak{o}^\times := \psi_1^{-1}(F^\times/l^\times) \subset K^\times/k^\times.
\]

By assumption on \( \psi_1 \), \( \mathfrak{o}^\times \) is a proper multiplicative subset of \( K^\times/k^\times \). The induced homomorphism

\[
\nu : K^\times/k^\times \to (K^\times/k^\times)/\mathfrak{o}^\times =: \Gamma_\nu
\]

is a valuation map, since it is a flag map on every line \( l \subset \mathbb{P}_k(K) \). Indeed, it is constant on all \( l(1, x) \subseteq u \) and a valuation map on all \( l(1, y) \not\subseteq \mathfrak{o}^\times \). Hence the same holds for any projective line in \( \mathbb{P}_k(K) \) which implies the result.

In Case (B), we conclude that \( \psi_1 \) is a flag map on \( \mathbb{P}_k(K) \) (see, e.g., Lemma 4.16 of [7]), i.e., there exists a valuation \( \nu \in V_K \) with value group \( \Gamma_\nu = \psi_1(K^\times/k^\times) \) such that the valuation homomorphism \( \nu = \psi_1 \).

**Remark 16.** The main steps of the proof (Lemmas 12, 13, and 14) are valid for more general fields: the splitting of \( \mathbb{P}^2 \) into subsets satisfying conditions (1) and (2) of Lemma 12 is related to a valuation, independently of the ground field (see [3]). Here we restricted to \( k = \bar{\mathbb{F}}_p \), since in this case the proof avoids some technical details which appear in the theory of general valuations. Furthermore, the condition that \( K, L \) are function fields is also not essential. The only essential property is the absence of an infinite tower of roots for the elements of \( K, L \) which are not contained in the ground field.

**5. Galois cohomology**

By duality, the main result of Section 4 confirms the general concept that birational properties of algebraic varieties are functorially encoded in the structure of the Galois group \( G_K^c \). On the other hand, it follows from the proof of the Bloch–Kato conjecture that \( G_K^c \) determines the full cohomology of \( G_K \). Here and in Section 5 we discuss group-theoretic properties of \( G_K \) and its Sylow subgroups which we believe are ultimately responsible for the validity of the Bloch–Kato conjecture.
Let $G$ be a profinite group, acting continuously on a topological $G$-module $M$, and let $H^i(G, M)$ be the (continuous) $i$-cohomology group. These groups are contravariant with respect to $G$ and covariant with respect to $M$; in most of our applications $M$ either $\mathbb{Z}/\ell$ or $\mathbb{Q}/\mathbb{Z}$, with trivial $G$-action. We recall some basic properties:

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

up to homotopy.

- if $G$ is abelian and $M$ finite with trivial $G$-action then $H^n(G, M) = \wedge^n(H^1(G, M))$, for all $n \geq 1$,

- if $M = \mathbb{Z}/\ell^m$ then $H^n(G, M) \hookrightarrow H^n(\mathcal{G}_\ell, M)$, for all $n \geq 0$,

where $\mathcal{G}_\ell$ is the $\ell$-Sylow subgroup of $G$.

See [1] for further background on group cohomology and [20], [24] for background on Galois cohomology. Let

$$G^{(n)} := [G^{(n-1)}, G^{(n-1)}]$$

the $n$-th term of its derived series, $G^{(1)} = [G, G]$. We will write

$$G^a = G/[G, G], \quad \text{and} \quad G^c = G/[[G, G], G]$$

for the abelianization, respectively, the second lower central series quotient of $G$. Consider the diagram, connecting the first terms in the derived series of $G$ with those in the lower central series:

$$
\begin{array}{cccccc}
1 & \longrightarrow & G^{(1)} & \longrightarrow & G & \longrightarrow & G^a & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & Z & \longrightarrow & G^c & \longrightarrow & G^c & \longrightarrow & 1
\end{array}
$$

We have a homomorphism between $E_2$-terms of the spectral sequences computing $H^n(G, \mathbb{Z}/\ell^m)$ and $H^n(G^c, \mathbb{Z}/\ell^m)$, respectively. Suppressing the coefficients, we have
\[
\begin{array}{ccccccccc}
H^p(G^a, H^q(Z)) & \rightarrow & E_2^{p,q}(G^c) & \rightarrow & E_2^{p+q}(G^c) & \rightarrow & H^{p+q}(G^c) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
H^p(G^a, H^q(G^{(1)})) & \rightarrow & E_2^{p,q}(G) & \rightarrow & E_2^{p+q}(G) & \rightarrow & H^{p+q}(G) \\
\end{array}
\]

We have \(H^0(G, \mathbb{Z}/\ell^m) = \mathbb{Z}/\ell^m\), for all \(m \in \mathbb{N}\), and
\[
H^0(G^a, H^1(Z)) = H^1(Z).
\]

The diagram of corresponding five term exact sequences takes the form:

\[
\begin{array}{ccccccccc}
H^1(G^a) & = & H^1(G) & \rightarrow & H^1(Z) & \rightarrow & H^2(G^a) & \rightarrow & H^2(G) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
H^1(G^a) & = & H^1(G) & \rightarrow & H^0(G^a, H^1(G^{(1)})) & \rightarrow & H^2(G^a) & \rightarrow & H^2(G) \\
\end{array}
\]

where the left arrows map \(H^1(G)\) to zero.

Let \(K\) be any field containing \(\ell^m\)-th roots of 1, for all \(m \in \mathbb{N}\), and let \(G_K\) be its absolute Galois group. We apply the cohomological considerations above to \(G_K\). By Kummer theory,

\[
(5.1) \quad H^1(G_K, \mathbb{Z}/\ell^m) = H^1(G_K^a, \mathbb{Z}/\ell^m) = K_1(K)/\ell^m
\]

and we obtain a diagram

\[
\begin{array}{ccccccccc}
H^1(G_K^a, \mathbb{Z}/\ell^m) & \otimes & H^1(G_K^a, \mathbb{Z}/\ell^m) & \xrightarrow{s_K} & \wedge^2 (H^1(G_K^a, \mathbb{Z}/\ell^m)) & = & H^2(G_K^a, \mathbb{Z}/\ell^m) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
K_1(K)/\ell^m \otimes K_1(K)/\ell^m & \xrightarrow{\sigma_K} & K_2(K)/\ell^m \\
\end{array}
\]

where \(s_K\) is the symmetrization homomorphism and \(\sigma_K\) is the symbol map, and \(\text{Ker}(\sigma_K)\) is generated by symbols of the form \(f \otimes (1 - f)\). The Steinberg relations imply that

\[
\text{Ker}(s) \subseteq \text{Ker}(\sigma_K)
\]

(see, e.g., [19, Section 11]). We obtain a diagram

\[
\begin{array}{ccccccccc}
H^1(Z_K, \mathbb{Z}/\ell^m) & \xleftarrow{d_2} & H^2(G_K^a, \mathbb{Z}/\ell^m) & \xrightarrow{\pi_K^*} & H^2(G_K, \mathbb{Z}/\ell^m) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
I_K(2)/\ell^m & \xleftarrow{\wedge^2 (H^1(G_K^a, \mathbb{Z}/\ell^m))} & K_2(K)/\ell^m
\end{array}
\]

\[
\begin{array}{ccccccccc}
H^1(Z_K, \mathbb{Z}/\ell^m) & \xleftarrow{d_2} & H^2(G_K^a, \mathbb{Z}/\ell^m) & \xrightarrow{\pi_K^*} & H^2(G_K, \mathbb{Z}/\ell^m) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
I_K(2)/\ell^m & \xleftarrow{\wedge^2 (H^1(G_K^a, \mathbb{Z}/\ell^m))} & K_2(K)/\ell^m
\end{array}
\]
where $h_K$ is the Galois symbol (cf. [24, Theorem 6.4.2]) and $I_K(2)$ is defined by the exact sequence

$$1 \to I_K(2) \to \wedge^2(K^\times) \to K_2(K) \to 1.$$ 

A theorem of Merkurjev–Suslin [18] states that $h_K$ is an isomorphism

(5.2) $H^2(G_K, \mathbb{Z}/\ell^m) = K_2(K)/\ell^m$.

This is equivalent to:

- $\pi^*_a: H^2(G^n_K, \mathbb{Z}/\ell^m) \to H^2(G_K)$ is surjective
- $H^1(Z_K, \mathbb{Z}/\ell^m) = I_K(2)/\ell^m$.

The Bloch–Kato conjecture, proved by Voevodsky, Rost, and Weibel, generalizes (5.1) and (5.2) to all $n$. This theorem is of enormous general interest, with far-reaching applications to algebraic and arithmetic geometry. It states that for any field $K$ and any prime $\ell$, one has an isomorphism between Galois cohomology and the mod $\ell$ Milnor $K$-theory:

(5.3) $H^n(G_K, \mu_{\ell^n}) = K^n_M(K)/\ell$.

It substantially advanced our understanding of relations between fields and their Galois groups, in particular, their Galois cohomology. Below we will focus on Galois-theoretic consequences of (5.3).

We have canonical central extensions

and the diagram

and the diagram

and the diagram

and the diagram
The following theorem relates the Bloch–Kato conjecture to statements in Galois-cohomology (see also [11], [12], [28], and [13]).

**Theorem 17.** [4, 9, Theorem 11] Let $k = \overline{\mathbb{F}}_p$, $p \neq \ell$, and $K = k(X)$ be the function field of an algebraic variety of dimension $\geq 2$. The Bloch–Kato conjecture for $K$ is equivalent to:

1. The map
   \[ \pi_a^*: H^*(G_K^a, \mathbb{Z}/\ell^n) \rightarrow H^*(G_K, \mathbb{Z}/\ell^n) \]
   is surjective and
2. \( \text{Ker}(\pi_a^* \circ \pi_c) = \text{Ker}(\pi_a^*). \)

This implies that the Galois cohomology of the pro-$\ell$- quotient $G_K$ of the absolute Galois group $G_K$ encodes important birational information of $X$. For example, in the case above, $G_K^a$, and hence $K$, modulo purely-inseparable extensions, can be recovered from the cup-products

\[ H^1(G_K, \mathbb{Z}/\ell^n) \times H^1(G_K, \mathbb{Z}/\ell^n) \rightarrow H^2(G_K, \mathbb{Z}/\ell^n), \quad n \in \mathbb{N}. \]

6. **Freeness**

Let $K$ be a function field over an arbitrary ground field $k$ and $G_K$ the absolute Galois group of $K$. The pro-$\ell$-quotient $G_K$ of $K$ is highly individual: for $k = \overline{\mathbb{F}}_p$ it determines $K$ up to purely-inseparable extensions. On the other hand, let $\mathfrak{S}_\ell(G_K)$ be an $\ell$-Sylow subgroup of $G_K$. This group is *universal*, in the following sense:

**Proposition 18.** [5] Assume that $X$ has dimension $n$ and that $X$ contains a smooth $k$-rational point. Then

\[ \mathfrak{S}_\ell(G_K) = \mathfrak{S}_\ell(G_{k(\mathbb{P}^n)}). \]

In particular, when $k$ is algebraically closed, the $\ell$-Sylow subgroups depend only on the dimension of $X$. This universal group will be denoted by $\mathfrak{S}_\ell$. The following *Freeness* conjecture captures an aspect of this universality. It implies the (proved) Bloch–Kato conjecture; but more importantly, it provides a structural explanation for its truth.

**Conjecture 19** (Bogomolov). Let $k$ be an algebraically closed field of characteristic $\neq \ell$, $X$ an algebraic variety over $k$ of dimension $\geq 2$, $K = k(X)$, and write

\[ \mathfrak{S}_\ell^{(1)} := [\mathfrak{S}_\ell, \mathfrak{S}_\ell] \]
for the commutator of an \( \ell \)-Sylow subgroup of \( G_K \). Then

\[
(6.1) \quad H^i(\mathfrak{g}_\ell^{(1)}, \mathbb{Z}/\ell^m) = 0, \quad \text{for all} \quad i \geq 2, m \in \mathbb{N}.
\]

**Remark 20.** For profinite \( \ell \)-groups, the vanishing in Equation (6.1) for \( i = 2 \) implies the vanishing for all \( i \geq 2 \) (see [17]).

We now return to the cohomological considerations in Section 5. The standard spectral sequence associated with

\[
1 \to G^{(1)} \to G \to G^a \to 1,
\]
gives

\[
H^p(G^a, H^q(G^{(1)}, \mathbb{Z}/\ell^m)) \Rightarrow H^n(G, \mathbb{Z}/\ell^m).
\]

We apply this to \( G = \mathfrak{g}_\ell \); suppressing the coefficients we obtain:

\[
\begin{array}{cccccc}
0 & 0 & 0 & \cdots \\
H^0(G^a, H^2(G^{(1)})) & 0 & 0 & \cdots \\
H^0(G^a, H^1(G^{(1)})) & H^1(G^a, H^1(G^{(1)})) & H^2(G^a, H^1(G^{(1)})) & \cdots \\
\end{array}
\]

Conjecture [19] would imply that, for \( G = \mathfrak{g}_\ell \), and also for \( G = G_K \), \( H^2(G^{(1)}) \) and consequently all entries above the second line vanish. In this case, we have a long exact sequence (see, e.g., [24, Lemma 2.1.3])

\[
0 \to H^1(G^a) \to H^1(G) \to H^0(G^a, H^1(G^{(1)})) \to H^2(G^a) \to \cdots
\]

\[
\cdots \to H^n(G^a, H^1(G^{(1)})) \xrightarrow{d_2} H^{n+2}(G^a) \to H^{n+2}(G) \to \cdots
\]

In Section 5 we saw that for \( n = 0 \) the homomorphism \( d_2' \) in the sequence

\[
H^n(G^a_K, H^1(G^{(1)})) \xrightarrow{d_2'} H^{n+2}(G^a_K) \to H^{n+2}(G_K) = K_{n+2}(K)/\ell^m
\]

can be interpreted as the embedding of the skew-symmetric relations:

\[
H^0(G^a, H^1(\mathbb{Z})) = I_K(2)/\ell^m \xrightarrow{d_2'} \wedge^2(H^1(G^a_K)) = \wedge^2(K^\times/\ell^m) \to K_2(K)/\ell^m.
\]
This relied on Kummer theory and the Merkurjev–Suslin theorem. We proceed to interpret the differential $d_2$ for higher $n$.

We work with $G = \mathfrak{G}_\ell$, an $\ell$-Sylow subgroup of the absolute Galois group of a function field $K$ over an algebraically closed field. We have an exact sequence of continuous $G^a$-modules

$$1 \to [G, G^{(1)}] \to G^{(1)}/G^{(2)} \to Z \to 1.$$  

Note that $G^a$ acts trivially on $Z$, and $H^1(Z)$, and via $x \mapsto gxg^{-1} - x$ on $G^{(1)}/G^{(2)}$. Dually we have a sequence of $G^a$-modules:

$$\text{Hom}([G, G^{(1)}], \mathbb{Z}/\ell^m) \leftarrow \text{Hom}(G^{(1)}/G^{(2)}, \mathbb{Z}/\ell^m) \leftarrow \text{Hom}(Z, \mathbb{Z}/\ell^m) \leftarrow 1.$$  

Define

$$M := \text{Hom}(G^{(1)}/G^{(2)}, \mathbb{Z}/\ell^m),$$  

then

$$M^{G^a} = \text{Hom}(Z, \mathbb{Z}/\ell^m) = H^1(Z) = I_K(2)/\ell^m.$$  

We have a homomorphism

$$H^n(M^{G^a}) \to H^n(M) \tag{6.2}$$  

via the natural embedding. Since $H^0(M^{G^a})$ embeds into $H^2(G^a)$ via $d_2$ we obtain a natural homomorphism

$$t_n : H^n(M^{G^a}) \to H^{n+2}(G^a)$$  

and the differential $d_2$ on the image of $H^n(M^{G^a}) \to H^n(M)$ coincides with $t_n$. Thus the fact that the kernel of $H^n(G^a) \to H^n(G)$ is generated by trivial symbols will follow from the surjectivity of the homomorphism in (6.2). This, in turn, would follow if the projection $M \to M/M^{G^a}$ defined a trivial map on cohomology. Thus we can formulate the following conjecture which complements the Freeness conjecture \cite{19}.

**Conjecture 21.** The projection $M \to M/M^{G^a}$ can be factored as

$$M \leftrightarrow D \to M/M^{G^a},$$  

where $D$ is a cohomologically trivial $G^a$-module.

We hope that a construction of a natural module $D$ can be achieved via algebraic geometry.
REFERENCES

[1] A. ADEM & R. J. MILGRAM – Cohomology of finite groups, second éd., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 309, Springer-Verlag, Berlin, 2004.

[2] E. ARTIN – “Selected topics in geometry, Part I”, 1954.

[3] F. BOGOMOLOV – “Abelian subgroups of Galois groups”, Izv. Akad. Nauk SSSR Ser. Mat. 55 (1991), no. 1, p. 32–67.

[4] ————, “On two conjectures in birational algebraic geometry”, in Algebraic geometry and analytic geometry (Tokyo, 1990), ICM-90 Satell. Conf. Proc., Springer, Tokyo, 1991, p. 26–52.

[5] ————, “On the structure of Galois groups of the fields of rational functions”, in K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992), Proc. Sympos. Pure Math., vol. 58, Amer. Math. Soc., Providence, RI, 1995, p. 83–88.

[6] F. BOGOMOLOV & Y. TSCHINKEL – “Commuting elements in Galois groups of function fields”, in Motives, Polylogarithms and Hodge theory, International Press, 2002, p. 75–120.

[7] ————, “Reconstruction of function fields”, Geom. Funct. Anal. 18 (2008), no. 2, p. 400–462.

[8] ————, “Milnor $K_2$ and field homomorphisms”, in Surveys in Differential Geometry XIII, International Press, 2009, p. 223–244.

[9] ————, “Introduction to birational anabelian geometry”, 2010, arXiv:1011.0883.

[10] ————, “Reconstruction of higher-dimensional function fields”, Moscow Math. Journal 11 (2011), no. 2, p. 185–204.

[11] S. K. CHEBOLU, I. EFRAT & J. MINÁČ – “Quotients of absolute Galois groups which determine the entire Galois cohomology”, 2009, arXiv:0905.1364.

[12] S. K. CHEBOLU & J. MINÁČ – “Absolute Galois groups viewed from small quotients and the Bloch-Kato conjecture”, in New topological contexts for Galois theory and algebraic geometry (BIRS 2008), Geom. Topol. Monogr., vol. 16, Geom. Topol. Publ., Coventry, 2009, p. 31–47.

[13] I. EFRAT & J. MINÁČ – “Galois groups and cohomological functors”, 2011, arXiv:1103.1508.

[14] ————, “Small Galois groups that encode valuations”, 2011, arXiv:1105.2427.

[15] A. GROTHENDIECK – “Brief an G. Faltings”, in Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, With an English translation on pp. 285–293, p. 49–58.

[16] Y. IHARA & H. NAKAMURA – “Some illustrative examples for anabelian geometry in high dimensions”, in Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, p. 127–138.

[17] H. KOCH – Galois theory of p-extensions, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.
[18] A. S. Merkur'ev & A. A. Suslin – “$K$-cohomology of Severi-Brauer varieties and the norm residue homomorphism”, Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982), no. 5, p. 1011–1046, 1135–1136.
[19] J. Milnor – *Introduction to algebraic $K$-theory*, Princeton University Press, Princeton, N.J., 1971, Annals of Mathematics Studies, No. 72.
[20] S. Mochizuki – “Topics surrounding the anabelian geometry of hyperbolic curves”, in *Galois groups and fundamental groups*, Math. Sci. Res. Inst. Publ., vol. 41, Cambridge Univ. Press, Cambridge, 2003, p. 119–165.
[21] H. Nakamura – “Galois rigidity of the étale fundamental groups of punctured projective lines”, J. Reine Angew. Math. 411 (1990), p. 205–216.
[22] H. Nakamura, A. Tamagawa & S. Mochizuki – “Grothendieck’s conjectures concerning fundamental groups of algebraic curves”, Sūgaku 50 (1998), no. 2, p. 113–129.
[23] J. Neukirch – “Kennzeichnung der $p$-adischen und der endlichen algebraischen Zahlkörper”, Invent. Math. 6 (1969), p. 296–314.
[24] J. Neukirch, A. Schmidt & K. Wingberg – *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.
[25] F. Pop – “Glimpses of Grothendieck’s anabelian geometry”, in *Geometric Galois actions, 1*, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, p. 113–126.
[26] ______, “Alterations and birational anabelian geometry”, in *Resolution of singularities (Obergurgl, 1997)*, Progr. Math., vol. 181, Birkhäuser, Basel, 2000, p. 519–532.
[27] ______, “On the birational anabelian program initiated by Bogomolov I”, 2011, to appear in Invent. Math.
[28] L. Positselski – “Koszul property and Bogomolov’s conjecture”, Int. Math. Res. Not. (2005), no. 31, p. 1901–1936.
[29] J.-P. Serre – *Galois cohomology*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.
[30] A. Tamagawa – “The Grothendieck conjecture for affine curves”, Compositio Math. 109 (1997), no. 2, p. 135–194.
[31] K. Uchida – “Isomorphisms of Galois groups of algebraic function fields”, Ann. Math. (2) 106 (1977), no. 3, p. 589–598.
[32] V. A. Voevodskiǐ – “Galois groups of function fields over fields of finite type over $\mathbb{Q}$”, Uspekhi Mat. Nauk 46 (1991), no. 5(281), p. 163–164.
[33] ______, “Galois representations connected with hyperbolic curves”, Izv. Akad. Nauk SSSR Ser. Mat. 55 (1991), no. 6, p. 1331–1342.
[34] A. N. Whitehead – *The axioms of projective geometry*, 1906.
GALOIS THEORY AND PROJECTIVE GEOMETRY

Courant Institute of Mathematical Sciences, N.Y.U., 251 Mercer str., New York, NY 10012, U.S.A.

E-mail address: bogomolo@cims.nyu.edu

Courant Institute of Mathematical Sciences, N.Y.U., 251 Mercer str., New York, NY 10012, U.S.A.

E-mail address: tschinkel@cims.nyu.edu