RECONSTRUCTION OF FUNCTION FIELDS

by

Fedor Bogomolov and Yuri Tschinkel

ABSTRACT. — We study the structure of abelian subgroups of Galois groups of function fields of surfaces.

Contents

KEY WORDS AND PHRASES. — Galois groups, function fields.

Introduction

We fix two distinct primes p and ℓ. Let $k = \bar{\mathbb{F}}_p$ be an algebraic closure of the finite field $\mathbb{F}_p$. Let X be an algebraic variety defined over k and $K = k(X)$ its function field. Let $\mathcal{G}_K^a$ be the abelianization of the pro-ℓ-quotient $\mathcal{G}_K$ of the absolute Galois group of K. Under our assumptions on k, $\mathcal{G}_K^a$ is a torsion-free $\mathbb{Z}_\ell$-module. Let $\mathcal{G}_K^c$ be its canonical central extension - the second lower central series quotient of $\mathcal{G}_K$. It determines the following structure: a *fan* Σ_K of distinguished (primitive) subgroups of $\mathcal{G}_K^a$ which are finite rank $\mathbb{Z}_\ell$-modules. A topologically noncyclic subgroup $\sigma \in \Sigma_K$ iff

- σ lifts to an abelian subgroup of $\mathcal{G}_K^c$;
- σ is maximal: there are no abelian subgroups $\sigma' \subset \mathcal{G}_K^a$ which lift to an abelian subgroup of $\mathcal{G}_K^c$ and contain σ as a proper subgroup.

THEOREM 1. — *Let K and L be function fields over algebraic closures of finite fields of characteristic $\neq \ell$. Assume that $K = k(X)$ is a function field of a surface X/k and that there exists an isomorphism*

$$\Psi = \Psi_{K,L} \,:\, \mathcal{G}_K^a \simeq \mathcal{G}_L^a$$

of abelian pro-ℓ-groups inducing a bijection of sets

$$\Sigma_K = \Sigma_L.$$

Then, for some $c \in \mathbb{Z}_\ell^*$, $c\Psi$ is induced by an isomorphism $\bar{\Psi}$ of the perfect closure of K with the perfect closure of L; the pair $(c, \bar{\Psi})$ is unique up to

$$(c, \bar{\Psi}) \mapsto (p^n c, (x \mapsto x^{p^n} \circ \bar{\Psi})).$$

We implement the program outlined in [1] and [2] describing the correspondence between higher-dimensional function fields and their abelianized Galois groups. For results concerning the reconstruction of function fields from their (full) Galois groups (the birational Grothendieck program) we refer to the works of Pop, Mochizuki and Efrat (see [9], [8],[5]).

Acknowledgments. Both authors were partially supported by the NSF. The second author was employed by the Clay Mathematics Institute. We are grateful to Laurent Lafforgue and Barry Mazur for their interest and the referee for many useful remarks. Comments by Pierre Deligne were of tremendous help.

2. Overview

In this section we outline our strategy of reconstruction, or rather recognition, of the function field K of an algebraic variety X over an algebraic closure k of a finite field from a certain quotient of its Galois group.

Let $\mathcal{G}^a_K$ be the pro-ℓ-quotient of the abelianization

$$\mathrm{G}_K/[\mathrm{G}_K, \mathrm{G}_K],$$

of the absolute Galois group $\mathrm{G}_K = \mathrm{Gal}(\bar{K}/K)$ of K, $\ell \neq \mathrm{char}(k)$. By Kummer theory, $\mathcal{G}^a_K$ determines the pro-ℓ-completion $\hat{K}^*$ of the multiplicative group K^*.

A Galois-theoretic characterization of the field K involves the recognition of the subgroup $K^*/k^* \subset \hat{K}^*$, and of the canonical projective structure, the projectivization of the *additive* group K, considered as a vector space over k. The necessary information is encoded in $\mathcal{G}^c_K$, the maximal pro-ℓ-quotient of

$$\mathrm{G}_K/[[\mathrm{G}_K, \mathrm{G}_K], \mathrm{G}_K].$$

Our main Galois-theoretic object is a pair $(\mathcal{G}^a_K, \Sigma_K)$, where the *fan* Σ_K is the set of all maximal (by inclusion) topologically noncyclic subgroups whose set-theoretic preimage in $\mathcal{G}^c_K$ is an abelian group.

Theorem 1 states that if for two function fields $K = k(X), L = l(Y)$, where X/k is an algebraic surface, Y/l an algebraic variety, k and l are algebraic closures of finite fields of characteristic $\neq \ell$, there is an isomorphism

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

then $k \simeq l$, Y is a surface and Ψ induces an isomorphism between perfect closures L^{perf} and K^{perf} of L and K respectively, and this isomorphism is unique up to natural transformations (Frobenius).

Thus the existence of an isomorphism between Galois data implies that L is isomorphic to a finite purely inseparable extension of K and vice versa. Note that the pair $(\mathcal{G}^a_K, \Sigma_K)$ has a conformal automorphism $\gamma \mapsto c\gamma$ with $c \in \mathbb{Z}^*_\ell$.

At the same time, the perfect field K^{perf} has Frobenius automorphisms Fr

$$\begin{array}{ccc} K^{perf} & \to & K^{perf} \\ x & \mapsto & x^{p^n}, \end{array}$$

for $n \in \mathbb{Z}$. Our main theorem implies the existence of a canonical isomorphism

$$\mathrm{Aut}((\mathcal{G}^a_K, \Sigma_K))/\mathbb{Z}_\ell^* \simeq \mathrm{Aut}(K^{perf})/\langle \mathrm{Fr} \rangle.$$

Define a subfan $\Sigma_K^{\mathrm{div}} \subset \Sigma_K$ as the set of those maximal liftable subgroups which have nontrivial intersection with at least one other subgroup in Σ_K. Note that $\Psi(\Sigma_K^{\mathrm{div}}) = \Sigma_L^{\mathrm{div}}$. There is a geometric reason to distinguish Σ_K^{div}. Let K be the function field of a surface X over k, D an irreducible divisor on X and $\nu = \nu_D$ the corresponding nonarchimedean divisorial valuation. Its abelian decomposition group $\mathcal{D}^a_\nu \subset \mathcal{G}^a_K$ is a (noncanonical) direct product of the inertia subgroup $\mathcal{I}^a_\nu \simeq \mathbb{Z}_\ell$ and the group $\mathcal{G}^a_{k(D)}$ of the field $k(D)$. Now a subgroup $\sigma \subset \mathcal{D}^a_\nu$ of $\mathbb{Z}_\ell$-rank 2 is liftable if and only if it contains $\mathcal{I}^a_\nu$. Thus Σ_K^{div} contains all liftable subgroups of $\mathbb{Z}_\ell$-rank 2 which are contained in groups $\mathcal{D}^a_\nu$.

The first important result says that Σ_K^{div} exactly coincides with the set of all liftable subgroups of $\mathbb{Z}_\ell$-rank 2 contained in the groups $\mathcal{D}^a_\nu$, for different $\nu = \nu_D$. This gives an purely group-theoretic description of the groups $\mathcal{D}^a_\nu$: the nontrivial intersection of two liftable groups σ, σ' is always $\mathcal{I}^a_\nu$, for some divisorial valuation $\nu = \nu_D$, and $\mathcal{D}^a_\nu$ "centralizes" $\mathcal{I}^a_\nu$, it consists of all those elements in $\mathcal{G}^a_K$ which commute with $\mathcal{I}^a_\nu$, after lifting to $\mathcal{G}^c_K$.

The proof is based on Kummer theory and the interpretation of $\mathcal{G}^a_K$ as a space of special (logarithmic) $\mathbb{Z}_\ell$-valued maps on the infinite-dimensional projective space $\mathbb{P}_k(K) = K^*/k^*$ over k. The description of liftable subgroups is then reduced to questions in finite-dimensional projective geometry. Complete proofs of these results for $K = \bar{\mathbb{F}}_q(X)$ are contained in Section 5. The case of arbitrary algebraically closed ground fields k is treated in [3],[2].

At this stage we characterized all pairs $\mathcal{D}^a_{\nu_D}, \mathcal{I}^a_{\nu_D}$ inside $\mathcal{G}^a_K$, or, vaguely speaking, we recovered "all curves" on all models X of K. Moreover, we know that Y is also a surface over some field l and that Ψ induces a canonical isomorphism between the set of all "curves" on all models X of K and the set of all "curves" on all models of L.

Next we recover the "points" on D, as inertia groups $\mathcal{I}^a_w \subset \mathcal{G}^a_{k(D)}$, using various subgroups $\mathcal{I}^a_{\nu_{D'}}$ as follows: the image of $\mathcal{I}^a_w$ under any homomorphism of $\mathcal{G}^a_K$ to a finite group, which is trivial on $I^a_{\nu_D}$, coincides with the image of some divisorial $\mathcal{I}^a_{\nu_{D'}}$, which depends on the homomorphism (see Section 10). Conversely, for any $\gamma \in \mathcal{D}^a_{\nu_D}/\mathcal{I}^a_{\nu_D} \setminus \mathcal{I}^a_w$, for some divisorial valuation on $k(D)$ (a point), there exists such a homomorphism with the property that the image of γ is not contained in the image of any inertia subgroup $\mathcal{I}^a_{\nu_{D'}}$.

Now we can recover the genus of D and distinguish the set of divisorial valuations of K which on some model of K are represented by curves of genus > 0. Note that these valuations have 1-dimensional centers on *every model* of K.

At this stage we conclude that Ψ induces a bijection between the sets of all curves on all models of K and L respectively. This bijection preserves the genus of the curves.

We switch our attention to the dual space $\hat{K}^*$ of $\mathcal{G}^a_K$ and the dual isomorphism $\Psi^* : \hat{L}^* \to \hat{K}^*$. Our goal is to show first that Ψ^* induces a natural isomorphism $\Psi^* : L^*/l^* \otimes \mathbb{Z}_\ell \to K^*/k^* \otimes \mathbb{Z}_\ell$.

Elements of $\hat{K}^*$ can be thought of as infinite products of elements $f_i^{\ell^i} \in K^*$, modulo natural identifications, and they can be represented by, in general, infinite sums of irreducible divisors on a projective model X of the field with $\mathbb{Z}_\ell$-adic coefficients which converge to 0 in the ℓ-adic topology. We introduce the subgroup $\mathcal{FS}(K) \subset \hat{K}^*$ consisting of elements whose support contains only finitely many nonrational divisors (characterized above). Given a model X of K we can also consider $\mathcal{FS}_X(K) \subset \hat{K}^*$ - the subgroup of elements with finite support on X. This subgroup does not depend on the choice of X and is very close to $K^*/k^* \otimes \mathbb{Z}_\ell$. We need to show that Ψ^* induces canonical isomorphisms:

– $\Psi^* : \mathcal{FS}(L) \to \mathcal{FS}(K)$ and
– $\Psi^* : \mathcal{FS}_Y(L) \to \mathcal{FS}_X(K)$, ($Y$ is a model of L and X a model of K).

We have $\mathcal{FS}(K) = \mathcal{FS}_X(K) = K^*/k^* \otimes \mathbb{Z}_\ell$, provided $\mathrm{Pic}^0(X) = 1$ and X contains only finite number of rational curves. In this case the claimed isomorphisms follow easily from the previous step.

In general, in order to distinguish $\mathcal{FS}_X(K)$ Galois-theoretically we use special properties of the element $f^s, f \in K^*/k^*, s \in \mathbb{Z}_\ell$. Namely, both f^s and $(f+a)/(f+b)^{s'}$, for $a, b \in k^*$, have the property that the restriction of

f^s is equal to 1 on any component of the divisor of $(f+a)/(f+b)^{s'}$ and vice versa. We can formalize this property using an ℓ-adic analog of a symbol $(f,g) \mod \ell^n \in \mathrm{K}_2(K)/\ell^n$. Note that $(f,g) = 0 \mod \ell^n$ for any $n \in \mathbb{N}$, if f, g belong to the same one-dimensional subfield of K. In particular, for any $f^s \in K \setminus k$ there is an element g which is not a power of f and such that $(f,g) = 0$ (we can take $g = f+1$). This imposes a strong condition on f since for a generic element in $\hat{K}^*$ the "commutator" of f consists of ℓ-adic powers of f only. We show that special elements of $K^*/(K^*)^\ell$ have the property that their arbitrary lifts into $\mathcal{FS}(K) \subset \hat{K}^*$ with big "commutator" are automatically contained in $\mathcal{FS}_X(K)$. These elements generate $K^*/(K^*)^\ell$ and have a simple geometric characterization, which allows to obtain the claimed isomorphisms.

The group $\mathcal{FS}_Y(L)$ ($\mathcal{FS}_X(K)$ respectively) is equal to $L^*/l^* \otimes \mathbb{Z}_\ell$ (resp., $K^*/k^* \otimes \mathbb{Z}_\ell$) modulo a subgroup $T_\ell(K) \in \hat{K}^*$ consisting of elements with trivial ℓ-adic divisors. The group $T_\ell(K)$ is dual to the connected component of the Picard group and since $\Psi^* : T_\ell(L) \to T_\ell(K)$ is a canonical isomorphism we obtain the desired isomorphism:

$$\Psi^* : L^*/l^* \otimes \mathbb{Z}_\ell \to K^*/k^* \otimes \mathbb{Z}_\ell.$$

The next step involves a normalization of Ψ^*. Inside $K^*/k^* \otimes \mathbb{Z}_\ell$ we cannot Galois-theoretically distinguish $\Psi^*(L^*/l^*) \otimes \mathbb{Z}_{(\ell)}$ from $c \cdot \Psi^*(L^*/l^*) \otimes \mathbb{Z}_{(\ell)}$, for $c \in \mathbb{Z}_\ell^*$. However, this conformal invariance is the only freedom there is. If we fix the values of $f \in L^*/l^* \otimes \mathbb{Z}_\ell$ on one (arbitrary) irreducible divisor on a model Y of L then the image of $L^*/l^* \otimes \mathbb{Z}_{(\ell)}$ is naturally identified inside $K^*/k^* \otimes \mathbb{Z}_\ell$. Thus, after multiplication by $c \in \mathbb{Z}_\ell^*$, we can assume that

$$c\Psi^* : L^*/l^* \otimes \mathbb{Z}_{(\ell)} \xrightarrow{\sim} K^*/k^* \otimes \mathbb{Z}_{(\ell)}.$$

Now we have K^*/k^* and $c\Psi^*(L^*/l^*)$ inside $K^*/k^* \otimes \mathbb{Z}_{(\ell)}$. We also know that subgroups generated by elements f, g with pairwise trivial symbol $(f,g) = 0$ correspond to one-dimensional subfields in K, respectively L. Most one-dimensional subfields in K are isomorphic to $k(x)$, for some x, and Galois data allow us to recognize these subfields. Hence if $k(x) \subset K$ then $k(x)^*/k^* \otimes \mathbb{Z}_{(\ell)} = c\Psi^*(l^*(t)/l^*) \otimes \mathbb{Z}_{(\ell)} \subset K^*/k^* \otimes \mathbb{Z}_{(\ell)}$, for some $t \in L$.

Next we show that the corresponding groups $k(x)^*/k^*$ and $c\Psi^*(l^*(x)/l^*)$ intersect in $k(x)^*/(k^*)^r = c\Psi^*(l^*(x)/(l^*)^s)$ for some rational r, s. This property implies that the intersection $c\Psi^*(L^*/l^*) \cap K^*/k^*$ is isomorphic (as a multiplicative group) to $K_1^*/k^* = c\Psi^*(L_1^*/l^*)$, where L/L_1 and K/K_1 are purely inseparable extensions.

Now we add the projective structure over k, l, respectively. The sets of lines $\{\mathbb{P}(k \oplus kx)\}$ and $\{\mathbb{P}(l \oplus lt)\}$ in K^*/k^* and L^*/l^*, over all x, t generating closed subfields $k(x) \subset K$ and $l(t) \subset L$, are the same. It turns out that the sets of these lines and their (multiplicative) translations are compatible with a unique projective structure on the (multiplicative) groups K_1^*/k^* and L_1^*/l^* - namely the one coming from the field structure. The multiplicative isomorphism $K_1^*/k^* \simeq c\Psi^*(L_1^*/l^*)$ extends therefore to a unique additive isomorphism and hence an isomorphism between fields $c\Psi^* : L_1 \to K_1$. This implies the canonical isomorphism $c\Psi^* : L^{perf} \to K^{perf}$ and finishes the proof of the main theorem.

3. Basic algebra and geometry of fields

NOTATIONS 3.1. — Throughout, k is an algebraic closure of the finite field $\mathbb{F}_p$. and $K = k(X)$ the function field of an algebraic variety X/k over k (its *model*). Its set of k-rational points is denoted by $X(k)$, the Picard group by $\mathrm{Pic}(X)$ and Néron-Severi group by $\mathrm{NS}(X)$.

In this paper we use the fact that two-dimensional function fields K have "nice" models: smooth projective surfaces X over k with $K = k(X)$, whose geometric properties play an important role in the recognition procedure. In this section we collect some technical results about function fields of curves and surfaces and their models.

LEMMA 3.2. — *Let C/k be a smooth curve and $Q \subset C(k)$ a finite set. Then there exists an $n_Q \in \mathbb{N}$ such that for every degree zero divisor D with support in Q the divisor $n_Q D$ is principal.*

Proof. — Finitely generated subgroups of torsion groups are finite. The group of degree zero divisors $\mathrm{Pic}^0(C)$ (over any finite field) is torsion and every subgroup of divisors with support in a finite set $Q \subset C(k)$ is finitely generated. □

LEMMA 3.3. — *Let $K/\mathfrak{K}$ be a purely inseparable extension. Then*

- $\mathfrak{K} \supset k$*;*
- $K/\mathfrak{K}$ *is a finite extension;*
- $\mathfrak{K} = k(X')$ *for some algebraic variety* X'.

DEFINITION 3.4. — *We write* $\overline{E}^K \subset K$ *for the normal closure of a subfield* $E \subset K$ *(elements in* K *which are algebraic over* E*). We say that* $x \in K \setminus k$ *is* generating *if* $\overline{k(x)}^K = k(x)$.

REMARK 3.5. — If $E \subset K$ is 1-dimensional then for all $x \in E \setminus k$ one has $\overline{k(x)}^K = \overline{E}^K$ (a finite extension of E).

LEMMA 3.6. — *For any subfield* $E \subset K$ *there is a sequence*

$$X \xrightarrow{\pi_E} C' \xrightarrow{\iota_E} C,$$

where

- π_E *is rational dominant with irreducible generic fiber;*
- ι_E *is quasi-finite and dominant;*
- $k(C') = \overline{E}^K$ *and* $k(C) = E$.

For generating $x \in K$ we write

$$\pi_x \, : \, X \to C$$

for the morphism from Lemma 3.6, with $k(C) = k(x)$. For $y \in K \setminus k(x)$ define $\deg_x(y)$ (the degree of y on the generic fiber of π_x) as the degree of the corresponding surjective map from the generic fiber of π_x under π_y.

LEMMA 3.7. — *Let* $K = k(X)$ *be the function field of a surface and* $x, y \in K \setminus k$ *be such that*

$$\deg_x(y) = \min_{f \in K \setminus \overline{k(x)}^K} (\deg_x(f))$$

and $\overline{k(y)}^K = k(y')$ *for some* $y' \in K^*$*. Then* y *is generating:* $k(y) = \overline{k(y)}^K$.

Proof. — If y is not generating then $y = z(y')$ for some $y' \in K$ and some function $z \in k(y')^*$ of degree ≥ 2. This implies that $\deg_x(y) \geq 2\deg_x(y')$, contradicting minimality. □

LEMMA 3.8. — *Let X be a model of K containing a rational curve R and $x \in K^*$ a function such that its restriction x_R to R is defined and such that $k(R) = k(x_R)$. Then x is generating: $\overline{k(x)}^K = k(x)$.*

Proof. — The restriction map extends to $\overline{k(x)}^K$ and hence is an isomorphism between $k(x_R)$ and $k(x) = \overline{k(x)}^K$. □

The next proposition characterizes multiplicative groups of fields $\mathfrak{K} \subset K$ such that $K/\mathfrak{K}$ is a purely inseparable extension. Notice that for a one-dimensional field $k(C)$ such subfields are always of the form $k(C)^{p^n}$, for some $n \in \mathbb{N}$. Thus for any one-dimensional subfield $E \subset K$ there is an $r(E) \in \mathbb{N}$ such that the intersection of $\mathfrak{K}^*$ with E^* consists exactly of $r(E)$-powers of the elements of E^*. Below we show that this property of intersection with subfields of the special form $k(x) = \overline{k(x)}^K$ already characterizes multiplicative groups of such $\mathfrak{K}$ among multiplicative subgroups of K^*.

DEFINITION 3.9. — *Let $\mathfrak{K}^* \subset K^*$ be a (multiplicative) subgroup such that for any subfield $E = k(x) = \overline{k(x)}^K \subset K$ there exists an $r = r(E)$ with the property that $\mathfrak{K}^* \cap E^* = (E^*)^r$ (r-powers of elements of E^*). For every $t \in E^* \setminus k^*$ we define $r(t) = r(E)$.*

REMARK 3.10. — Note that $r(t)$ is not defined for $t \in K^* \setminus k^*$ iff $\overline{k(t)}^K$ is the function field of a curve of genus ≥ 1.

DEFINITION 3.11. — *We will say that $y \in K^*$ is a* power *if there exist an $x \in K^*$ and an integer $n \geq 2$ such that $y = x^n$.*

PROPOSITION 3.12. — *Let $K = k(X)$ be the function field of a surface and $\mathfrak{K}^* \subset K^*$ a subset such that*

(1) *$\mathfrak{K}^*$ is a multiplicative subgroup of K^*;*
(2) *for every $E = k(x) = \overline{k(x)}^K \subset K$ there exists an $r = r(E) \in \mathbb{N}$ with*
$$\mathfrak{K}^* \cap E^* = (E^*)^r;$$
(3) *there exists a $y \in K \setminus k$ with $r(y) = 1$.*

Then $\mathfrak{K} := \mathfrak{K}^* \cup 0$ is a field, whose multiplicative group is $\mathfrak{K}^*$ and $K/\mathfrak{K}$ is a purely inseparable finite extension.

Proof. — Once we know that $\mathfrak{K}$ is a field we can conclude that every $x \in K^*$, or some power of x, is in $\mathfrak{K}^*$. Of course, it can only be a power of p so that $K/\mathfrak{K}$ is a purely inseparable extension, of finite degree (by Lemma 3.3).

By (3), $k \subset \mathfrak{K}$. To conclude that $\mathfrak{K}$ is a field, it suffices to show that for every $x \in \mathfrak{K}$ one has $x+1 \in \mathfrak{K}$ (and then use multiplicativity). For every $x \in \mathfrak{K} \setminus k$ with $r(x) = 1$ we have $\mathfrak{K}^* \cap k(x)^* = k(x)^*$ and

$$x + \kappa \in \mathfrak{K}^*, \text{ for all } \kappa \in k.$$

In particular, this holds for y.

Consider $x \in \mathfrak{K}^*$ with $r(x) > 1$ or not defined. We claim that for some $\kappa \in k$

$$z := \frac{x+y+\kappa}{y+\kappa-1} \in \mathfrak{K} \text{ and } r(z) = 1.$$

This implies that

$$z - 1 = (x+1)/(y+\kappa-1) \in \mathfrak{K}^* \text{ and } x+1 \in \mathfrak{K}^*,$$

(by multiplicativity). We can assume that $K/k(C)(y)$, where $k(C) = \overline{k(x)}^K$, is a finite separable extension. (Otherwise, we can let K be a minimal proper subfield in $\mathfrak{K}' \subset K$ containing $k(C)(y)$ and such that $K/\mathfrak{K}'$ is purely inseparable and use the intersection of $\mathfrak{K}$ with $\mathfrak{K}'$ instead of $\mathfrak{K}$.)

To prove the claim, choose a model X of K such that both maps

$$\begin{array}{rcl} \pi_x : X & \to & C, \ \ k(C) = \overline{k(x)}^K \\ \pi_y : X & \to & \mathbb{P}^1 = (y:1) \end{array}$$

are proper morphisms (as in Lemma 3.6). Since x and y are algebraically independent ($r(x) > 1$), only finitely many components of the fibers of π_x are contained in the fibers of π_y and there exists a $\kappa \in k$ such that both fibers

$$\pi_y^{-1}(-\kappa) \text{ and } \pi_y^{-1}(1-\kappa)$$

are transversal to the fibers of π_x, since we assume that $K/k(C)(y)$ is separable. Note that

$$\mathrm{div}_0(y+\kappa-1) \not\subset \mathrm{div}(x+y+\kappa),$$

since $y+\kappa = -1$ on $\mathrm{div}_0(y+\kappa-1)$ and x is nonconstant on these fibers (where div_0 is the divisor of zeroes). It follows in the first case that *both*

$$t := (y+\kappa)/x \ \text{ and } \ z := (x+y+\kappa)/(y+\kappa-1)$$

are not powers.

Note that t, z are generating elements. Indeed, if we blow up the smooth point q of transversal intersection $\{y + \kappa = 0\} \cap \{x = 0\}$ then t restricts nontrivially to $\mathbb{P}^1_q$ and similarly

$$z := (x + y + \kappa)/(y + \kappa - 1) = x + 1/(y + \kappa - 1) + 1$$

restricts nontrivially to $\mathbb{P}^1_{q'}$, where $q' = \{x = -1\} \cap \{y = 1 - \kappa\}$.

Note that $t \subset \mathfrak{K}^*$ and since it is not a power $r(t) = 1$ and

$$(1/t) + 1 = (x + y + \kappa)/(y + \kappa) \in \mathfrak{K}.$$

To show that $z \in \mathfrak{K}$ observe that both $x, y + \kappa \in \mathfrak{K}$ so that $t \in \mathfrak{K}$. Therefore,

$$t + 1 = (x + y + \kappa)/x \in \mathfrak{K}$$

and, by (1), $x + y + \kappa \in \mathfrak{K}$. Finally, since $(y + \kappa - 1) \in \mathfrak{K}$ we get $z \in \mathfrak{K}$. □

REMARK 3.13. — If assumption (3) is not satisfied then we can take

$$(\mathfrak{K}^*)^{1/r(y)} \bigcap K^*,$$

which satisfies all the conditions of the lemma. Thus in general without the assumption (3) we have $\mathfrak{K} = (\mathfrak{K}')^r$, where $K/\mathfrak{K}'$ is purely inseparable and $r \in \mathbb{N}$.

In our analysis of Galois groups we need to keep track of rational curves on a surface.

LEMMA 3.14. — *Let X be a surface over k. There three mutually disjoint possibilities:*

(1) $\mathrm{Pic}^0(X) = 0$*;*
(2) $\mathrm{Pic}^0(X) \neq 0$ *and X contains finitely many rational curves;*
(3) $\mathrm{Pic}^0(X) \neq 0$ *and, after a finite purely inseparable extension, X admits a fibration over a curve C of genus* $\mathrm{g}(C) \geq 1$ *with generic fiber a rational curve.*

Proof. — Follows from the classification of surfaces. Indeed, if X is smooth and $\mathrm{Pic}^0(X) \neq 0$ then there is a nontrivial map into the Albanese variety of X, and all rational curves lie in fibers. The generic fiber of this map is either rational or there are only finitely many rational curves on X. □

Let X be a surface over k and $\mathrm{Alb}(X)$ its Albanese variety. Recall that $\mathrm{Alb}(X)$ is a principal homogeneous space for an abelian variety $A^0(X)$, with $\dim A^0(X) = \dim \mathrm{Alb}(X)$.

LEMMA 3.15. — *Let $\mathcal{D} := \{D_j\}_{j\in J}$ be a finite set of irreducible divisors on X. Assume that there is an $f \in k(X)^*$ whose divisor is supported in $\mathcal{D}$. Let $B \subset A^0(X)$ be the smallest abelian subvariety such that the image of D_j under the map $\alpha : \mathrm{Alb}(X) \to A := \mathrm{Alb}(X)/B$ is a point, for all $j \in J$.*

Assume that $B \neq A^0(X)$. Then the image of X in A is a curve C and A is isomorphic to the Jacobian $\mathrm{Jac}(C)$ of degree 1 zero-cycles on C.

Proof. — First of all, $\dim \alpha(X) \geq 1$: the surface X is connected and $\alpha(X)$ generates A. Further, $\alpha(X)$ is not a surface: otherwise if $X' \to \alpha(X)$ is the normalization, then there is a map $\mu : X \to X'$ and the image of $\{D_j\}_{j\in J}$ is a finite set of points on X'. The intersection matrix of the set of irreducible components in the divisorial support of $\mu^{-1}(x')$, for any $x' \in X'$, is negative definite, contradicting the assumption that there is a function supported in $\mathcal{D}$.

Let $C := \alpha(X) \subset A$, we have $k(C) \subset K$. Let C' be a curve with function field $k(C') = \overline{k(C)}^K \subset K$. The map $C' \to C$ is finite. The map $\alpha : X \to A$ factors through the Jacobian $\mathrm{Jac}(C')$: we have

$$\begin{array}{ccc} X & \xrightarrow{\alpha_{C'}} & \mathrm{Jac}(C') \\ & & \downarrow \\ & & A \end{array}$$

The image of $\{D_j\}_{j\in J}$ under $\alpha_{C'}$ is a finite set of points in $\mathrm{Jac}(C')$. We have surjections $\mathrm{Jac}(C') \to \mathrm{Jac}(C) \to A$ and a canonical map $\mathrm{Alb}(X) \to \mathrm{Jac}(C')$. Then $B = \mathrm{Ker}(\alpha_{C'})$ and $C' = C$. □

4. Projective structures

In this section we explain the connection between fields and axiomatic projective geometry. We follow closely the exposition in [7].

DEFINITION 4.1. — *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*

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

For $s \in S$ and $S' \subset S$ define the *join*

$$s \vee S' := \{s'' \in S \mid s'' \in \mathfrak{l}(s, s') \text{ for some } s' \in S'\}.$$

For any finite set of points $s_1, \dots, s_n$ define

$$\langle s_1, \dots s_n \rangle := s_1 \vee \langle s_2 \vee \cdots \vee s_n \rangle$$

(this does not depend on the order of the points). Write $\langle S' \rangle$ for the join of a *finite* set $S' \subset S$. A finite set $S' \subset S$ of pairwise distinct points is called *independent* if for all $s' \in S'$ one has

$$s' \notin \langle S' \setminus \{s'\} \rangle.$$

A set of points $S' \subset S$ *spans* a set of points $T \subset S$ if

- $\langle S'' \rangle \subset T$ for every finite set $S'' \subset S'$;
- for every $t \in T$ there exists a finite set of points $S_t \subset S'$ such that $t \in \langle S_t \rangle$.

A set $T \subset S$ spanned by an independent set S' of points of cardinality ≥ 1 is called a projective *subspace* of dimension $|S'| - 1$.

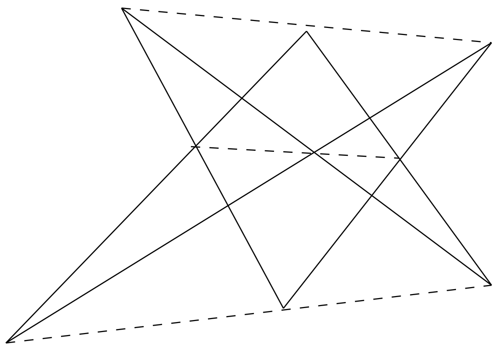
The axioms imply that projective subspaces of a given projective space S form a lattice and that the dimension function is well defined, i.e.,

$$\dim(T \cup T') + \dim(T \cap T') = \dim(T) + \dim(T')$$

for all pairs of projective subspaces $T, T' \subset S$. Here we put $\dim(\emptyset) := -1$.

DEFINITION 4.2. — *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.

The main theorem of abstract projective geometry is:

THEOREM 4.3. — *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 L and an isomorphism*

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

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

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

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

Proof. — See [7], Chapter 6. □

DEFINITION 4.4. — *A morphism of projective structures*

$$\rho : (S, \mathfrak{L}) \to (S', \mathfrak{L}')$$

is an injection of sets $\rho : S \hookrightarrow S'$ such that $\rho(\mathfrak{l}) \in \mathfrak{L}'$ for all $\mathfrak{l} \in \mathfrak{L}$.

EXAMPLE 4.5. — Let k be a field and $\mathbb{P}_k^n$ the usual projective space over k of dimension $n \geq 2$. Then $\mathbb{P}_k^n$ carries a projective structure: the set of lines is the set of usual projective lines $\mathbb{P}_k^1 \subset \mathbb{P}_k^n$.

Let K/k be an extension of fields (not necessarily finite). Then the set

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

carries a natural (possibly, infinite-dimensional) projective structure. Moreover, multiplication by elements in the group K^*/k^* preserves this structure.

THEOREM 4.6. — *Let K/L and K'/L' be field extensions of degree ≥ 3 and*

$$\bar{\phi} : S = \mathbb{P}_L(K) \to \mathbb{P}_{L'}(K') = S'$$

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

$$L \simeq L' \text{ and } K \simeq K'.$$

Proof. — Consider $V := K$ as a vector space over L. By Theorem 4.3, to S there are canonically attached the L-algebra $\mathrm{End}(V)$ and $\mathrm{GL}(V) \subset \mathrm{End}(V)$, as the set of elements preserving the collineations of the projective space S (because the action of homotheties on $\mathrm{End}(V)$ is trivial). This allows to recover the field K as the subfield of the L-algebra $\mathrm{End}(V)$ given by

$$\{0\} \cup \{x \in \mathrm{GL}(V) \subset \mathrm{End}(V) \,|\, x \text{ induces a group-translation on } S\}.$$

□

DEFINITION 4.7. — *Let K/k be the function field of an algebraic variety X of dimension ≥ 2 and $S = \mathbb{P}_k(K)$ the associated projective structure from Example 4.5. The lines passing through 1 and a generating element of K (see Definition 3.4) and their multiplicative translations by elements in K^*/k^* will be called* primary.

LEMMA 4.8. — *Let $K = k(X)$ be the function field of a surface. For every line $\mathfrak{l} = \mathfrak{l}(1, x)$ there exists a $\mathbb{P}^2 \subset \mathbb{P}_k(K)$ such that all other lines in this $\mathbb{P}^2$ are primary.*

Proof. — Choose a smooth model X of K and two points $q_1, q_2 \in X$ such that $x(q_1) = 0, x(q_2) = 1$. Blow up q_1, q_2 and let $\mathbb{P}^1_i$ be the corresponding exceptional curves. Let $y \in K^*$ be an element restricting to a generator of $k(\mathbb{P}^1_i)$. The restriction map extends to the normal closure $\overline{k(y)} \subset K$. Hence the normal closure $\overline{k(y)} \subset K$ coincides with $k(y)$.

To prove that every line $\mathfrak{l} \neq \mathfrak{l}(1, x) \subset \mathbb{P}^2 = \mathbb{P}_k(k \oplus kx \oplus ky)$ is primary we need to show that $(y + a + bx)/(y + c + dx)$ is generating, provided $(a, b) \neq (c, d)$. If $a \neq c$ then the restriction of $(y+a+bx)/(y+c+dx)$ to $\mathbb{P}^1_{q_1}$ is equal to $(y+a)/(y+c)$ and hence is a generator of $k(\mathbb{P}^1_{q_1})$. By the argument of the previous lemma, $(y+a+bx)/(y+c+dx)$ is generating. If $a = c, b \neq d$ then $(y + a + bx)/(y + c + dx)$ on $\mathbb{P}^1_{q_2}$ coincides with $(y + a + b)/(y + c + d)$ and is also generating since $a + b \neq c + d$, by assumption. □

LEMMA 4.9. — *Assume that a set S has two projective structures $(S, \mathfrak{L}_1)$ and $(S, \mathfrak{L}_2)$, both of dimension ≥ 2, and that for some $\mathbb{P}^2_1$ (in the first projective structure) every line $\mathfrak{l}_1 \in (\mathfrak{L}_1 \cap \mathbb{P}^2_1)$, except possibly one line, is also a line in the second structure. Then the* set *$\mathbb{P}^2_1$ is a projective plane in the second structure $(S, \mathfrak{L}_2)$, projectively isomorphic to $\mathbb{P}^2_1 \in (S, \mathfrak{L}_1)$.*

Proof. — Let $\hat{\mathbb{P}}^2_1$ be the set of all lines in $\mathbb{P}^2_1$ and $\hat{\mathbb{P}}^2_1 \setminus \mathfrak{l}$ the set of lines which remain projective lines in $\mathbb{P}^2_2$. Let $\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3$ be three lines from $\hat{\mathbb{P}}^2_1 \setminus \mathfrak{l}$ which don't have a common intersection point. Then $\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3$ lie in the same plane $\mathbb{P}^2_2$. Since every other line $\mathfrak{l}' \in \hat{\mathbb{P}}^2_1 \setminus \mathfrak{l}$ intersects $\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3$ then $\mathfrak{l}' \subset \mathbb{P}^2_2$. Thus all lines from $\hat{\mathbb{P}}^2_1 \setminus \mathfrak{l}$ are in $\mathbb{P}^2_2$ which contains all the points of $\mathbb{P}^2_1$.

They are isomorphic since it is an isomorphism between lines and every point, except possibly one point, is an intersection of two lines in $\hat{\mathbb{P}}^2_1 \setminus \mathfrak{l}$. Since $\hat{\mathbb{P}}^2_2$ coincides with $\hat{\mathbb{P}}^2_1$ outside of one point they coincide. □

COROLLARY 4.10. — *Let K/k and K'/k' be function fields of algebraic surfaces*

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

an isomorphism of (multiplicative) abelian groups inducing a bijection on the set of primary lines in the corresponding projective structures. Then $\bar{\phi}$ is an isomorphism of projective structures and

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

Proof. — By Lemma 4.8 and Lemma 4.9 $\bar{\phi}$ induces an isomorphism of projective structures. It remains to apply Theorem 4.6. □

5. Flag maps

NOTATIONS 5.1. — We fix two distinct prime numbers ℓ and p. Let

- $\mathbb{F} = \mathbb{F}_q$ be a finite field with $q = p^n$ and $\mathbb{F}^*$ its multiplicative group;
- $\mathrm{Vect}_{\mathbb{F}}$ - the set of finite-dimensional $\mathbb{F}$-vector spaces;
- A a vector space over $\mathbb{F}$ and $\mathbb{P}(A) = \mathbb{P}_{\mathbb{F}}(A) = (A \setminus 0)/\mathbb{F}^*$ its projectivization;
- $\mathcal{M}(A)$ the set of maps from $A \setminus \{0\}$ to $\mathbb{Z}_\ell$;
- for $\mu \in \mathcal{M}(A)$ and $B \subset A$ an $\mathbb{F}$-linear subspace, μ_B the restriction of μ to $B \setminus \{0\}$.

DEFINITION 5.2. — *A map $\mu \in \mathcal{M}(A)$ will be called $\mathbb{F}^*$-invariant if for all $a \in A \setminus \{0\}$ and all $\kappa \in \mathbb{F}^*$ one has*

$$\mu(\kappa \cdot a) = \mu(a).$$

DEFINITION 5.3. — *A map μ on $A \backslash \{0\}$, for a (possibly infinite-dimensional) vector space A, will be called an $\mathbb{F}$-flag map, if*

- *μ is $\mathbb{F}^*$-invariant;*
- *every finite-dimensional $\mathbb{F}$-vector space $B \subset A$ has a flag of $\mathbb{F}$-subspaces*

$$B = B_0 \supset B_1 \supset \ldots \supset B_d = 0$$

such that μ_B is constant on $B_n \setminus B_{n+1}$, for all $n = 0, \ldots, d-1$.

The value of μ on $B = B_0 \setminus B_1$ is called the generic *value of μ on B; we denote it by $\mu^{\mathrm{gen}}(B)$. The set of $\mathbb{F}$-flag maps will be denoted by $\Phi_{\mathbb{F}}(A)$.*

EXAMPLE 5.4. — Let $K = k(X)$ be a function field. We can consider it as a vector space over k or over any of the finite subfields $\mathbb{F} \subset k$. Let ν be a nonarchimedean valuation on K and $\chi : \Gamma_\nu \to \mathbb{Z}_\ell$ a homomorphism from the value group of ν (see Section 7). Then $\chi \circ \nu \in \Phi_k(K)$.

DEFINITION 5.5. — *Let A be an $\mathbb{F}$-algebra (without zero-divisors). A map $\mu \in \mathcal{M}(A)$ will be called logarithmic if*

$$\mu(a \cdot a') = \mu(a) + \mu(a'), \text{ for all } a, a' \in A \setminus 0.$$

The set of such maps will be denoted by $\mathcal{L}_{\mathbb{F}}(A)$.

Since $\mathbb{F}$ is torsion, a logarithmic map to $\mathbb{Z}_\ell$ is $\mathbb{F}^*$-invariant.

DEFINITION 5.6. — *Let A be an $\mathbb{F}$-vector space. Two maps $\mu, \mu' \in \mathcal{M}(A)$ will be called a c-pair (commuting pair) if for all two-dimensional $\mathbb{F}$-subspaces $B \subset A$ there exist constants $\lambda, \lambda', \lambda'' \in \mathbb{Z}_\ell$ (depending on B) with $(\lambda, \lambda') \neq (0,0)$ such that for all $b \in B \setminus 0$ one has*

$$\lambda \mu_B(b) + \lambda' \mu'_B(b) = \lambda''.$$

THEOREM 5.7. — *Let $\mathbb{F} \subset k$ be a finite field with $\#\mathbb{F} \geq 11$, and $\mu, \mu' \in \mathcal{L}_{\mathbb{F}}(K)$ nonproportional maps forming a c-pair. Then there exists a pair $(\lambda, \lambda') \in \mathbb{Z}_\ell^2 \setminus (0,0)$ such that $\lambda\mu + \lambda'\mu' \in \Phi_{\mathbb{F}}(K)$.*

Proof. — This is a special case of the main theorem of [3], where it is proved over general ground fields k. However, the case when $k = \bar{\mathbb{F}}_q$ is easier. Following the request of the referee, we now give a complete proof in this special case. The main steps in the proof are:

- characterization of flag maps by their restriction to 2-dimensional $\mathbb{F}$-linear subspaces, for $\#\mathbb{F} \geq 11$ (see Lemma 5.16);
- reduction to linear spaces over prime fields, resp. $\mathbb{F}_4$, see Lemma 5.18: if $\mu \notin \Phi_{\mathbb{F}'}(A)$, for a finite field $\mathbb{F}'$, and μ is $\mathbb{F}^*$-invariant with respect to a large finite extension $\mathbb{F}/\mathbb{F}'$ then there is a subgroup $C \simeq \mathbb{F}_p^2 \subset A$, (resp. $\mathbb{F}_4^2$), so that $\mu_C \notin \Phi_{\mathbb{F}_p}(C)$.
- reduction to dimension 3: if the rank two $\mathbb{Z}_\ell$-module $\sigma := \langle \mu, \mu' \rangle$ does not contain a flag map then there is a subgroup $B \simeq \mathbb{F}_p^3 \subset A$ (resp. $\mathbb{F}_4^3$), such that for any nontrivial $\mu'' \in \sigma$ there is a proper subspace $C = C_{\mu''} \subsetneq B$ where $\mu''_C \notin \Phi_{\mathbb{F}_p}(C)$ (this step uses the logarithmic property);
- geometry of collineations on $\mathbb{P}^2 = \mathbb{P}_{\mathbb{F}}(B)$ over prime fields $\mathbb{F} = \mathbb{F}_p$ (resp. $\mathbb{F}_4$): such subgroups B cannot exist. This shows the existence of the desired flag map on A.

□

LEMMA 5.8. — *If $A \in \mathrm{Vect}_{\mathbb{F}}$ and $\mu \in \Phi_{\mathbb{F}}(A)$ then there exists a canonical $\mathbb{F}$-flag $(A_n)_{n=0,\dots,d}$ such that*

$$\mu^{\mathrm{gen}}(A_n) \neq \mu^{\mathrm{gen}}(A_{n+1}),$$

for all $n = 0, \dots, d-1$.

Proof. — Put $A_0 = A$ and let A_{n+1} be the additive subgroup of A_n spanned by a with $\mu(a) \neq \mu^{\mathrm{gen}}(A_n)$. Since μ is $\mathbb{F}^*$-invariant, A_{n+1} is an $\mathbb{F}$-vector space. Indeed, for $a, a' \in A_{n+1}$ and $\kappa, \kappa' \in \mathbb{F}^*$ write

$$a = \sum_{i \in I} b_i, \quad a' = \sum_{j \in J} b'_j$$

with finite I, J. Since

$$\mu(b_i) \neq \mu^{\mathrm{gen}}(A_n), \quad \mu(b'_j) \neq \mu^{\mathrm{gen}}(A_n),$$

for all $i \in I, j \in J$, we have

$$\mu(\kappa b_i) = \mu(b_i) \neq \mu^{\mathrm{gen}}(A_n) \quad \text{and} \quad \mu(\kappa' b'_j) = \mu(b'_j) \neq \mu^{\mathrm{gen}}(A_n)$$

so that $\kappa a + \kappa' a' \in A_{n+1}$. □

REMARK 5.9. — Since a flag map μ is $\mathbb{F}^*$-invariant, it defines a unique map on $(A \setminus \{0\})/\mathbb{F}^* = \mathbb{P}_{\mathbb{F}}(A)$. Conversely, a map μ on $\mathbb{P}_{\mathbb{F}}(A)$ gives rise to an $\mathbb{F}^*$-invariant maps on $A \setminus \{0\}$. An $\mathbb{F}$-flag map on $A \in \mathrm{Vect}_{\mathbb{F}}$ defines a flag by projective subspaces on $\mathbb{P}_{\mathbb{F}}(A)$. We denote by *generic* elements of $\mathbb{P}_{\mathbb{F}}(A)$ the image of generic elements from A.

NOTATIONS 5.10. — We denote by $\hat{\mathbb{P}}(A) = \hat{\mathbb{P}}_{\mathbb{F}}(A)$ the set of codimension one projective $\mathbb{F}$-subspaces of $\mathbb{P}(A)$.

DEFINITION 5.11. — *Assume that $A \in \mathrm{Vect}_{\mathbb{F}}$, and for all codimension one $\mathbb{F}$-subspaces $B \subset A$ one has $\mu_B \in \Phi_{\mathbb{F}}(B)$. Define $\hat{\mu}$ by*

$$\begin{array}{ccl} \hat{\mathbb{P}}(A) & \to & \mathbb{Z}_\ell \\ B & \mapsto & \hat{\mu}(\mathbb{P}(B)) := \mu^{\mathrm{gen}}(B). \end{array}$$

LEMMA 5.12. — *If $A \in \mathrm{Vect}_{\mathbb{F}}$ and $\mu \in \Phi_{\mathbb{F}}(A)$ then either $\hat{\mu}$ is constant on $\hat{\mathbb{P}}(A)$ or it is constant on the complement to one point.*

Proof. — Consider the canonical flag $(A_n)_{n=0,\dots,d}$. If $\mathrm{codim}(A_1) \geq 2$ then for every $\mathbb{P}(B) \in \hat{\mathbb{P}}(A)$ one has $\mu^{\mathrm{gen}}(B) = \mu^{\mathrm{gen}}(A)$ and $\hat{\mu}$ is constant. Otherwise, $\mu^{\mathrm{gen}}(B) = \mu^{\mathrm{gen}}(A)$, on any $B \neq A_1$ (and differs at $\mathbb{P}(A_1) \in \hat{\mathbb{P}}(A)$). □

LEMMA 5.13. — *Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with $q \geq 11$ and $\mathbb{P}^m = \mathbb{P}^m_{\mathbb{F}}$, $m \geq 2$ a projective space over $\mathbb{F}$. For any four projective hyperplanes and any ten projective subspaces of codimension at least two (all defined over $\mathbb{F}$) there exists a line (over $\mathbb{F}$) not contained in any of the above hyperplanes and not intersecting any of the ten codimension two subspaces.*

Proof. — One has

$$\#\mathrm{Gr}(2, m)(\mathbb{F}) \leq \#\mathrm{Gr}(2, m+1)(\mathbb{F})/q^2.$$

The number of $\mathbb{F}$-lines intersecting a subspace of codimension two in $\mathbb{P}^m_{\mathbb{F}}$ is bounded by $\#\mathrm{Gr}(2, m+1)(\mathbb{F})/q^2$. Our claim holds for $q \geq 11$. □

LEMMA 5.14. — *Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with $q \geq 11$, $A \in \mathrm{Vect}_{\mathbb{F}}$ and $\mu \in \mathcal{M}(A)$ an $\mathbb{F}^*$-invariant map. Assume that there exist $\mathbb{F}$-subspaces $B_i \subset A$, $\mathrm{codim}(B_i) = 1$, for $i = 1, \dots, 4$ such that*

(1) *either* $\#\{\mu^{\rm gen}(B_i)\} \geq 3$ *or*
(2) $\mu^{\rm gen}(B_1) = \mu^{\rm gen}(B_2) \neq \mu^{\rm gen}(B_3) = \mu^{\rm gen}(B_4)$.

Then there exists an $\mathbb{F}$*-subspace* $C \subset A$, $\dim_{\mathbb{F}}(C) = 2$ *such that* $\mu_C \notin \Phi_{\mathbb{F}}(C)$.

Proof. — By Lemma 5.13, there exists a $\mathbb{P}^1 = \mathbb{P}(C) \in \mathbb{P}(A)$ such that its intersection points with $\mathbb{P}(B_i)$ are pairwise distinct and generic in the corresponding $\mathbb{P}(B_i)$ (the nongeneric points of $\mathbb{P}(B_i)$ are contained in 4 subspaces in $\mathrm{codim}_{\mathbb{F}} \geq 2$, the intersections of B_i give rise to 6 more subspaces). Then either μ takes at least three distinct values on $\mathbb{P}(C)$ or has distinct values in at least two pairs of points. In both cases $\mu \notin \Phi_{\mathbb{F}}(C)$. □

COROLLARY 5.15. — *Assume that* $\mu_B \in \Phi_{\mathbb{F}}(B)$ *for all* $\mathbb{P}(B) \in \hat{\mathbb{P}}(A)$ *(and* $\#\mathbb{F} \geq 11$*). Then* $\hat{\mu}$ *is constant outside of one point.*

Proof. — The map $\hat{\mu}$ takes two different values on $\hat{\mathbb{P}}(B)$. By Lemma 5.14, among any three hyperplanes two have the same generic value, so that there can be at most three such values. If there are hyperplanes $h_1, h_2, h_3 \in \hat{\mathbb{P}}(A)$, where $\hat{\mu}(h_1) = \hat{\mu}(h_2) \neq \hat{\mu}(h_3)$ then for any other $h \in \hat{\mathbb{P}}(A)$ we have $\hat{\mu}(h) = \hat{\mu}(h_1)$ and $\hat{\mu}$ is constant outside of h_3. □

LEMMA 5.16. — *Let* $A \in \mathrm{Vect}_{\mathbb{F}}$*, with* $\#\mathbb{F} \geq 11$*, and* $\mu \in \mathcal{M}(A)$ *be an* $\mathbb{F}^*$*-invariant map such that for every two-dimensional* $\mathbb{F}$*-subspace* $B \subset A$, $\mu_B \in \Phi_{\mathbb{F}}(B)$*. Then* $\mu \in \Phi_{\mathbb{F}}(A)$.

Proof. — Assume the statement holds if $\dim(A) \leq n-1$. Then $\hat{\mu}$ is defined and, by Corollary 5.15, either $\hat{\mu}$ is constant on $\hat{\mathbb{P}}(A)$ or constant on the complement to one point.

If $\hat{\mu}$ is constant, then the $\mathbb{F}$-linear envelope of points $b \in A$ such that $\mu(b) \neq \hat{\mu}$ has codimension at least two. Indeed, if there is a codimension one subspace $B \subset A$ generated by such b then by assumption $\mu \in \Phi_{\mathbb{F}}(B)$ and $\mu^{\rm gen}(B) \neq \hat{\mu}$, contradicting the assumption that $\hat{\mu}$ is constant. Otherwise, put $B := A_1$. By induction, $\mu \in \Phi_{\mathbb{F}}(B)$ and is constant on $A \setminus B$. Hence $\mu \in \Phi_{\mathbb{F}}(A)$.

Assume that $\hat{\mu}$ is nonconstant and let $B \subset A$ be the unique codimension one subspace with differing $\mu^{\rm gen}(B)$. Choose an $\mathbb{F}$-basis $b_1, \ldots, b_{n-1}$ in B such that $\mu(b_i) = \mu^{\rm gen}(B)$. Assume that there is a point $a \in A \setminus B$ such that $\mu(a) \neq$ the generic value of $\hat{\mu}$ and let B' be the codimension one $\mathbb{F}$-subspace spanned $b_1, \ldots, b_{n-2}, a$. Then $\mu^{\rm gen}(B') \neq$ the generic value of $\hat{\mu}$, contradicting the uniqueness of B. It follows that μ is constant on $A \setminus B$. □

REMARK 5.17. — Let $\mathbb{F}/\mathbb{F}'$ be a finite extension, $A \in \mathrm{Vect}_{\mathbb{F}}$, considered as an $\mathbb{F}'$-vector space, and $\mu \in \Phi_{\mathbb{F}'}(A)$. If μ is $\mathbb{F}^*$-invariant, then $\mu \in \Phi_{\mathbb{F}}(A)$. Indeed, by the proof of Lemma 5.8, the canonical $\mathbb{F}'$-flag is a flag of $\mathbb{F}$-vector spaces. We use this observation to reduce our problem to prime fields (resp. $\mathbb{F}_4$).

LEMMA 5.18. — *Let $\mathbb{F}/\mathbb{F}'$ be a quadratic extension, with $\#\mathbb{F}' > 2$. Let A be an $\mathbb{F}$-vector space of dimension 2, considered as an $\mathbb{F}'$-vector space of dimension 4. Let $\mu \in \mathcal{M}(A)$ be an $\mathbb{F}^*$-invariant map such that for every $\mathbb{F}'$-subspace $C \subset A$, $\dim_{\mathbb{F}'}(C) = 2$, one has $\mu_C \in \Phi_{\mathbb{F}'}(C)$. Then $\mu \in \Phi_{\mathbb{F}}(A)$.*

Proof. — First assume that μ takes only two values on $A \setminus \{0\}$, say $0, 1$, and that $\mu \notin \Phi_{\mathbb{F}}(A)$. Since $\mathbb{P}_{\mathbb{F}}(A) = \mathbb{P}^1_{\mathbb{F}}$ there exist elements $a_1, a_2, a_3, a_4 \in A \setminus \{0\}$ such that the orbits $\mathbb{F}^* \cdot a_i$ do not intersect and

$$0 = \mu(a_1) = \mu(a_2) \neq \mu(a_3) = \mu(a_4) = 1.$$

Then $\mathbb{F}^* \cdot a_i = \Lambda_i \setminus \{0\}$, where Λ_i is a linear subspace over $\mathbb{F}'$. The $\mathbb{F}'$-span Λ_{12} of two nonzero vectors $x_1 \in \Lambda_1, x_2, \in \Lambda_2$ has $\mu^{\mathrm{gen}}(\Lambda_{12}) = 0$. Hence Λ_{12} contains at most one $\mathbb{F}'$-subspace $\langle b \rangle$ of $\mathbb{F}'$-dimension 1 with generic value 1. The union of the spaces Λ_{12}, for different choices of x_1, x_2, covers A and

$$\#\{b \in \mathbb{P}_{\mathbb{F}'}(A) \,|\, \mu(b) = 1\} \leq (q+1)^2,$$

where $\#\mathbb{F}' = q$. Similarly, there are at most $(q+1)^2$ such nongeneric $c \in \mathbb{P}_{\mathbb{F}'}(A)$ with $\mu(c) = 0$. Since $\#\mathbb{P}^3(\mathbb{F}') = q^3 + q^2 + q + 1 > 2(q^2 + 2q + 1)$, for $q > 2$, we get a contradiction.

Assume now that μ takes at least 3 distinct values on $A \setminus \{0\}$, say $0, 1, 2$, and that there are two vectors $a_1, a_2 \subset A$ such that the orbits $\mathbb{F}^* \cdot a_1, \mathbb{F}^* \cdot a_2$ don't intersect and $0 = \mu(a_1) = \mu(a_2)$. Such a configuration must exist (take two $\mathbb{F}'$-spaces of $\mathbb{F}'$-dimension two spanned by $\mathbb{F}^*$-orbits; the $\mathbb{F}'$ span of two generic vectors in these spaces contains elements whose μ-value coincides with the value of μ on one of the two orbits). The modified map, given by

$$\tilde{\mu}(a) := \begin{cases} 0 & \text{if } \mu(a) = 0 \\ 1 & \text{otherwise} \end{cases},$$

satisfies the conditions of the Lemma, and by the above argument $\tilde{\mu} \in \Phi_{\mathbb{F}}(A)$. In particular, $\tilde{\mu} = 0$ outside one $\mathbb{F}^*$-orbit on $A \setminus \{0\}$. Since μ is $\mathbb{F}^*$-invariant it follows that μ takes two values, and not three as we assumed. Contradiction. □

LEMMA 5.19. — *Let $\mathbb{F}' = \mathbb{F}_p$ (resp. $\mathbb{F}_4$), and $\mathbb{F}/\mathbb{F}'$ be an extension of degree divisible by 4. Consider $K = k(X)$ as an $\mathbb{F}$-vector space and let $\mu, \mu' \in \mathcal{L}_{\mathbb{F}}(K)$ be a c-pair such that the linear span $\sigma = \langle \mu, \mu', 1\rangle_{\mathbb{Z}_\ell}$ does not contain an $\Phi_{\mathbb{F}}$-map. Then there exist an $\mathbb{F}'$-subspace $B \subset K$ with $\dim_{\mathbb{F}'}(B) = 3$, two distinct $\mathbb{F}'$-subspaces $C, C' \subset B$ of dimension 2 and maps $\tilde{\mu}, \tilde{\mu}' \in \sigma$ such that*

- *$\tilde{\mu}_C \notin \Phi_{\mathbb{F}'}(C)$ and $\tilde{\mu}_{C'}$ is constant;*
- *$\tilde{\mu}'_{C'} \notin \Phi_{\mathbb{F}'}(C')$ and $\tilde{\mu}'_C$ is constant;*

In particular, for every (nonzero) map $\mu'' \in \sigma$ there exists an $\mathbb{F}'$-subspace $C'' \subset B$, $\dim_{\mathbb{F}'} C'' = 2$ with the property that $\mu''_{C''} \notin \Phi_{\mathbb{F}'}(C'')$.

Proof. — We consider K as an $\mathbb{F}$-vector space as well as an $\mathbb{F}'$-vector space. Let μ be an $\mathbb{F}^*$-invariant map on K. If μ were an $\mathbb{F}'$-flag map on every two-dimensional $\mathbb{F}'$-subspace of K then, by Lemma 5.18, μ would be an $\mathbb{F}$-flag map on every $\mathbb{F}$-subspace $B \subset K$ of $\dim_{\mathbb{F}} B = 2$. Since $\#\mathbb{F} \geq 11$ we could apply Lemma 5.16 and conclude that $\mu \in \Phi_{\mathbb{F}}(K)$.

Thus, since $\mu \notin \Phi_{\mathbb{F}}(K)$, there is an $\mathbb{F}'$-subspace $C \subset K$, $\dim_{\mathbb{F}'}(C) = 2$ such that $\mu_C \notin \Phi_{\mathbb{F}'}(C)$. If μ'_C is constant, put $\tilde{\mu}' := \mu$. Otherwise, using the c-pair property on C we find constants d_C, d'_C, d''_C, with $d'_C \neq 0$, such that

$$d_C\mu + d'_C\mu'_C = d''_C \ \text{ and put } \tilde{\mu}' = \mu' - \frac{d''_C - d_C\mu}{d'_C}.$$

Then $\tilde{\mu}'_C = 0$. Since the linear combination $\tilde{\mu}'$ is not a flag map, there exists a C', $\dim_{\mathbb{F}'}(C') = 2$, where $\tilde{\mu}' \notin \Phi_{\mathbb{F}'}(C')$. If $\mu_{C'}$ is constant, put $\tilde{\mu} := \mu$. Otherwise, using the c-pair property on C' we find constants $d_{C'}, d'_{C'}, d''_{C'}$, with $d'_{C'} \neq 0$, such that

$$d_{C'}\mu + d'_{C'}\mu'_{C'} = d''_{C'} \ \text{ and put } \tilde{\mu} = \mu - \frac{d''_{C'} - d'_{C'}\tilde{\mu}'}{d_{C'}}.$$

Then $\tilde{\mu}_{C'} = 0$ and $\tilde{\mu}_C \notin \Phi_{\mathbb{F}'}(C)$ (since $\tilde{\mu}'_C$ is constant). Now put

$$B := C + \frac{c}{c'} \cdot C',$$

for some nonzero $c \in C$ and $c' \in C'$. Then $\dim_{\mathbb{F}'}(B) = 3$, the maps $\tilde{\mu}_B, \tilde{\mu}'_B$ are linearly independent, and they satisfy the required conditions. For $s \neq 0$, we have $s\tilde{\mu} + s'\tilde{\mu}' \notin \Phi_{\mathbb{F}'}(C)$. Otherwise, $s\tilde{\mu} + s'\tilde{\mu}' \notin \Phi_{\mathbb{F}'}(\frac{c}{c'} \cdot C')$. Note that the logarithmic property of the maps is used to reduce to dimension 3. □

A detailed analysis of c-pairs on projective planes as above shows that such planes cannot exist. This will complete the proof of the main theorem.

LEMMA 5.20 (Lemma 4.3.2 in [3]). — *Let $V \subset \mathbb{Z}_\ell^2$ be such that for any two pairs of distinct points the affine line through one pair and the affine line through the other have a common point and that this point of intersection is contained in V. Then V is contained in a line union one point.*

Proof. — Otherwise, V contains four points in general position. Embed $\mathbb{Z}_\ell^2$ into $\mathbb{P}^2(\mathbb{Q}_\ell)$, choose coordinates for these four points

$$(1:0:0), (0:1:0), (0:0:1) \text{ and } (1:1:1)$$

and close V for the operation

$$x, y, z, t \mapsto \mathfrak{l}(x,y) \cap \mathfrak{l}(z,t), \quad \text{when} \quad x \neq y, z \neq t, \mathfrak{l}(x,y) \neq \mathfrak{l}(z,t).$$

The closure $\bar{V}$ of V satisfies the axioms of a projective plane (see Definition 4.1). For example, to verify that any “line” in $\bar{V}$ contains at least three points it suffices to pick one of the four initial points not on this line and to draw lines through this point and the remaining three points in the initial set.

By the fundamental theorem of projective geometry, $\bar{V} = \mathbb{P}^2(\mathbb{Q})$. On the other hand, $\mathbb{P}^2(\mathbb{Q})$ is dense in $\mathbb{P}^2(\mathbb{Q}_\ell)$. In particular, it cannot be contained in $\mathbb{Z}_\ell^2$. Contradiction. □

COROLLARY 5.21. — *Let $B = \mathbb{F}^3$ and $\mu, \mu' \in \mathcal{M}(B)$ be a c-pair of $\mathbb{F}^*$-invariant maps. Then the image of $\mathbb{P}(B)$ under the map*

$$\begin{array}{cccc} \varphi & : & \mathbb{P}(B) & \to & \mathbb{A}^2(\mathbb{Z}_\ell) \\ & & b & \mapsto & (\mu(b), \mu'(b)) \end{array}$$

is contained in a union of an affine line and (possibly) one more point.

Proof. — The c-pair condition for μ, μ' implies that the image of every $\mathbb{P}^1 \subset \mathbb{P}(B)$ is contained in an affine line in $\mathbb{Z}_\ell^2$. Next, for any two pairs of distinct points $(a,b), (a',b')$ in $\varphi(\mathbb{P}(B))$ the affine lines $\mathfrak{l} = \mathfrak{l}(a,b), \mathfrak{l}' = \mathfrak{l}'(a',b')$ in $\mathbb{A}^2 = \mathbb{Z}_\ell^2$ through these pairs of points must intersect. (Choose $\tilde{a}, \tilde{b}, \tilde{a}', \tilde{b}'$ in the preimages of a, b, a', b'; the projective lines $\tilde{\mathfrak{l}}, \tilde{\mathfrak{l}}' \subset \mathbb{P}(B) = \mathbb{P}^2$ through these points intersect in some x and, by the first observation, $\varphi(x)$ must lie on both $\mathfrak{l}$ and $\mathfrak{l}'$). Now it suffices to apply Lemma 5.20. □

ASSUMPTION 5.22. — *We may now assume that*

- $\mathbb{F} = \mathbb{F}_p$ *or* $\mathbb{F}_4$;
- $\mu, \mu' \in \mathcal{L}_{\mathbb{F}}(A)$ *is a* c*-pair of linearly independent maps as in Lemma 5.19,*
- B *is as in Lemma 5.19: for every two-dimensional* $C'' \subset B$ *there exists a* $\mu'' \in \langle \mu, \mu' \rangle$ *such that* $\mu''_{C''} \notin \Phi_{\mathbb{F}}(C'')$.

We can exclude the following degenerate cases, which contradict our assumption that no linear combination of μ, μ' *is a flag map on* B*:*

(1) $\varphi(\mathbb{P}(B))$ *is contained in a line; this means that* μ, μ' *are linearly dependent (modulo constants);*
(2) $\varphi(\mathfrak{l})$ *is a point, for some* $\mathfrak{l} \subset \mathbb{P}(B)$*; this implies that* $\varphi(\mathfrak{l}) \in \varphi(\mathfrak{l}')$*, for all* $\mathfrak{l}' \subset \mathbb{P}(B)$ *and* $\varphi(\mathbb{P}(B))$ *is contained in a line, contradiction to (1);*
(3) φ *is constant outside one line; here the affine map* $\mathbb{Z}_\ell^2 \to \mathbb{Z}_\ell$ *projecting* $\varphi(\mathfrak{l})$ *to one point gives a nontrivial flag map in the span of* μ, μ'.

LEMMA 5.23. — *Let* $\mathfrak{l}, \mathfrak{l}' \subset \mathbb{P}^2$ *be distinct lines. Let* $x \in \mathbb{P}^2$ *be a point such that* $\varphi(x) \notin (\varphi(\mathfrak{l}) \cup \varphi(\mathfrak{l}'))$*. Then there is a natural projective isomorphism* $\pi_{x,\mathfrak{l}'} : \mathfrak{l} \to \mathfrak{l}'$ *respecting the level sets of* φ*. Namely, for every pair* $y_1, y_2 \in \mathfrak{l}$ *with* $\varphi(y_1) = \varphi(y_2)$ *one has*

$$\varphi(\pi_{x,\mathfrak{l}'}(y_1)) = \varphi(\pi_{x,\mathfrak{l}'}(y_2))$$

(and vice versa). In particular, if $\varphi(\mathfrak{l}) \subset \varphi(\mathfrak{l}')$ *then* $\varphi(\mathfrak{l}) = \varphi(\mathfrak{l}')$.

Proof. — The images $\varphi(\mathfrak{l}(x, y_1))$ and $\varphi(\mathfrak{l}(x, y_2))$ span the same affine line L_x. We have $\varphi(\mathfrak{l}') \not\subset L_x$. Define $\pi_{x,\mathfrak{l}'}(y_i) := \mathfrak{l}(x, y_i) \cap \mathfrak{l}'$. By Corollary 5.21, $\varphi(\pi_{x,\mathfrak{l}'}(y_i))$ are contained in the intersection of $\varphi(\mathfrak{l}')$ and L_x, so that $\varphi(\pi_{x,\mathfrak{l}'}(y_1)) = \varphi(\pi_{x,\mathfrak{l}'}(y_2))$. □

COROLLARY 5.24. — *If there exist a line* $\mathfrak{l} \subset \mathbb{P}^2$ *and a point* $x \in \mathfrak{l}$ *such that* φ *is constant on* $\mathfrak{l} \setminus x$ *then there is a nontrivial flag map in the span of* μ, μ'.

Proof. — By Assumption 5.22, φ is nonconstant on every line. Assume that there exists a point $a \in \varphi(\mathbb{P}^2)$ such that $\varphi^{-1}(a)$ consists exactly of x. Then for all $\mathfrak{l}', \mathfrak{l}''$ not containing x one has $\varphi(\mathfrak{l}') = \varphi(\mathfrak{l}'')$ and φ is constant on the complement to x on every line through x. Then a linear combination of μ, μ' is constant on $\mathbb{P}^2 \setminus x$, thus a flag map, contradicting the assumption.

Let x' be a point in $\mathbb{P}^2 \setminus \mathfrak{l}$ with $\varphi(x') = \varphi(x)$. The lines $\mathfrak{l}$ and $\mathfrak{l}(x, x')$ are not equivalent, $\varphi(\mathfrak{l}) \neq \varphi(\mathfrak{l}')$. For any line $\mathfrak{l}'' \neq \mathfrak{l}(x, x')$ through x' we have

$\varphi(\mathfrak{l} \cap \mathfrak{l}'') \neq \varphi(x)$. Using a point on $y \in \mathfrak{l}'$ with $\varphi(y) \neq \varphi(x)$ and applying Lemma 5.23 we find that $\varphi(\mathfrak{l}'') = \varphi(\mathfrak{l})$. For any $y \notin (\mathfrak{l} \cup \mathfrak{l}')$ consider the line $\mathfrak{l}(x', y)$. It follows that $\varphi(y)$ equals the value of φ on $\mathfrak{l} \setminus x$, thus φ is constant on the complement to $\mathfrak{l}'$, contradicting Assumption 5.22(3). □

COROLLARY 5.25. — *Let $x, y \in \mathbb{P}^2_{\mathbb{F}}$ be distinct points so that $\varphi(x), \varphi(y) \notin (\varphi(\mathfrak{l}) \cup \varphi(\mathfrak{l}'))$ and the line $\mathfrak{l}(x, y)$ through x, y passes through the intersection $q_0 := \mathfrak{l} \cap \mathfrak{l}'$. Then the composition*

$$\pi_{x,\mathfrak{l}} \circ \pi_{y,\mathfrak{l}}^{-1} \,:\, \mathfrak{l} \to \mathfrak{l}$$

induces a nontrivial translation on $\mathfrak{l}$, with fixed point q_0, preserving the level sets of φ. (By symmetry we have a similar translation on $\mathfrak{l}'$.)

In particular, if $\mathbb{F} = \mathbb{F}_p$ (the prime field) then the group generated by this translation is transitive on $\mathfrak{l} \setminus (\mathfrak{l} \cap \mathfrak{l}')$ and φ is constant on this complement. If $\mathbb{F} = \mathbb{F}_4$ then the complement $\mathfrak{l} \setminus (\mathfrak{l} \cap \mathfrak{l}')$ is a union of two (two point) orbits of this translation and φ is constant on each orbit.

Proof of Theorem 5.7. — We keep the Assumptions 5.22.

For every point $x \in \mathbb{P}^2$ and every line $\mathfrak{l}$ through x there exist lines $\mathfrak{l}', \mathfrak{l}''$ through x such that $\varphi(\mathfrak{l}) = \varphi(\mathfrak{l}')$ and $\varphi(\mathfrak{l}') \neq \varphi(\mathfrak{l}'')$. Indeed, consider a line $\tilde{\mathfrak{l}}$ with $\varphi(x) \notin \varphi(\tilde{\mathfrak{l}})$. If on all such lines φ takes more than two values, then all these lines are equivalent and φ is constant on the complement to x on every line through x, contradiction to Corollary 5.24. Otherwise, each value on $\tilde{\mathfrak{l}}$ will be taken at least twice, hence the claim.

Corollary 5.25 gives a translation on $\mathfrak{l} \setminus x$ preserving the level sets of φ. Over the prime field $\mathbb{F}_p$, $p > 2$, φ restricted to $\mathfrak{l}$ is constant on the complement to x and we can apply Corollary 5.24.

Over $\mathbb{F}_4$, φ is either constant on $\mathfrak{l} \setminus x$, contradicting Corollary 5.24, or the level sets of φ on $\mathfrak{l} \setminus x$ fall into two orbits of cardinality two. Since we can pick x on $\mathfrak{l}$ arbitrarily, φ must be constant on $\mathfrak{l}$, contradicting Assumption 5.22(2). □

6. Galois groups

Let k be an algebraic closure of a finite field of characteristic $\neq \ell$, K the function field of an algebraic variety X over k, $\mathcal{G}^a_K$ the abelianization of the pro-ℓ-quotient $\mathcal{G}_K$ of the Galois group G_K of a separable closure of K,

$$\mathcal{G}_K^c = \mathcal{G}_K/[[\mathcal{G}_K, \mathcal{G}_K], \mathcal{G}_K] \xrightarrow{\mathrm{pr}} \mathcal{G}_K^a$$

its canonical central extension and pr the natural projection.

DEFINITION 6.1. — *We say that $\gamma, \gamma' \in \mathcal{G}_K^a$ form a* commuting pair *if for some (and therefore any) of their preimages $\tilde{\gamma}, \tilde{\gamma}'$ in $\mathcal{G}_K^c$ one has $[\tilde{\gamma}, \tilde{\gamma}'] = 0$. A subgroup $\mathcal{H}$ of $\mathcal{G}^a$ is called* liftable *if any two elements in $\mathcal{H}$ form a commuting pair.*

DEFINITION 6.2. — *The* fan $\Sigma_K = \{\sigma\}$ *on $\mathcal{G}_K^a$ is the set of all topologically noncyclic liftable subgroups $\sigma \subset \mathcal{G}_K^a$ which are not properly contained in any other liftable subgroup of $\mathcal{G}_K^a$.*

REMARK 6.3. — For function fields K/k of surfaces all groups $\sigma \in \Sigma_K$ are isomorphic to torsion-free primitive $\mathbb{Z}_\ell$-submodules σ of rank 2, see Section 9.

NOTATIONS 6.4. — Let

$$\boldsymbol{\mu}_{\ell^n} := \{ \sqrt[\ell^n]{1} \}$$

and

$$\mathbb{Z}_\ell(1) = \lim_{n\to\infty} \boldsymbol{\mu}_{\ell^n}.$$

We often identify $\mathbb{Z}_\ell$ and $\mathbb{Z}_\ell(1)$ (since k is algebraically closed). Write

$$\hat{K}^* := \lim_{n\to\infty} K^*/(K^*)^{\ell^n}$$

for the multiplicative group of (formal) rational functions on X.

THEOREM 6.5 (Kummer theory). — *The group K^*/k^* is a free $\mathbb{Z}$-module. One has*

- *$K^*/(K^*)^{\ell^n} = (K^*/k^*)/\ell^n$, for all $n \in \mathbb{N}$;*
- *the discrete group $K^*/(K^*)^{\ell^n}$ and the compact profinite group $\mathcal{G}_K^a/\ell^n$ are Pontryagin dual to each other, for a $\boldsymbol{\mu}_{\ell^n}$-duality;*
- *for $K^*/k^* \xrightarrow{\sim} \mathbb{Z}^I$, one has $K^*/(K^*)^{\ell^n} \xrightarrow{\sim} (\mathbb{Z}/\ell^n)^I$ and*

$$\mathcal{G}_K^a/\ell^n \xrightarrow{\sim} (\mathbb{Z}/\ell^n(1))^I,$$

hence the duality between $\hat{K}^* = \widehat{K^*/k^*}$ and $\mathcal{G}_K^a$ is modeled on that between

$$\{ \textit{functions } I \to \mathbb{Z}_\ell \textit{ tending to } 0 \textit{ at } \infty\} \textit{ and } \mathbb{Z}_\ell^I.$$

LEMMA 6.6. — *Let E/k be the function field of a curve. Then $\Sigma_E = \emptyset$.*

Proof. — By a result of Grothendieck, the pro-ℓ fundamental group $(\pi_1)\hat{}_\ell$ of a curve punctured in finitely many points is free. We have

$$\mathcal{G}_E^a = \lim_{\substack{\longleftarrow \\ J\subset I}} \mathbb{Z}_\ell^J, \quad \mathcal{G}_E^c = \lim_{\substack{\longleftarrow \\ J\subset I}} \wedge^2(\mathbb{Z}_\ell^J),$$

with the commutation map equal to $\wedge$. This implies that a liftable subgroup of $\mathcal{G}_E^a$ is topologically cyclic. □

7. Valuations

In this section we recall basic results concerning valuations and valued fields (we follow [4]). Most of this material is an adaptation of well-known facts to our context.

NOTATIONS 7.1. — A *value group,* denoted by Γ, is a totally ordered (torsion-free) abelian group. We use the additive notation $''+''$ for the group law and $\geq$ for the order. We have

$$\Gamma = \Gamma^+ \cup \Gamma^-, \;\; \Gamma^+ \cap \Gamma^- = \{0\} \;\text{ and }\; \gamma \geq \gamma' \;\text{ iff }\; \gamma - \gamma' \in \Gamma^+.$$

Then $\Gamma_\infty = \Gamma \cup \{\infty\}$ is a totally ordered monoid, by the conventions

$$\gamma < \infty, \;\; \gamma + \infty = \infty + \infty = \infty, \;\; \forall \gamma \in \Gamma.$$

DEFINITION 7.2. — *A (nonarchimedean)* valuation *on a field K is a pair $\nu = (\nu, \Gamma_\nu)$ consisting of a value group Γ_ν and a map*

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

such that

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

REMARK 7.3. — In particular, since Γ_ν is nontorsion, $\nu(\zeta) = 0$ for every element ζ of finite order in K^*.

A valuation is called *trivial* if $\Gamma = \{0\}$. If $K = k(X)$ is a function field over an algebraic closure k of a finite field then every valuation of K restricts to a trivial valuation on k (every element in k^* is torsion).

LEMMA 7.4. — *Let* $K = k(X)$ *and* ν *be a nonarchimedean valuation on* $k(X)$. *Then* $\mathrm{Hom}(\Gamma_\nu, \mathbb{Z}_\ell)$ *is a finitely generated* $\mathbb{Z}_\ell$*-module.*

Proof. — Note that the $\mathbb{Q}$-rank of ν is bounded by $\dim(X)$ (see [11]). □

NOTATIONS 7.5. — We denote by K_ν, $\mathfrak{o}_\nu, \mathfrak{m}_\nu$ and $\boldsymbol{K}_\nu$ 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

$$\boldsymbol{K}_\nu := \mathfrak{o}_\nu / \mathfrak{m}_\nu.$$

If X (over k) is a model for K then the *center* $\mathfrak{c}(\nu)$ of a valuation is the irreducible subvariety defined by the prime ideal $\mathfrak{m}_\nu \cap k[X]$ (provided ν is nonnegative on $k[X]$).

It is useful to keep in mind the following exact sequences:

$$1 \to \mathfrak{o}_\nu^* \to K^* \to \Gamma_\nu \to 1 \tag{7.1}$$

and

$$1 \to (1 + \mathfrak{m}_\nu) \to \mathfrak{o}_\nu^* \to \boldsymbol{K}_\nu^* \to 1. \tag{7.2}$$

NOTATIONS 7.6. — Write $\mathcal{I}_\nu^a \subset \mathcal{D}_\nu^a \subset \mathcal{G}_K^a$ for the images of the inertia and the decomposition group of the valuation ν in $\mathcal{G}_K^a$.

NOTATIONS 7.7. — If $\chi : \Gamma_\nu \to \mathbb{Z}_\ell(1)$ is a homomorphism then

$$\chi \circ \nu \; : \; K^* \to \mathbb{Z}_\ell(1)$$

defines an element of $\mathcal{G}_K^a$, called an inertia element of the valuation ν. The group of such elements is $\mathcal{I}_\nu^a \subset \mathcal{G}_K^a$.

NOTATIONS 7.8. — The decomposition group $\mathcal{D}_\nu^a$ is by definition equal to the image of $\mathcal{G}_{K_\nu}^a$ in $\mathcal{G}_K^a$.

LEMMA 7.9. — *There is a natural embedding* $\mathcal{G}_{K_\nu}^a \hookrightarrow \mathcal{G}_K^a$ *and a (canonical) isomorphism*

$$\mathcal{D}_\nu^a / \mathcal{I}_\nu^a \simeq \mathcal{G}_{\boldsymbol{K}_\nu}^a.$$

Proof. — See Theorem 19.6 in [6], for example. □

DEFINITION 7.10. — *Let* $K = k(X)$ *be a function field. Its valuation* ν *is*

- positive-dimensional *if* $\mathrm{tr}\deg_k \boldsymbol{K}_\nu \geq 1$*;*
- divisorial *if* $\mathrm{tr}\deg_k \boldsymbol{K}_\nu = \dim(X) - 1$.

NOTATIONS 7.11. — We let $\mathcal{V}_K$ be the set of all nontrivial (nonarchimedean) valuations of K and $\mathcal{DV}_K$ the subset of divisorial valuations. If $\nu \in \mathcal{DV}_K$ is realized by a divisor D on a model X of K (see Example 7.13) we sometimes write $\mathcal{I}^a_D$, resp. $\mathcal{D}^a_D$, for the corresponding inertia, resp. decomposition group.

EXAMPLE 7.12. — Let $E = k(C)$ be the function field of a smooth curve. Every point $q \in C(k)$ defines a nontrivial valuation ν_q on E (the order of a function $f \in E^*$ at q). Conversely, every nontrivial valuation ν on E defines a point $q := \mathfrak{c}(\nu)$ on C.

EXAMPLE 7.13. — Let $K = k(X)$ be the function field of a surface.

- Every positive-dimensional valuation is divisorial.
- Every (irreducible) curve $D \subset X$ defines a valuation ν_D on K with value group $\mathbb{Z}$. Conversely, every valuation on K with value group $\mathbb{Z}$ and algebraically nonclosed residue field defines a curve D on some model X of K.
- Every flag (D, q), (curve, point on its normalization), defines a valuation $\nu_{D,q}$ on K with value group $\mathbb{Z}^2$.
- There exist valuations on K with value group $\mathbb{Q}$ and center supported in a point (on every model).

LEMMA 7.14. — *Let $K = k(X)$ be the function field of a surface. If $\mathcal{D}^a_\nu/\mathcal{I}^a_\nu$ is nontrivial then ν is divisorial.*

Proof. — The only 1-dimensional valuations on function fields of surfaces are divisorial valuations. For other valuations, the residue field $\boldsymbol{K}_\nu = k$ is algebraically closed and $\mathcal{G}^a_{\boldsymbol{K}_\nu}$ trivial. □

8. A dictionary

Write

$$\begin{array}{rclcl} \mathcal{L}_K & := & \mathcal{L}_k(K) & = & \{\,\text{homomorphisms } K^* \to \mathbb{Z}_\ell(1)\} \\ \Phi_K & := & \Phi_k(K) & = & \{\,\text{flag maps } K \to \mathbb{Z}_\ell(1)\} \end{array}$$

PROPOSITION 8.1. — *One has the following identifications:*

$$\begin{array}{rcl} \mathcal{G}^a_K & = & \mathcal{L}_K, \\ \mathcal{D}^a_\nu & = & \{\mu \in \mathcal{L}_K \,|\, \mu \text{ trivial on } (1+\mathfrak{m}_\nu)\}, \\ \mathcal{I}^a_\nu & = & \{\mu \in \mathcal{L}_K \,|\, \mu \text{ trivial on } \mathfrak{o}^*_\nu\}. \end{array}$$

If two nonproportional $\mu, \mu' \in \mathcal{G}_K^a$ form a commuting pair then the corresponding maps $\mu, \mu' \in \mathcal{L}_K$ form a c-pair (in the sense of Definition 5.6).

Proof. — The first identification is a consequence of Kummer theory 6.5. The second identification can be checked on one-dimensional subfields of K, where it is evident. For this and the third identification we use (7.1) and (7.2). For the last statement, assume that $\mu, \mu' \in \mathcal{L}_K$ don't form a c-pair. Then there is an $x \in K$ such that the restrictions of $\mu, \mu' \in \mathcal{L}_K$ to the subgroup $\langle 1, x\rangle$ are linearly independent. Therefore, $\mu, \mu' \in \mathcal{G}_K^a$ define a rank 2 liftable subgroup in $\mathcal{G}_{k(x)}^a$. Such subgroups don't exist since $\mathcal{G}_{k(x)}$ is a free pro-ℓ-group (see [10]). $\square$

EXAMPLE 8.2. — If $\mu \in \mathcal{D}_\nu^a$ and $\alpha \in \mathcal{I}_\nu^a$ then μ, α form a commuting pair.

PROPOSITION 8.3. — *Let K be a field and $\alpha \in \Phi_K \cap \mathcal{L}_K$. Then there exists a unique valuation $\nu = (\nu_\alpha, \Gamma_{\nu_\alpha})$ (up to equivalence) and a homomorphism $\mathrm{pr} : \Gamma_{\nu_\alpha} \to \mathbb{Z}_\ell(1)$ such that*

$$\alpha(f) = \mathrm{pr}(\nu_\alpha(f))$$

for all $f \in K^*$. In particular, $\alpha \in \mathcal{I}_\nu^a$ (under the identification of Proposition 8.1).

Proof. — Let $\mathbb{F}$ be a finite subfield of k and assume that $\alpha(f) \neq \alpha(f')$ for some $f, f' \in K$ and consider the line $\mathbb{P}^1 = \mathbb{P}(\mathbb{F}f + \mathbb{F}f')$. Since α is a flag map, it is constant outside one point on this $\mathbb{P}^1$ so that either $\alpha(f+f') = \alpha(f)$ or $= \alpha(f')$. This defines a relation: $f' >_\alpha f$ (in the first case) and $f >_\alpha f'$ (otherwise). If $\alpha(f) = \alpha(f')$ and there exists an f'' such that $\alpha(f) \neq \alpha(f'')$ and $f >_\alpha f'' >_\alpha f'$ then we put $f >_\alpha f'$. Otherwise, we put $f =_\alpha f'$.

It was proved in [3], Section 2.4, that the above definitions are correct and that $>_\alpha$ is indeed an order which defines a filtration on the additive group K by subgroups $(K_\gamma)_{\gamma\in\Gamma}$ such that

- $K = \cup_{\gamma\in\Gamma} K_\gamma$ and
- $\cap_{\gamma\in\Gamma} K_\gamma = \emptyset$,

where Γ is the set of equivalence classes with respect to $=_\alpha$. Since $\alpha \in \mathcal{L}_K$ this order is compatible with multiplication in K^*, so that the map $K \to \Gamma$ is a valuation and α factors as $K^* \to \Gamma \to \mathbb{Z}_\ell \simeq \mathbb{Z}_\ell(1)$. By (7.1), $\alpha \in \mathcal{I}_\nu^a$. $\square$

COROLLARY 8.4. — *Every (topologically) noncyclic liftable subgroup of $\mathcal{G}_K^a$ contains an inertia element of some valuation.*

Proof. — By Theorem 5.7, every such liftable subgroup contains an Φ-map, which by Proposition 8.3 belongs to some inertia group. □

9. Flag maps and valuations

In this section we give a Galois-theoretic description of inertia and decomposition subgroups of divisorial valuations.

LEMMA 9.1. — *Let $\alpha \in \Phi_K \cap \mathcal{L}_K$, $\nu = \nu_\alpha$ be the associated valuation and $\mu \in \mathcal{L}_K$. Assume that α, μ form a c-pair. Then*

$$\mu(1 + \mathfrak{m}_\nu) = \mu(1) = 0.$$

In particular, the restriction of μ to $\mathfrak{o}_\nu$ is induced from $\boldsymbol{K}_\nu$.

Proof. — First of all, $\mu(1) = 0$, since μ is logarithmic. We have

(1) $\alpha(\kappa) = 0$ for all $\kappa \in \mathfrak{o}_\nu \setminus \mathfrak{m}_\nu$;
(2) $\alpha(\kappa + m) = \alpha(\kappa)$ for all $\kappa \in \mathfrak{o}_\nu \setminus \mathfrak{m}_\nu$ and $m \in \mathfrak{m}_\nu$ as above;
(3) $\mathfrak{m}_\nu$ is additively generated by $m \in \mathfrak{o}_\nu$ such that $\alpha(m) \neq 0$.

If $m \in \mathfrak{m}_\nu$ is such that $\alpha(m) \neq 0$ and $\kappa \in \mathfrak{o}_\nu \setminus \mathfrak{m}_\nu$ then α is nonconstant on the subgroup $A := \langle \kappa, m \rangle$. Then

$$\mu(\kappa + m) = \mu(\kappa).$$

Indeed, if μ is nonconstant on A the restriction μ_A is proportional to α_A (by the c-pair property) and α satisfies (2). In particular, for such m we have $\mu(1 + m) = \mu(1) = 0$.

Assume that $\alpha(m) = 0$. Then there exists an $m' \in \mathfrak{m}_\nu$ such that $m > m' > 1$ and $\alpha(m') \neq \alpha(1) = 0$. Using the first step with $\kappa = 1$ and observing that $\alpha(m+m') \neq 0$ we have $\mu(1+m+m') = \mu(1) = 0$. On the other hand, putting $\kappa = 1 + m$ and using that $\alpha(m') \neq 0$ we see that $\mu(1 + m + m') = \mu(1 + m)$. Thus $0 = \mu(1) = \mu(1 + m)$ as claimed. □

COROLLARY 9.2. — *Inertia elements $\alpha \in \mathcal{I}^a_\nu$ commute only with elements $\mu \in \mathcal{D}^a_\nu$.*

PROPOSITION 9.3. — *Let $K = k(X)$ be the function field of a surface. Every $\sigma \in \Sigma_K$ has $\mathrm{rk}_{\mathbb{Z}_\ell}\, \sigma = 2$. Moreover, it defines a unique valuation $\nu = \nu_\sigma$ of K so that either every element of σ is inertial for ν, or ν is divisorial and there is an element $\mu \in \sigma$ which is not inertial for ν, but $\mu \in \mathcal{D}^a_\nu$.*

If distinct $\sigma, \sigma' \in \Sigma_K$ have a nonzero intersection then there exists a divisorial valuation ν'' such that

- $\sigma, \sigma' \in \mathcal{D}^a_{\nu''}$;
- $\sigma \cap \sigma' = \mathcal{I}^a_{\nu''}$.

Conversely, if $\sigma \in \Sigma_K$ is not contained in a $\mathcal{D}^a_{\nu''}$ for any divisorial valuation ν'' then for all $\sigma' \in \Sigma_K$, $\sigma' \neq \sigma$, one has $\sigma \cap \sigma' = 0$.

Proof. — We saw that $\sigma \in \Sigma_K$ contains an inertia element α for *some* valuation ν. Since σ is topologically noncyclic there is a $\mu \in \sigma$, $\mathbb{Z}_\ell$-independent on α, and commuting with α. If μ is not inertial, that is, $\mu \notin \Phi_K$, then μ gives a nontrivial element in the (abelianized) Galois group of the residue field $\boldsymbol{K}_\nu$ of ν. Thus ν is divisorial, $\boldsymbol{K}_\nu$ is 1-dimensional and every liftable subgroup in $\mathcal{G}^a_{\boldsymbol{K}_\nu}$ has $\mathbb{Z}_\ell$-rank equal to one. Hence $\mathrm{rk}_{\mathbb{Z}_\ell} \sigma = 2$ in this case and, by Corollary 9.2, $\mu \in \mathcal{D}^a_\nu$. Such a valuation ν is unique, since $\mathcal{I}^a_\nu \cap \mathcal{I}^a_{\nu'} = 0$ for distinct divisorial ν, ν'.

If σ contains *only* inertia elements, then there exists a unique valuation ν such that $\sigma \in \mathcal{I}^a_\nu$. Indeed, either $\mathfrak{m}_\nu + \mathfrak{m}_{\nu'} = K$ or we may assume that $\mathfrak{m}_\nu \subset \mathfrak{m}_{\nu'}$ (and $\mathfrak{o}_\nu \supset \mathfrak{o}_{\nu'}$). The first case is impossible since the corresponding inertia groups don't intersect. In the second case, $\mathcal{I}^a_\nu \subset \mathcal{I}^a_{\nu'}$, as claimed. Moreover, it follows that $\mathrm{rk}_{\mathbb{Z}_\ell} \sigma = 2$, since the $\mathbb{Q}$-rank of any valuation on a surface (over $\bar{\mathbb{F}}_q$) is at most two. This gives of $\nu = \nu_\sigma$ in this case.

If distinct σ, σ' have a nontrivial intersection, then the subgroup $\mathcal{D} \subset \mathcal{G}^a_K$ generated by σ, σ' is not the inertia group of any valuation (the rank of those is ≤ 2, as we have seen above). If the $\sigma \cap \sigma'$ contains a nontrivial inertia element α then $\mathcal{D}$ is contained in the decomposition group of this element (all elements of $\mathcal{D}$ commute with α) and the corresponding valuation is divisorial. If $\mu \in \sigma \cap \sigma'$ is not an inertia element then there exist inertia elements $\alpha \in \sigma$ and $\alpha' \in \sigma'$ corresponding to distinct *divisorial* valuations ν, ν'. The decomposition groups of distinct divisorial valuations don't intersect. □

Proposition 9.3 allows us to identify intrinsically (in terms of the Galois group) inertia subgroups of divisorial valuations as well as their decomposition groups as follows. Every pair of distinct groups $\sigma, \sigma' \in \Sigma_K$ with a nontrivial intersection defines a divisorial valuation ν, whose inertia group

$$\mathcal{I}^a_\nu = \sigma \cap \sigma'.$$

The corresponding decomposition subgroup is

$$\mathcal{D}^a_\nu = \cup_{\sigma \supset \mathcal{I}^a_\nu} \sigma.$$

10. Galois groups of curves

Here we give a Galois-theoretic characterization of subgroups $\sigma \in \Sigma_K$ which are inertia subgroups of rank two valuations of K arising from a flag (C, q), where C is a smooth irreducible curve (on some model of K) and $q \in C(k)$ is a point (see Example 7.13). We show that Galois-theoretic data determine the genus of C and all "points" on C, as special liftable subgroups of rank two inside $\mathcal{G}^a_{k(C)}$.

Throughout, $E = k(C)$ is the function field of a smooth curve of genus g. We have an exact sequence

$$0 \to E^*/k^* \to \mathrm{Div}(C) \to \mathrm{Pic}(C) \to 0$$

(where $\mathrm{Div}(C)$ can be identified with the free abelian group generated by points in $C(k)$). This gives a dual sequence

$$0 \to \mathbb{Z}_\ell \xrightarrow{\Delta} \mathcal{M}(C(k), \mathbb{Z}_\ell) \to \mathcal{G}^a_E \to \mathbb{Z}_\ell^{2\mathrm{g}} \to 0, \tag{10.1}$$

with the identifications

- $\mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}_\ell) = \Delta(\mathbb{Z}_\ell)$ (since $\mathrm{Pic}^0(C)$ is torsion);
- $\mathcal{M}(C(k), \mathbb{Z}_\ell) = \mathrm{Hom}(\mathrm{Div}(C), \mathbb{Z}_\ell)$ is the $\mathbb{Z}_\ell$-linear space of maps from $C(k) \to \mathbb{Z}_\ell$;
- $\mathbb{Z}_\ell^{2\mathrm{g}} = \mathrm{Ext}^1(\mathrm{Pic}^0(C), \mathbb{Z}_\ell)$.

Using this model and the results in Section 6, in particular the identification

$$\mathcal{G}^a_E = \mathrm{Hom}(E^*/k^*, \mathbb{Z}_\ell),$$

we can interpret

$$\mathcal{G}^a_E \subset \mathcal{M}(C(k), \mathbb{Q}_\ell)/\text{constant maps} \tag{10.2}$$

as the $\mathbb{Z}_\ell$-linear subspace of all maps $\mu : C(k) \to \mathbb{Q}_\ell$ (modulo constant maps) such that

$$[\mu, f] \in \mathbb{Z}_\ell \quad \text{for all} \quad f \in E^*/k^*.$$

Here $[\cdot,\cdot]$ is the pairing:

$$
\begin{array}{rcl}
\mathcal{M}(C(k),\mathbb{Q}_\ell)\times E^*/k^* & \to & \mathbb{Q}_\ell \\
(\mu,f) & \mapsto & [\mu,f]:=\sum_q \mu(q)f_q,
\end{array}
\tag{10.3}
$$

where $\mathrm{div}(f)=\sum_q f_q q$.

In detail, let $\gamma\in\mathcal{G}^a_E$ be an element of the Galois group. By Kummer theory, γ is a homomorphism $K^*/k^*\to\mathbb{Z}_\ell(1)\simeq\mathbb{Z}_\ell$. Choose a point $c_0\in C(k)$. For every point $c\in C(k)$, there is an $m_c\in\mathbb{N}$ such that the divisor $m_c(c-c_0)$ is principal (see Lemma 3.2). Define a map

$$
\begin{array}{rccc}
\mu_\gamma: & C(k) & \to & \mathbb{Q}_\ell, \\
& c & \mapsto & \gamma(m_c(c-c_0))/m_c.
\end{array}
$$

Changing c_0 we get maps differing by a constant map.

In this interpretation, an element of an inertia subgroup $\mathcal{I}^a_w\subset\mathcal{G}^a_E$ corresponds to a "delta"-map (constant outside the point q_w). Each $\mathcal{I}^a_w$ has a canonical (topological) generator δ_w, given by $\delta_w(f)=\nu_w(f)$, for all $f\in E^*/k^*$. The (diagonal) map $\Delta\in\mathcal{M}(C(k),\mathbb{Q}_\ell)$ from (10.1) is then given by

$$
\Delta=\sum_{w\in\mathcal{V}_E}\delta_w=\sum_{q_w\in C(k)}\delta_{q_w}.
$$

DEFINITION 10.1. — *We say that the support of a subgroup $\mathcal{I}\subset\mathcal{G}^a_E$ is $\le s$ and write*

$$
|\mathrm{supp}(\mathcal{I})|\le s
$$

if there exist valuations $w_1,\dots,w_s\in\mathcal{V}_E$ such that

$$
\mathcal{I}\subset\langle\mathcal{I}^a_{w_1},\dots,\mathcal{I}^a_{w_s}\rangle_{\mathbb{Z}_\ell}\subset\mathcal{G}^a_E.
$$

Otherwise, we write $|\mathrm{supp}(\mathcal{I})|>s$.

LEMMA 10.2. — *Let $E=k(x)$ and let $\mathcal{I}\subset\mathcal{G}^a_E$ be a topologically cyclic subgroup which is not equal to $\mathcal{I}^a_w$ for some divisorial valuation (point) on E ($\mathbb{P}^1(k)$). Then for any nonzero $\iota\in\mathcal{I}$ there exist a finite group V and a homomorphism $\psi:\mathcal{G}^a_E\to V$ such that for all $w\in\mathcal{V}_E$ one has $\psi(\iota)\notin\psi(\mathcal{I}^a_w)$.*

Proof. — By the assumption on $\mathcal{I}$, the element $\iota\in\mathcal{I}$ corresponds to a $\mathbb{Z}_\ell$-map μ_ι on $\mathbb{P}^1(k)$ which is not a delta-map of a point (modulo addition of constants). If μ_ι takes at least three distinct values there are three distinct $q_1,q_2,q_3\in\mathbb{P}^1(k)$ and $n\in\mathbb{N}$ so that the values $\mu_\iota(q_i)\mod\ell^n$ are pairwise distinct for $i=1,2,3$. Consider a map $\psi:\mathcal{G}^a_E\to(\mathbb{Z}/\ell^n)^2$ defined by elements of $E = k(x)$ with divisors $(q_1 - q_2), (q_1 - q_3)$. Note that $\psi(\mathcal{I}^a_w) = 0,\ q_w \in \mathbb{P}^1(k)$ unless $q_w = q_1, q_2, q_3$ and $\psi(\iota) \notin \psi(\mathcal{I}^a_{w_i}), i = 1, 2, 3$, as claimed.

Similarly, if μ_ι takes two values on $\mathbb{P}^1(k)$ there are points $q_i, i = 1, \dots, 4$ and $n \in \mathbb{N}$ so that

$$\mu_\iota(q_1) = \mu_\iota(q_2) \neq \mu_\iota(q_3) = \mu_\iota(q_4) \mod \ell^n.$$

Then $\psi : \mathcal{G}^a_E \to (\mathbb{Z}/\ell^n)^3$, given by elements of E with divisors

$$(q_1 - q_2), (q_1 - q_3), (q_3 - q_4),$$

satisfies the claim. □

The next step is an *intrinsic* definition of inertia subgroups

$$\mathcal{I}^a_w \subset \mathcal{D}^a_\nu / \mathcal{I}^a_\nu = \mathcal{G}^a_{k(C)}.$$

We have a projection

$$\pi_\nu : \mathcal{G}^a_K \to \mathcal{G}^a_K / \mathcal{I}^a_\nu$$

and an inclusion

$$\mathcal{G}^a_{\boldsymbol{K}_\nu} = \mathcal{D}^a_\nu / \mathcal{I}^a_\nu \hookrightarrow \mathcal{G}^a_K / \mathcal{I}^a_\nu$$

PROPOSITION 10.3. — *Let ν be a divisorial valuation of K. A topologically cyclic subgroup*

$$\mathcal{I} \subset \mathcal{D}^a_\nu / \mathcal{I}^a_\nu$$

is the inertia subgroup of a divisorial valuation of $k(C) = \boldsymbol{K}_\nu$ iff for every homomorphism

$$\psi : \mathcal{G}^a_K / \mathcal{I}^a_\nu \to V$$

onto a finite abelian group V there exists a divisorial valuation ν_ψ such that

$$\psi(\mathcal{I}) = \psi \circ \pi_\nu(\mathcal{I}^a_{\nu_\psi}).$$

Proof. — Let C be the smooth model for $\boldsymbol{K}_\nu = k(C)$,

$$\mathcal{I} = \mathcal{I}^a_w \subset \mathcal{D}^a_\nu / \mathcal{I}^a_\nu$$

the inertia subgroup of a divisorial valuation of $k(C)$ corresponding to a point $q = q_w \in C(k)$ and

$$\psi : \mathcal{G}^a_K / \mathcal{I}^a_\nu \to V$$

a homomorphism onto a finite abelian group. Since $\mathcal{G}^a_K$ is a pro-ℓ-group, we may assume that

$$V = \oplus_{j \in J} \mathbb{Z}/\ell^{n_j},$$

for some $n_j \in \mathbb{N}$. Let $n = \max_j(n_j)$. By Kummer theory,

$$\mathrm{Hom}(\mathcal{G}_K^a, \mathbb{Z}/\ell^n) = K^*/(K^*)^{\ell^n}$$

so that ψ determines elements

$$\bar{f}_j \in K^*/(K^*)^{\ell^n}$$

(for all $j \in J$). Choose functions f_j projecting to $\bar{f}_j$. They define a finite set of divisors D_{ij} on X, the irreducible components of the divisors of f_j. Moreover, f_j are not simultaneously constant on C (otherwise, $\psi(\mathcal{G}^a_{k(C)}) = \psi(\mathcal{I}^a_{k(C)})$). Changing the model $\tilde{X} \to X$, if necessary, we can ensure that the full preimage of a finite set of divisors becomes a divisor with normal crossings. In particular, we may assume that

- C is smooth (and irreducible);
- there exists exactly one irreducible component D in the full preimage of $\cup D_{ij}$ which intersects C in q. Moreover, this intersection is transversal.

Then the image of $\mathcal{I}^a_D$ under ψ is equal to the image of $\mathcal{I}^a_w$.

Conversely, we need to show that if $\mathcal{I} \neq \mathcal{I}^a_w$ (for some $w \in \mathcal{DV}_{\boldsymbol{K}_\nu}$), then there exists a homomorphism

$$\psi : \mathcal{G}^a_K/\mathcal{I}^a_\nu \to V$$

onto a finite abelian group V such that for all $\nu' \in \mathcal{DV}_K$ one has

$$\psi(\mathcal{I}) \neq \psi \circ \pi_\nu(\mathcal{I}^a_{\nu'}).$$

Let $\bar{\iota} \in \mathcal{I}$ be any nonzero element. Its lift ι to $\mathcal{G}^a_K$ is not a flag map on K^*. By Lemma 5.16 there exists a $\mathbb{P}^1_\iota = \mathbb{P}^1(k) \subset \mathbb{P}_k(K)$ such that the restriction of ι to $\mathbb{P}^1_\iota$ is is not a flag map. By the logarithmic property of ι we can assume that $\mathbb{P}^1_\iota$ is the projectivization of the k-span of $1, x$, for some $x \in K^*$. This defines a birational surjective map $\pi_x : X \to \mathbb{P}^1$ and a corresponding map of Galois groups $\pi_x^a : \mathcal{G}^a_K \to \mathcal{G}^a_{k(x)}$. Under this map, the image of $\mathcal{I}^a_\nu$ is zero (otherwise, C lies in a fiber of π_x and the whole group $\mathcal{G}^a_{\boldsymbol{K}_\nu}$ is mapped to the valuation group of $\pi_x(C) \subset \mathbb{P}^1$, contradicting the assumption that the image of ι is not a flag map on $\mathbb{P}^1_\iota = \mathbb{P}_k(k \oplus k \cdot x) = \mathbb{P}^1(k)$).

This gives a homomorphism $\eta_\nu : \mathcal{D}^a_\nu/\mathcal{I}^a_\nu \to \mathcal{G}^a_{k(x)}$ so that $\eta_\nu(\bar{\iota})$ is not a flag map on $k(x)$. Let $\psi_x : \mathcal{G}^a_{k(x)} \to V$ be any homomorphism such that $\psi_x(\bar{\iota}) \notin \psi(\mathcal{I}^a_w)$ for every $\mathcal{I}^a_w \subset \mathcal{G}^a_{\boldsymbol{K}_\nu}$, as in Lemma 10.2. The composition $\psi := \psi_x \circ \eta_\iota$ has the required properties. □

LEMMA 10.4. — *Let $E = k(C)$ be the function field of a curve. Then* $\mathrm{g}(C) \geq 1$ *iff there exists a nonzero homomorphism from $\mathcal{G}^a_E$ to a finite (abelian) group which maps all inertia elements to* 0.

Proof. — Indeed, every curve of genus ≥ 1 over a finite field of characteristic p has unramified coverings of degree ℓ. These coverings define maps of Galois groups, which are trivial on all inertia elements. If C is rational then $\mathcal{G}^a_E$, and hence its image under every homomorphism (onto any finite group), is generated by inertia elements (see the exact sequence (10.1)). □

REMARK 10.5. — Combining this with Proposition 10.3 we can decide in purely Galois-theoretic terms which divisorial valuations of K correspond to nonrational (irreducible) curves C on some model X of K. We call such valuations *nonrational*.

11. Valuations on surfaces

Next we are lead to the following problem: How to characterize subgroups $\widehat{k(C)}^* \subset \hat{K}^*$? We recall a geometric argument (from algebraic K-theory) characterizing pairs $f, g \in K^*$ which are contained in $k(C)^* \subset K^*$, for some curve C (such curves correspond to projections $X \to C$).

Let ν be a divisorial valuation of K and

$$\nu \,:\, K^* \to \mathbb{Z}$$

the valuation map. We have the residue map

$$\mathrm{res}_\nu \,:\, \mathrm{Ker}(\nu) \to \boldsymbol{K}^*_\nu$$

and a bilinear (with respect to multiplication) symbol

$$\begin{array}{ccc} K^* \times K^* & \xrightarrow{\varrho_\nu} & \boldsymbol{K}^*_\nu \\ f, g & \mapsto & (-1)^{\nu(f)\cdot\nu(g)} f^{\nu(g)}/g^{\nu(f)}. \end{array} \tag{11.1}$$

On a smooth model X of K, where $\nu = \nu_D$ for a divisor $D \subset X$, we define

$$\varrho_\nu = \varrho_D \,:\, K^* \times K^* \to \boldsymbol{K}^*_\nu \tag{11.2}$$

as follows:

- $\varrho_\nu(f, g) = 1$ if both f, g are invertible on D;

– $\varrho_\nu(f, g) = f_D^m$ if f is invertible (f_D is the restriction to D) and g has multiplicity m along D;
– $\varrho_\nu(f, g) = (f^{m_g}/g^{m_f})_D$ in the general case, when f, g have multiplicities m_f, m_g, respectively.

The definition does not depend on the choice of the model.

The following is a standard result in K-theory. We include a proof since we will need its ℓ-adic version.

LEMMA 11.1. — *For* $f, g \in K^*$

$$\varrho_\nu(f, g) = 1 \ \forall \nu \in \mathcal{DV}_K \iff f, g \in E = k(C) \subset K \textit{ for some curve } C.$$

Proof. — ($\Leftarrow$) On an appropriate model X we have $\nu = \nu_D$ for a divisor $D \subset X$ and $\pi : X \to C$ is regular and flat with irreducible generic fiber (and $f, g \in k(C)^*$). By definition, $\varrho_\nu(f, g) = 1$ if D is not in a fiber of π. If D is in a fiber then there is a $t \in k(C)^*, \nu_D(t) \neq 0$ such that both ft^{m_f}, gt^{m_g} are regular and constant on D (for some $m_f, m_g \in \mathbb{N}$) so that $\varrho_\nu(f, g) = 1$.

($\Rightarrow$) Assume that $\varrho_\nu(f, g) = 1$ for every $\nu \in \mathcal{DV}_K$. Every nonconstant function f defines a unique map (with irreducible generic fiber)

$$\pi_f : X \to C_f$$

which corresponds to the algebraic closure of $k(f)$ in K (we will say that f is induced from C_f). We claim that $\pi_f = \pi_g$.

Since f is induced from C_f, we have

$$\mathrm{div}(f) = \sum_{q \in Q} a_q D_q,$$

where $Q \subset C_f(k)$ is finite and $D_q = \pi^{-1}(q)$. Then $D_q^2 = 0$ and D_q is either a multiple of a fiber of π_g or it has an irreducible component $D \subset D_q$ which dominates C_g (under π_g). In the second case, the restriction of g to D_q is a nonconstant element in $k(D_q)$. Then $\nu_D(f) \neq 0$, while $\nu_D(g) = 0$. Hence $\varrho_D(f, g) \neq 1$ since it coincides with $g_D^{-\nu_D(f)} \neq 1$, a contradiction. Therefore, all D_q are contained in the finitely many fibers S of π_g. That means $\mathrm{div}(f)$ does not intersect the fibers $R_t, t \in C_g, t \notin S$ which implies that f is constant on such R_t. Hence f belongs to the normal closure of $k(C_g)$ in K, and in fact $f \in k(C_g)$ since $k(C_g)$ is algebraically closed in K, by construction. Thus f is induced from C_g and hence $C_f = C_g$ and $\pi_f = \pi_g$. □

12. ℓ-adic analysis: generalities

Let X be a smooth model of K. An element $f \in K^*/k*$ gives rise to a divisor $D = D_f$ on X and conversely, such a D uniquely determines f. Recall that the Galois group $\mathcal{G}_K^a$ determines $\hat{K}^*$, a group substantially bigger than K^*/k^*. In this section we introduce ℓ-adic versions of standard geometric notions in algebraic geometry (divisors, Picard group etc.).

For any smooth algebraic variety X over k with function field $K = k(X)$ we have an exact sequence

$$0 \to K^*/k^* \xrightarrow{\rho_X} \mathrm{Div}(X) \xrightarrow{\varphi} \mathrm{Pic}(X) \to 0, \tag{12.1}$$

where $\mathrm{Div}(X)$ is the group of (Weil or Cartier) divisors of X. Write

$$\mathrm{Div}(X)_\ell := \mathrm{Div}(X) \otimes \mathbb{Z}_\ell \quad \text{and} \quad \mathrm{Pic}(X)_\ell := \mathrm{Pic}(X) \otimes \mathbb{Z}_\ell$$

for the group of *finite* ℓ-adic divisors, resp. ℓ-adic Picard group. We have an exact sequence:

$$0 \to K^* \otimes \mathbb{Z}_\ell \xrightarrow{\rho_{X,\ell}} \mathrm{Div}(X)_\ell \xrightarrow{\varphi_\ell} \mathrm{Pic}(X)_\ell \to 0 \tag{12.2}$$

Let

$$\widehat{\mathrm{Div}}(X) := \{D = \sum_{m \in M} \hat{a}_m D_m\}, \quad \text{resp.} \quad \widehat{\mathrm{Div}}_{\mathrm{nr}}(X) \subset \widehat{\mathrm{Div}}(X),$$

be the group of divisors (resp. nonrational divisors) with *decreasing coefficients*:

- M is a countable set;
- for all $r \in \mathbb{Z}$ the set
$$\{m \,|\, |\hat{a}_m|_\ell \le r\}$$
is finite;
- for $D \in \widehat{\mathrm{Div}}_{\mathrm{nr}}(X)$, all D_m are nonrational.

Clearly, $\mathrm{Div}(X)_\ell \subset \widehat{\mathrm{Div}}(X)$. Every element

$$\hat{f} \in \hat{K}^* = \lim_{n \to \infty} K^*/(K^*)^{\ell^n}$$

has a representation

$$\hat{f} = (f_n)_{n \in \mathbb{N}} \text{ or } f = f_0 f_1^\ell f_2^{\ell^2} \cdots ,$$

with $f_n \in K^*$. We have homomorphisms

$$\begin{array}{rcl} \hat{\rho}_X : \hat{K}^* & \to & \widehat{\mathrm{Div}}(X), \\ \hat{f} & \mapsto & \mathrm{div}(\hat{f}) := \sum_{n\in\mathbb{N}} \ell^n \cdot \mathrm{div}(f_n) = \sum_m \hat{a}_m D_m, \end{array}$$

$$\hat{\rho}_{X,\mathrm{nr}} : \hat{K}^* \to \widehat{\mathrm{Div}}(X) \xrightarrow{\mathrm{pr}} \widehat{\mathrm{Div}}_{\mathrm{nr}}(X),$$

where $D_m \subset X$ are irreducible divisors,

$$\hat{a}_m = \sum_{n\in\mathbb{N}} a_{nm}\ell^n \in \mathbb{Z}_\ell,$$

with $a_{nm} \in \mathbb{Z}$, and

$$\mathrm{div}(f_n) = \sum_m a_{nm} D_m.$$

Here $\mathrm{div}(f_n)$ is the Cartier divisor of f_n and $\sum_m a_{nm} D_m$ is its image in the group of Weil divisors.

LEMMA 12.1. — *Let X/k be a smooth projective surface, M a* finite *set and*

$$D = \sum_{m\in M} a_m D_m \in \mathrm{Div}(X)_\ell, \quad a_m \in \mathbb{Z}_\ell$$

a divisor such that $\varphi_\ell(D) = 0$. Then there exist a finite set I, functions $f_i \in K^*$ and numbers $a_i \in \mathbb{Z}_\ell$, linearly independent over $\mathbb{Z}$, such that for all $i \in I$

$$\mathrm{supp}_X(f_i) \subset \mathrm{supp}_X(D)$$

and

$$D = \sum a_i \mathrm{div}(f_i).$$

Proof. — It suffices to consider equation (12.2) and to observe that any $\mathbb{Z}_\ell$-lattice of principal divisors with support in a finite set of divisors contains a generating $\mathbb{Z}$-lattice of principal divisors. □

The map $\hat{\rho}_X$ has a kernel

$$T_\ell(X) := \varprojlim \mathrm{Tor}_1(\mathbb{Z}/\ell^n, \mathrm{Pic}(X)[\ell]),$$

where $\mathrm{Pic}(X)[\ell] \subset \mathrm{Pic}(X)$ is the ℓ-power torsion subgroup. In particular $T_\ell(X) = \mathbb{Z}_\ell^{2\mathrm{g}}$, where g is the dimension of $\mathrm{Pic}^0(X)$. We now collect several facts about T_ℓ which will be used later on.

LEMMA 12.2. — *For varieties over k we have*

(1) *a morphism $\xi : X \to Y$ induces a homomorphism $\xi^*_\ell : T_\ell(Y) \to T_\ell(X)$;*
(2) *the canonical morphism $\mathrm{alb} : X \to \mathrm{Alb}(X)$ to the Albanese variety induces a canonical isomorphism $\mathrm{alb}^*_\ell : T_\ell(\mathrm{Alb}(X)) \to T_\ell(X)$;*
(3) *if $\xi : X' \to X$ is a birational isomorphism between smooth varieties then $\xi^*_\ell : T_\ell(X) \to T_\ell(X')$ is an isomorphism;*
(4) *an exact sequence of abelian varieties*

$$1 \to A' \to A \to A'' \to 1$$

induces an exact sequence

$$1 \to T_\ell(A'') \to T_\ell(A) \to T_\ell(A').$$

Proof. — The follows from the corresponding properties of the functor Pic^0 for smooth algebraic varieties over k. □

We have a diagram

(12.3)

$$\begin{array}{ccccccccccc} & & 0 & \to & K^* \otimes \mathbb{Z}_\ell & \xrightarrow{\rho_{X,\ell}} & \mathrm{Div}(X)_\ell & \xrightarrow{\varphi_\ell} & \mathrm{Pic}(X)_\ell & \to & 0 \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & T_\ell(X) & \to & \hat{K}^* & \xrightarrow{\hat\rho_X} & \widehat{\mathrm{Div}}(X) & \xrightarrow{\hat\varphi_\ell} & \widehat{\mathrm{Pic}}(X) & \to & 0, \end{array}$$

where

$$\widehat{\mathrm{Pic}}(X) := \varprojlim \mathrm{Pic}(X) \otimes \mathbb{Z}/\ell^n = \mathrm{NS}(X) \otimes \mathbb{Z}_\ell.$$

Every $\nu \in \mathcal{DV}_K$ gives rise to a homomorphism

$$\hat\nu : \hat{K}^* \to \mathbb{Z}_\ell$$

and a homomorphism

$$\hat{\mathrm{res}}_\nu : \mathrm{Ker}(\hat\nu) \to \hat{\boldsymbol{K}}^*_\nu$$

and a symbol

$$\hat\varrho_\nu : \hat{K}^* \times \hat{K}^* \to \hat{\boldsymbol{K}}^*_\nu.$$

On a smooth model X, where $\nu = \nu_D$ for a divisor $D \subset X$, $\hat\nu(\hat f)$ is the ℓ-adic coefficient at D of $\mathrm{div}(\hat f)$, while $\hat\varrho_\nu$ is the natural $\mathbb{Z}_\ell$-bilinear generalization of (11.1).

LEMMA 12.3. — *Let X be a smooth surface or a smooth curve over k and $K = k(X)$. Then*

$$T_\ell(X) = \cap_{\nu \in \mathcal{DV}_K} \mathrm{Ker}(\hat{\nu}).$$

Proof. — Follows from Lemma 12.2. □

In particular, we have the map $\hat{\mathrm{res}}_\nu : T_\ell(K) := T_\ell(X) \to \hat{\boldsymbol{K}}^*_\nu$.

LEMMA 12.4. — *For all $\nu \in \mathcal{DV}_K$ we have*

$$\hat{\mathrm{res}}_\nu(T_\ell(K)) \subset T_\ell(\boldsymbol{K}_\nu).$$

Proof. — Let X be a model of K such that $\nu = \nu_D$, where D is a smooth curve. We may assume (after blowing up) that X contains a divisor D' intersecting D in exactly one point. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(\nu) & \longrightarrow & \mathrm{Div}(X \setminus D) & \longrightarrow & \mathrm{Pic}(X) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{res}_\nu} & & \downarrow & & \downarrow{\scriptstyle \delta} & & \\ 0 & \longrightarrow & \boldsymbol{K}^*_\nu & \longrightarrow & \mathrm{Div}(D) & \longrightarrow & \mathrm{Pic}(D) & \longrightarrow & 0 \end{array}$$

where $\mathrm{Div}(X \setminus D)$ is the $\mathbb{Z}$-module spanned by divisors different from D. By the choice of X, the restriction δ induces a surjection $\mathrm{NS}(X) \to \mathrm{NS}(D)$.

Tensoring all $\mathbb{Z}$-modules with $\mathbb{Z}/\ell^n$ and passing to the projective limit we obtain a map

$$T_\ell(K) \to T_\ell(\boldsymbol{K}_\nu),$$

and the claim. □

13. ℓ-adic analysis: finite support

Our goal is to characterize the ℓ-adic space $K^*/k^* \otimes \mathbb{Z}_\ell \subset \hat{K}^*$. The Galois datum $(\mathcal{G}^a_K, \Sigma_K)$ allows us to distinguish between rational and nonrational irreducible divisors on X (via the corresponding valuations) and to describe intrinsically a subspace $\mathcal{FS}(K) \subset \hat{K}^*$ (of divisors with finite nonrational support, see 13.2 and 13.3). In this section we further shrink $\mathcal{FS}(K)$, giving an intrinsic characterization of those elements which have finite divisorial support on every smooth model X.

By Lemma 3.14, if $T_\ell(K) \neq 0$ then either X contains only finitely many rational curves, or X, modulo purely inseparable covers, is a rational pencil over a curve C of genus $\mathrm{g}(C) \geq 1$.

DEFINITION 13.1. — *We say that* $\hat{f}, \hat{g} \in \hat{K}^*$ commute *if* $\hat{\varrho}_\nu(\hat{f}, \hat{g}) = 1$, *for all divisorial* ν. *We say that they have* disjoint support *if for all divisorial valuations* $\nu \in \mathcal{DV}_K$

$$\hat{\nu}(\hat{f}) \cdot \hat{\nu}(\hat{g}) = 0.$$

We say that $\hat{f} \in \hat{K}^*$ *has nontrivial commutators if there exist* $\hat{g} \in \hat{K}^*$ *with disjoint support (from* $\hat{f}$*) which commute with* $\hat{f}$.

NOTATIONS 13.2. — We put

$$\begin{array}{lll} \mathrm{supp}_K(\hat{f}) & := \{ \ \nu \in \mathcal{DV}_K & | \ \ \hat{f} \text{ nontrivial on } \mathcal{I}^a_\nu \ \}; \\ \mathrm{supp}_X(\hat{f}) & := \{ \ \ D_m \subset X & | \ \ \hat{a}_m \neq 0 \ \}. \end{array}$$

DEFINITION 13.3. — *We say that* $\hat{f}$ *has* finite nonrational support *if the set of nonrational* $\nu \in \mathrm{supp}_K(\hat{f})$ *is finite (see Lemma 10.4 for the definition and Galois-theoretic characterization of nonrational valuations). Let*

$$\mathcal{FS}(K) \subset \hat{K}^*$$

be the subgroup of such elements.

Note that for $\hat{f} \in \mathcal{FS}(K)$, its nonrational component $\hat{\rho}_{X,\mathrm{nr}}(\hat{f})$ is independent of the model X. More precisely, for any birational morphism $X' \to X$ we can identify $\widehat{\mathrm{Div}}_{\mathrm{nr}}(X') = \widehat{\mathrm{Div}}_{\mathrm{nr}}(X)$. Under this identification

$$\rho_{X',\mathrm{nr}}(\hat{f}) = \rho_{X,\mathrm{nr}}(\hat{f}).$$

DEFINITION 13.4. — *We say that* $\hat{f}$ *has* finite support *on the model* X *if* $\mathrm{supp}_X(\hat{f})$ *is finite. Put*

$$\mathcal{FS}_X(K) \quad := \{\hat{f} \in \hat{K}^* \mid \rho_X(\hat{f}) \in \mathrm{Div}(X)_\ell\}.$$

LEMMA 13.5. — *The definition of* $\mathcal{FS}_X(K)$ *does not depend on the choice of a smooth model* X.

Proof. — For any two smooth models X', X'' we can find a smooth model X dominating both. The difference between the sets of irreducible divisors $\mathrm{Div}(X')$, resp. $\mathrm{Div}(X'')$, and $\mathrm{Div}(X)$ is finite and consists of rational curves. □

Equation (12.3) implies the exact sequence

$$0 \to T_\ell(X) \to \mathcal{FS}_X(K) \to K^*/k^* \otimes \mathbb{Z}_\ell \to 0. \tag{13.1}$$

Indeed, if $\hat{f} \in \mathcal{FS}_X(K)$ then $\mathrm{div}(\hat{f}) \in \mathrm{Div}(X)_\ell$ and its image in $\mathrm{Pic}(X)_\ell$ is zero. Thus there is an element $f \in K^*/k^* \otimes \mathbb{Z}_\ell$ with the same ℓ-adic divisor. By definition $\hat{f}/f \in T_\ell(X)$.

We proceed to give a Galois-theoretic characterization of $\mathcal{FS}_X(K)$.

Case I. Let K be the function field of a surface X containing only finitely many rational curves. Then

$$\mathcal{FS}(K) = \mathcal{FS}_X(K).$$

Case II. Assume that, after a purely inseparable extension, X admits a fibration over a curve of genus ≥ 1, with generic fiber a rational curve.

Let $\mathcal{FS}'(K) \subset \hat{K}^*$ be the group generated by all $\hat{f}$ such that

- $\hat{f}$ has nontrivial nonrational support;
- $\hat{f}$ has nontrivial commutators.

Then, for every model X of K, we have

$$\mathcal{FS}'(K) = \mathcal{FS}_X(K).$$

Indeed, an infinite rational tail in $\hat{f}$ in this case consists of an infinite number of fibers. Same holds for $\hat{g}$. Thus the divisor of $\hat{f}$ (resp. $\hat{g}$) intersects all but finitely many fibers in the infinite rational tail of $\hat{g}$ (resp. $\hat{f}$) with intersection multiplicity some power of $p = \mathrm{char}(k)$. Consider ν corresponding to rational curves in the divisor of $\hat{g}$ intersecting the divisor of $\hat{f}$ as above. Then

$$\hat{\varrho}_\nu(\hat{f}, \hat{g}) \neq 1,$$

contradiction.

Case III. By Lemma 3.14, we can now assume that $\mathrm{Pic}^0(X) = 0$.

Let $\mathcal{F}_X(K)$ be the set of all $f \in K(X)^*/k^*$ such that

(1) $\rho_{X,\mathrm{nr}}(f) \neq 0$ and

(2) for every rational curve $D \subset X$ with $\nu = \nu_D$ either $D \in \mathrm{supp}_X(f)$ or $\mathrm{res}_\nu(f) \neq 0 \mod \ell$ in $\boldsymbol{K}^*_\nu/k^*$.

Geometrically, condition (2) means that if a rational curve D is not a component of the divisor of f then there is a point in $D \cap \mathrm{div}(f)$ whose multiplicity is prime to ℓ.

LEMMA 13.6. — *Let $x \in K^*$ and let $k(y) := \overline{k(x)}^K$ be its normal closure in K. Let $\pi_y : \mathbb{P}^1_y \to \mathbb{P}^1_x$ be the corresponding morphism. Assume that*

(1) *$k(y)/k(x)$ is a separable extension of degree > 1;*
(2) *the preimage under π_y^{-1} of the divisor $0 + \infty \in \mathrm{Div}(\mathbb{P}^1_x)$ contains at least 4 points with multiplicities prime to ℓ.*

Then the image of x in K^*/k^* is in $\mathcal{F}_X(K)$.

Proof. — Let X be a smooth model of K and

$$\beta_x : X \to \mathbb{P}^1_x, \quad \beta_y : X \to \mathbb{P}^1_y$$

regular maps with $\beta_x = \pi_y \circ \beta_y$. Let R be an irredicible curve in X which surjects geometrically onto $\mathbb{P}^1_x$. We can assume that the map $\beta_x : R \to \mathbb{P}^1_x$ is separable (after a Frobenius twist of the function field of R).

Assume that the multiplicities of all poles and zeroes of the function y on R are divisible by ℓ (this does not change after a Frobenius twist). Thus the map $\beta_x : R \to \mathbb{P}^1_x$ has ramifications over 4-points divisible by ℓ. By the Hurwitz formula, $\mathrm{g}(R) > 0$.

In particular, for any rational curve $R \subset X$ either $\beta_y(R)$ is constant, so that R is contained in the fiber of β_y, or the intersection of R with some component of $\mathrm{Div}(x)$ contains points with multiplicity prime to ℓ. Thus, the image of x in K^*/k^* is in $\mathcal{F}_X(K)$.

□

COROLLARY 13.7. — *The set $\mathcal{F}_X(K)$ generates K^*/k^*.*

Proof. — The multiplicative group of every closed subfield $k(x) \subset K$ is generated by elements y satisfying the lemma. Indeed, for a y which is not generating $k(x)$ and which is not an $\ell - th$ power all elements of the form $y(x-a)/(x-b)$, where a, b run through k minus $\mathrm{Div}(y) \subset \mathbb{P}^1_x$, satisfy the lemma. By assumption, $\mathrm{Pic}^0(X) = 0$ so that every closed one-dimensional subfield of K is isomorphic to $k(x)$ for some x. □

LEMMA 13.8. — *For every pair of nonzero commuting elements* $\hat{f}, \hat{g} \in \mathcal{FS}(K)$ *with nontrivial nonrational support and disjoint support such that there exists an* $f \in \mathcal{F}_X(K)$ *with*

$$f = \hat{f} \mod \ell, \textit{ in } \hat{K}^*$$

one has $\hat{f} \in \mathcal{FS}_X(K)$ *and* $\hat{g} \in \mathcal{FS}_X(K)$.

Proof. — Write

$$\begin{array}{rcl} \rho_X(\hat{f}) & = & \sum_{i \in I} n_i D_i + \ell \sum_{j=1}^{\infty} n_j C_j, \\ \rho_X(\hat{g}) & = & \sum_{i \in I'} n'_i D'_i + \ell \sum_{j=1}^{\infty} n'_j C'_j, \end{array}$$

where I, I' are finite sets and the second sum is an infinite series over distinct rational curves $C_j, C'_j \subset X$. By assumption, the sets $\{D_i\}_{i\in I}$, $\{C_j\}_{j\in\mathbb{N}}$, $\{D'_i\}_{i\in I'}$, $\{C'_j\}_{j\in\mathbb{N}}$ are disjoint.

By assumption, $\hat{\varrho}_\nu(\hat{f}, \hat{g}) = 1$, for all ν. For $\nu = \nu_D$, where $D \in \mathrm{supp}_X(\hat{g})$, this symbol equals the residue of $\hat{f}$ on D, which equals the corresponding residue of $f \mod \ell$. For rational curves in the support of $\hat{g}$ it is nonzero by (2). Since the generic fiber of f is nonrational, there are only a finite number of rational curves on X which are mapped to points by f. It follows that every divisor in $\mathrm{supp}_X(\hat{g})$ is nonrational, unless it is in the fiber of f, and that $\hat{g} \in \mathcal{FS}_X(K)$.

Since $T_\ell(X) = 0$, we can write $\mathrm{div}(\hat{g}) = \sum_{m\in M} a_m D_m$, where M is a finite set, some $D_m \subset X$ are nonrational divisors and $a_m \in \mathbb{Z}_\ell$, or $\hat{g} = \prod_{i\in I''} g_i^{b_i}$, with I'' a finite set, $g_i \in K^*/k^*$ and $b_i \in \mathbb{Z}_\ell$.

The restriction of g_i to every irreducible component of the divisor of $\hat{f}$ is identically zero. This means that under the map

$$\pi_{g_i} : X \to C$$

all components of $\mathrm{supp}_X(\hat{f})$ map to points (note that $C = \mathbb{P}^1$, since $\mathrm{Pic}^0(X) = 0$). Since some components of the divisor of g_i, for some i, are nonrational, the generic fiber of π_{g_i} is also nonrational. Thus $\mathrm{supp}_X(\hat{f})$ contains only a finite number of rational divisors, so that $\hat{f} \in \mathcal{FS}_X(K)$. □

EXAMPLE 13.9. — Let $K = k(x, y)$ be the function field of $\mathbb{P}^2$. Let D_x, D_y be the divisors of functions x, y so that $a_x D_x + a_y D_y = a_z D_z$

with nonzero $a_x, a_y, a_z \in \mathbb{Z}_\ell$, for a principal divisor $D_z \subset \mathbb{P}^2$, iff $a_x/a_y \in \mathbb{Q}$. Indeed, the function $z = x^{b_x}y^{b_y}$, for $b_x, b_y \in \mathbb{Z}$. Then $a_xD_x + a_yD_y = a_z(b_xD_x + b_yD_y)$ and $a_x = a_zb_x$, $a_y = a_zb_y$. Thus $a_x/a_y = b_x/b_y \in \mathbb{Q}$.

Generalizing this example, we have:

LEMMA 13.10. — *Let $x, y \in \mathcal{FS}_X(K)$ be noncommuting elements. Assume that the three elements x, y, xy have nontrivial commutators in $\mathcal{FS}_X(K)$. Then there exists a unique $a \in \mathbb{Z}_\ell$, modulo $\mathbb{Z}_{(\ell)}$, such that*

$$x, y, xy \in a \cdot K^*/k^* \subset \mathcal{FS}_X(K)$$

Proof. — Let P_x, P_y and P_{xy} be minimal $\mathbb{Z}$-sublattices of $\mathcal{FS}_X(K)$ such that $x \in P_x \otimes \mathbb{Z}_\ell$, $y \in P_y \otimes \mathbb{Z}_\ell$ and $xy \in P_{xy} \otimes \mathbb{Z}_\ell$. We have

$$P_{xy} \otimes \mathbb{Z}_\ell \subset P_x \otimes \mathbb{Z}_\ell \oplus P_y \otimes \mathbb{Z}_\ell.$$

Note that $P_x \cap P_y = 0$, and $P_x \cap P_{xy} = 0$, resp. $P_y \cap P_{xy} = 0$, since there are no $\mathbb{Z}$-relations - the elements of P_x, resp. P_y, resp. P_{xy}, belong to the same pencil and nontrivial elements of different pencils are distinct. The lattice $P_{xy} \otimes \mathbb{Z}_\ell$ surjects onto both $P_x \otimes \mathbb{Z}_\ell$ and $P_y \otimes \mathbb{Z}_\ell$. If one of the projections had a kernel, there would be an element in P_x belonging to the pencil P_{xy}, and similarly for P_y, but there are no common elements. We conclude that both projections are isomorphisms of $\mathbb{Z}_{(\ell)}$-lattices, as claimed. □

COROLLARY 13.11. — *Let $\mathcal{K} \subset \mathcal{FS}(K)$ be a lattice such that*
- *every element in $\mathcal{K}$ has a nontrivial commutator and*
- *$\mathcal{K}$ surjects onto K^*/ℓ.*

Then then there is $a \in \mathbb{Z}_\ell^*$ such that $a \cdot \mathcal{K} \subset K^* \otimes \mathbb{Z}_{(\ell)}$.

Proof. — Since $\mathcal{K}$ is generated by the preimages of the reduction of $\mathcal{F}_X(K)$ modulo ℓ (only such elements have nontrivial commutators, by Lemma 13.8), the lattice $\mathcal{K}$ is contained in $\mathcal{FS}_X(K)$. Then we apply Lemma 13.10. □

In particular, any such lattice is contained in $a^{-1} \cdot K^* \otimes \mathbb{Z}_{(\ell)}$ with the same property. It follows that there is a unique maximal lattice for any triple of elements x, y, xy with nontrivial commutators so that $\rho_\nu(x, y) \neq 0 \mod \ell$ for some $\nu \in \mathcal{DV}_K$. It equals $a \cdot K^* \otimes \mathbb{Z}_{(\ell)}$, for some $a \in \mathbb{Z}_\ell^*$.

14. ℓ-adic analysis: curves

In this section we begin the process of recognition of the lattice $K^*/k^* \subset \hat{K}^*$. We solve an analogous problem for the function field of a rational curve. This result will play an essential role in the analysis of surfaces.

PROPOSITION 14.1. — *Let $\tilde{k}$ be the algebraic closure of a finite field, with* $\mathrm{char}(\tilde{k}) \neq \ell$, *$C$ a curve over $\tilde{k}$ of genus* g *with function field $E = \tilde{k}(C)$ and*

$$\Psi \,:\, \mathcal{G}^a_E \to \mathcal{G}^a_{k(\mathbb{P}^1)}$$

an isomorphism of Galois groups inducing an isomorphism on inertia groups of divisorial valuations, that is, a bijection on the set of such groups and isomorphisms of corresponding groups. Let

$$\Psi^* \,:\, \widehat{k(\mathbb{P}^1)^*} \to \hat{E}^*$$

be the dual isomorphism. Then $E = \tilde{k}(\mathbb{P}^1)$ and there is a constant $a \in \mathbb{Z}_\ell^*$ such that $\Psi^*(k(\mathbb{P}^1)^*/k^*) = a \cdot E^*/\tilde{k}^*$.

Proof. — Recalling the exact sequence (10.1), we have a commuting diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_\ell(\Delta_{C(\tilde{k})}) & \longrightarrow & \mathcal{M}(C(\tilde{k})) & \longrightarrow & \mathcal{G}^a_E & \longrightarrow & \mathbb{Z}_\ell^{2\mathrm{g}} \longrightarrow 0 \\ & & & & & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}_\ell(\Delta_{\mathbb{P}^1(k)}) & \longrightarrow & \mathcal{M}(\mathbb{P}^1(k)) & \longrightarrow & \mathcal{G}^a_{k(\mathbb{P}^1)} & \longrightarrow & 0 \end{array}$$

Since Ψ is an isomorphism on inertia groups $\mathcal{I}^a_w$, for each w, the *sets* $C(\tilde{k})$ and $\mathbb{P}^1(k)$ coincide and we get a *unique* isomorphism of $\mathbb{Z}_\ell$-modules (of maps to $\mathbb{Z}_\ell$)

$$\mathcal{M}(C(\tilde{k})) = \mathcal{M}(\mathbb{P}^1(\tilde{k})).$$

In particular, we find that $\mathrm{g} = 0$ and $E = \tilde{k}(\mathbb{P}^1)$. Further, we have an induced isomorphism

$$\mathbb{Z}_\ell(\sum_{w\in\mathcal{V}_E} \delta_w) = \mathbb{Z}_\ell(\sum_{w'\in\mathcal{V}_{k(\mathbb{P}^1)}} \delta_{w'})$$

so that

$$(\sum_{w\in\mathcal{V}_E} \delta_w) = a(\sum_{w'\in\mathcal{V}_{k(\mathbb{P}^1)}} \delta_{w'})$$

for some $a \in \mathbb{Z}_\ell^*$. This implies that $\delta_w = a\delta_{w'}$, for all $w \in \mathcal{V}_E$ and the corresponding $w' \in \mathcal{V}_{\mathbb{P}^1}$. For the dual groups we obtain

$$E^*/\tilde{k}^* = (K^*/k^*)^a,$$

where $a \in \mathbb{Z}_\ell^*$. □

15. ℓ-adic analysis: surfaces

We will need an ℓ-adic version of Lemma 11.1 .

PROPOSITION 15.1. — *Let $\hat{f}, \hat{g} \in \mathcal{FS}_X(K)$ be elements with nontrivial support such that*

- $\varrho_\nu(\hat{f}, \hat{g}) = 1$ *for every* $\nu \in \mathcal{DV}_K$*;*
- $\mathrm{supp}_K(\hat{f}) \cap \mathrm{supp}_K(\hat{g}) = \emptyset$,

that is, $\hat{f}$ has nontrivial commutators. Then there is a 1-dimensional field $E = k(C) \subset K$ such that $\hat{f}, \hat{g} \in \hat{E}^*$.

Proof. — By Lemma 12.1,

$$\hat{f} = t_f \cdot f, \quad \text{where} \quad f := \prod_{i \in I} f_i^{a_i}, \text{ resp. } \hat{g} = t_g \cdot g, \quad \text{where} \quad g := \prod_{j \in J} g_j^{b_j},$$

where

- $t_f, t_g \in T_\ell(X)$;
- I, J are finite sets;
- $f_i, g_j \in K^*$ for all i, j;
- $a_i \in \mathbb{Z}_\ell$ (resp. $b_j \in \mathbb{Z}_\ell$) are linearly independent over $\mathbb{Z}$.

Fix a valuation $\nu = \nu_D$, where D is in the support of $\hat{g}$ on a (smooth) model X. By assumption

$$\hat{\mathrm{res}}_\nu(t_f \cdot \prod_{i \in I} f_i^{a_i}) = 1 \in \hat{\boldsymbol{K}}_\nu^*.$$

By Lemma 12.4, $\hat{\mathrm{res}}_\nu(t_f) \in T_\ell(\boldsymbol{K}_\nu)$ so that t_f has trivial support on D. We claim that for all $i \in I$, $\mathrm{res}_\nu(f_i) = 1 \in \boldsymbol{K}_\nu^*/k^*$. The divisor of the restriction of f_i to D is $\sum_{i'} r_{ii'} q_{ii'}$, where $q_{ii'}$ are points on D and $r_{ii'} \in \mathbb{Z}$. This gives a relation

$$\sum_{i \in I} a_i (\sum_{i'} r_{ii'} q_{ii'}) = 0.$$

However, a_i were linearly independent over $\mathbb{Z}$ which implies that $r_{ii'} = 0$, for all i, i'. In particular, $\mathrm{res}_\nu(f_i) \in k^*$. The same argument for g shows that g and f commute and that all pairs f_i, g_j commute as well. By Lemma 11.1, all $f_i, g_j \in E = k(C) \subset K$ for some curve C.

We now have a diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_\ell(E) & \longrightarrow & \hat{E}^* & \longrightarrow & \widehat{\mathrm{Div}}(C) & \longrightarrow & \widehat{\mathrm{Pic}}(C) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T_\ell(K) & \longrightarrow & \hat{K}^* & \longrightarrow & \widehat{\mathrm{Div}}(X) & \longrightarrow & \widehat{\mathrm{Pic}}(X) & \longrightarrow & 0 \end{array}$$

We need to show that t_f (resp. t_g) is in the image of $T_\ell(E)$. Let D be an irreducible component in the divisor of g (resp. f). Changing the model, we may assume that D is smooth. We have a diagram

$$\begin{array}{ccccc} D & \longrightarrow & X & & \\ \downarrow & & \downarrow & & \\ \mathrm{Jac}(D) & \xrightarrow[\iota]{} & \mathrm{Alb}(X) & \xrightarrow[\alpha]{} & A = \mathrm{Alb}(X)/B \end{array}$$

where α is a surjection with connected fibers and $B = B_D$ is as in Lemma 3.15: it is the minimal abelian subvariety of $A^0(X)$ so that the image of D in $\mathrm{Alb}(X)/B$ is a point, a_D (note that D is irreducible). We have

$$\iota(\mathrm{Jac}(D)) = \alpha^{-1}(a_D) \simeq B.$$

Applying Lemma 12.2 (4) we conclude that the induced sequence

$$T_\ell(A) \xrightarrow{\alpha_\ell^*} T_\ell(\mathrm{Alb}(X)) \xrightarrow{\iota_\ell^*} T_\ell(B)$$

of free finite rank $\mathbb{Z}_\ell$-modules is exact in the middle term. We have shown that $\mathrm{res}_\nu(f_i) = 1$, for all $i \in I$. It follows that $\hat{\mathrm{res}}_\nu(t_f) = 1 \in \boldsymbol{K}_\nu^*$, where $\nu = \nu_D$ is the corresponding valuation. In particular,

$$t_f = 1 \in T_\ell(B) \hookrightarrow T_\ell(\boldsymbol{K}_\nu) = T_\ell(D).$$

It follows that there is an $a \in T_\ell(A)$ such that $\alpha_\ell^*(a) = t_f$. We apply this argument to every component D_j of the divisor of g and find that t_f is induced from quotients $\mathrm{Alb}(X)/B_j$, where $B_j := B_{D_j}$, for $j \in J$. Let B be the abelian subvariety of $A^0(X)$ generated by B_j. By Lemma 3.15, $\mathrm{Alb}(A)/B \simeq \mathrm{Jac}(C)$, and X maps to C with connected fibers. We have the diagrams

$$\begin{array}{ccc} X & \longrightarrow & \mathrm{Alb}(X) \\ \downarrow & & \downarrow \\ C & \longrightarrow & \mathrm{Jac}(C) \end{array} \qquad \begin{array}{ccc} T_\ell(X) & \longleftarrow & T_\ell(\mathrm{Alb}(X)) \\ \uparrow & & \uparrow \\ T_\ell(C) & \xleftarrow{\sim} & T_\ell(\mathrm{Jac}(C)) \end{array}$$

It follows that t_f, and similarly t_g, is in $T_\ell(C) = T_\ell(E)$. $\square$

REMARK 15.2. — For every $f \in K^*$ the element $g = (f+a)(f+b)$ where $a \neq b$ and $ab \neq 0$, satisfies the conditions of Proposition 15.1.

Proposition 15.1 characterizes Galois-theoretically subgroups $\hat{E}^* \subset \hat{K}^*$ corresponding to 1-dimensional subfields of K. We now have:

PROPOSITION 15.3. — *The group $K^*/k^* \otimes \mathbb{Z}_\ell \subset \mathcal{FS}_X(K)$ is generated by subgroups $\hat{E}^* \cap \mathcal{FS}_X(K)$ with $E = k(C)$ so that that $T_\ell(E)$ is trivial. Moreover,*

$$(K^*/k^* \otimes \mathbb{Z}_\ell) \cap T_\ell(X) = 1.$$

Proof. — First of all, $T_\ell(C) \hookrightarrow T_\ell(X)$, for every 1-dimensional subfield $k(C) \subset K$. It suffices to note that multiplicative groups $E^*/k*$ of normally closed subfields $E = k(x)$, with $T_\ell(E)$ trivial, generate K^*/k^*. $\square$

COROLLARY 15.4. — *We have a canonical isomorphism*

$$\Psi^* \,:\, L^*/l^* \otimes \mathbb{Z}_\ell \to K^*/k^* \otimes \mathbb{Z}_\ell.$$

PROPOSITION 15.5. — *Let $\mathfrak{M}^* \subset K^*/k^* \otimes \mathbb{Z}_\ell$ be a subset with the following properties:*

1. *$\mathfrak{M}^*$ is closed under multiplication;*
2. *$\mathfrak{M}^* \cap \hat{E}^* = a_E \cdot E^*/k^*$ for every 1-dimensional normally closed subfield $E = k(x) \subset K$, with $a_E \in \mathbb{Z}_\ell^*$;*
3. *there exists a $\nu_0 \in \mathcal{DV}_K$ such that*

$$\{[\delta_0, \hat{f}] \mid \hat{f} \in \mathfrak{M}^*\} = \mathbb{Z}$$

for a topological generator δ_0 of $\mathcal{I}^a_{\nu_0}$. (Here $[\cdot, \cdot]$ is the value of $\hat{f}$ on the element of the Galois group δ_0, see Theorem 6.5.)

Then

$$\mathfrak{M}^* \subset K^*/k^* \otimes \mathbb{Z}_{(\ell)} \quad \textit{and} \quad \mathfrak{M}^* \otimes \mathbb{Z}_{(\ell)} = K^*/k^* \otimes \mathbb{Z}_{(\ell)}.$$

Proof. — For $x \in K \setminus k$ let $E = k(x)$ be the corresponding 1-dimensional field, assumed to be normally closed in K. By assumption, there exists an $a_E \in \mathbb{Z}_\ell^*$ such that

$$\mathfrak{M}^* \cap \hat{E}^* = a_E \cdot E^*/k^*.$$

If some (any) topological generator δ_0 of $\mathcal{I}^a_{\nu_0}$ is not identically zero on $\hat{E}^*$ then there exists a (smooth) model X, where ν_0 is realized by a divisor D_0, together with a morphism

$$X \to \mathbb{P}^1 = \mathbb{P}^1_E$$

such that D_0 dominates $\mathbb{P}^1$. It follows that

$$a_E \in \mathbb{Q} \cap \mathbb{Z}_\ell^* = \mathbb{Z}_{(\ell)}.$$

It remains to observe that every $x \in K^*$ can be written as a product

$$x = x' \cdot x''$$

such that δ_0 is nontrivial on both normally closed $E' = k(x')$ and $E'' = k(x'')$.

Finally, every group $k(x)^*/k^* \otimes \mathbb{Z}_{(\ell)}$ is generated over $\mathbb{Z}_{(\ell)}$ by elements from $\mathfrak{M}^*$. □

COROLLARY 15.6. — *There exists a constant $c \in \mathbb{Z}_\ell^*$ such that*

$$c\Psi^* \,:\, cL^*/l^* \otimes \mathbb{Z}_{(\ell)} \to K^*/k^* \otimes \mathbb{Z}_{(\ell)}.$$

is an isomorphism.

Proof. — Note that $\Psi^*(L^*/l^*)$ satisfies all conditions of Proposition 15.5, except possibly (3). Multiplication of the lattice $\Psi(L^*/l^*)$ by a constant $c \in \mathbb{Z}_\ell^*$ gives (3). □

COROLLARY 15.7. — *After a choice of δ_0, for every 1-dimensional $E \subset K$ and every $f \in E^*/k^* \otimes \mathbb{Z}_{(\ell)}$ we can Galois-theoretically distinguish its poles from its zeroes.*

16. Projective structure

In Section 15 we have proved that

$$c\Psi^*(L^*/l^*) \subset K^*/k^* \otimes \mathbb{Z}_{(\ell)} \supset K^*/k^*$$

for some $c \in \mathbb{Z}_\ell^*$. Let $\mathfrak{M}^* := c\Psi^*(L^*/l^*) \cap (K^*/k^*)$ be the intersection. Then $\mathfrak{M}^* \subset K^*/k^*$ and $(c\Psi^*)^{-1}(\mathfrak{M}^*) \subset L^*/l^*$ satisfy all conditions of Proposition 15.5. Moreover, the full preimages of these groups to K^*, resp. L^*, satisfy the conditions of Proposition 3.12. Therefore, there exist subfields $K_1 \subset K$ and $L_1 \subset L$ so that K/K_1 and L/L_1 are finite purely inseparable extensions and

$$c\Psi^*(L_1/l^*) = \mathfrak{M}^* = K_1^*/k^*.$$

The sets $c\Psi^*(L_1/l^*)$ and K_1^*/k^* carry canonical projective structures coming from field structures of L_1 and K_1. A priori, this induces two projective structures on $\mathfrak{M}^*$. The last essential step is to show that these structures on $\mathfrak{M}^*$ coincide. It suffices to show that primary lines in both structures are the same on $\mathfrak{M}^*$ (see Definition 3.4 and Definition 4.7).

LEMMA 16.1. — *Let $x \in K^*$ be a generating element, $E := k(x)$ and $r = r(x) \in \mathbb{N}$ the smallest positive integer such that x^r, modulo k^* is in $\mathfrak{M}^*$. Then*

- $r = p^m$ *for some* $m \in \mathbb{N}$ *(with* $p = \mathrm{char}(k)$*);*
- $(E^*/k^*) \cap \mathfrak{M}^* = (E^{p^m})^*/k^*$*;*
- *(pointwise)* p^m*-th powers of primary lines in* E^*/k^* *coincide with primary lines in* $(E^{p^m})^*/k^*$.

Proof. — The first property follows since K/K_1 is a finite purely inseparable extension, by Propositions 3.12 and 15.5. Next, we claim that a generating element $y \in K_1$ (see 3.4) is a p^m-th power of a generating element of K (for some m depending on y). Indeed, $E := \overline{k(y)}^K \subset K$ is a finite and purely inseparable extension of $k(y)$, $E := k(x)$ (for some $x \in K$). Thus

$$y = (ax^{p^m} + b)/(cx^{p^m} + d) = ((a'x + b')/(c'x + d'))^{p^m}$$

for some $m \in \mathbb{Z}$, $a, b, c, d \in k$ and their p^m-th roots $a', b', c', d' \in k$ (since k is algebraically closed).

In particular, a generating element $y \in K_1$ is in $E^*/k^* \cap \mathfrak{M}^*$ (and is the minimal positive power of a generator in E contained in $E^*/k^* \cap \mathfrak{M}^*$). This implies the third property: the generating elements of E^{p^m} are p^m-th powers of generators of E. □

LEMMA 16.2. — *The isomorphism $c\Psi^* : L_1^*/l^* \to K_1^*/k^*$ induces isomorphisms of multiplicative groups*

$$c\Psi^* : l(t)^*/l^* \to k(x)^*/k^*,$$

where $l(t)$, resp. $k(x)$ are algebraically closed 1-dimensional subfields in L_1, resp. K_1, inducing a bijection on (the images of) generating elements of the corresponding fields.

Proof. — For elements of $l(t)^*/l^*$, resp. $k(x)^*/k^*$, we have a Galois-theoretic notion of divisorial "support". This characterizes elements of minimal, by inclusion, divisorial support. These elements have also minimal support on $\mathbb{P}^1_x$ and hence their support on $\mathbb{P}^1_x$ consists of two points. Thus they are powers of the images of generating elements in $k(x)$. Among all elements with fixed minimal divisorial support we distinguished the primitive elements (with respect to multiplication). These primitive elements are generating elements of L_1, resp. K_1, and $c\Psi^*$ establishes a bijection on (images in L_1^*/l^*, resp. K_1^*/k^*, of) generating elements. □

COROLLARY 16.3. — *The isomorphism $c\Psi^* : L_1^*/l^* \to K_1^*/k^*$ identifies primary lines of the corresponding projective structures.*

Proof. — By Corollary 15.7 we can Galois-theoretically distinguish zeroes and poles of elements in L_1^*/l^* and K_1^*/k^*. By Lemma 16.2, if $l(t)$, resp. $k(x)$, is a normally closed 1-dimensional subfield in L_1, resp. K_1, then the restriction

$$c\Psi^* : l(t)^*/l^* \to k(x)^*/k^*$$

induces a bijection on (the images of) generating elements which have the same poles. The set of elements of $l(t)$, resp. $k(x)$, with the same pole is a primary line in $\mathbb{P}_l(L_1)$, resp. $\mathbb{P}_k(K_1)$. In particular, $c\Psi^*$ identifies the primary lines in the projective structures on $\mathcal{M}^*$. □

17. Proof

In this section we prove our main theorem: if

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

where L is a function field over an algebraic closure of a finite field of characteristic $\neq \ell$, then K is a purely inseparable extension of L. Moreover, for some $c \in \mathbb{Z}_\ell^*$, $c\Psi$ is induced by an isomorphism $\bar{\Psi}$ of the perfect closure of K with the perfect closure of L and the pair $(c, \bar{\Psi})$ is unique up to

$$(c, \bar{\Psi}) \mapsto (p^n c, (x \mapsto x^{p^n} \circ \bar{\Psi}).$$

Step 1. We have a nondegenerate pairing

$$\mathcal{G}_K^a \times \hat{K}^* \to \mathbb{Z}_\ell(1).$$

This induces the dual isomorphism

$$\Psi^* \,:\, \hat{L}^* \to \hat{K}^*.$$

Step 2. In Sections 4-9 we characterize intrinsically the inertia and decomposition groups of divisorial valuations:

$$\mathcal{I}_\nu^a \subset \mathcal{D}_\nu^a \subset \mathcal{G}_K^a :$$

every liftable subgroup $\sigma \in \Sigma_K^{\mathrm{div}} \subset \Sigma_K$ contains an inertia element of a divisorial valuation (which is also contained in at least one other $\sigma' \in \Sigma_K$). The corresponding decomposition group is the "centralizer" of the (topologically) cyclic inertia group (the set of all elements which "commute" with inertia).

By assumption, the isomorphism Ψ of Galois groups induces a bijection on the sets of maximal topologically noncyclic liftable subgroups. This gives a bijection of sets of divisorial valuations of the corresponding fields

$$\Psi \,:\, \mathcal{DV}_K \to \mathcal{DV}_L,$$

and induces a canonical isomorphism of Galois groups of the residue fields

$$\Psi_\nu \,:\, \mathcal{D}_\nu^a/\mathcal{I}_\nu^a = \mathcal{G}_{\boldsymbol{K}_\nu}^a \to \mathcal{G}_{\boldsymbol{L}_{\Psi(\nu)}}^a,$$

for all $\nu \in \mathcal{DV}_K$.

Step 3. For every $\nu \in \mathcal{DV}_K$ the isomorphism Ψ_ν defines a canonical isomorphism of inertia subgroups

$$\Psi_\nu : \qquad \mathcal{G}_{\boldsymbol{K}_\nu}^a \longrightarrow \mathcal{G}_{\boldsymbol{L}_{\Psi(\nu)}}^a$$

$$\Psi_{\nu,w} : \qquad \mathcal{I}_w^a \longrightarrow \mathcal{I}_{\Psi_\nu(w)}^a$$

of divisorial valuations of the corresponding residue fields: points on smooth models - curves - of these fields (see Proposition 10.3). In practical terms, this establishes a bijection on the sets of all curves, and all points on these curves, on all models of K, resp. L. This bijection does not change when Ψ is multiplied by a constant $c \in \mathbb{Z}_\ell^*$ and under purely inseparable extensions of K or L.

Step 4. We distinguish divisorial valuations with nonrational centers (see Lemma 10.4 and Remark 10.5).

Step 5. For $\hat{f} \in \hat{K}^*$ we have two notions of support: $\mathrm{supp}_K(\hat{f})$ (intrinsic) and $\mathrm{supp}_X(\hat{f})$ (depending on a model X) and two notions of finiteness: $\hat{f}$ is nontrivial on at most finitely many nonrational divisorial valuations ν, resp. $\hat{f}$ has finite divisorial support on a model. We defined $\mathcal{FS}(K) \subset \hat{K}^*$ as the subgroup of elements satisfying the first notion of finiteness, and $\mathcal{FS}_X(K) \subset \hat{K}^*$ as the subgroup of elements satisfying the second notion (this subgroup does not depend on the choice of a model X of K). By Step 4, the characterization of $\mathcal{FS}(K)$ is Galois-theoretic and we obtain an isomorphisms

$$\Psi^* \,:\, \mathcal{FS}(L) \to \mathcal{FS}(K).$$

Step 6. If some (any) model X of K contains only finitely many rational curves then $\mathcal{FS}(K) = \mathcal{FS}_X(K)$. In general, it may happen that the Ψ^*-image of some $g \in L^*/l^*$ has an "infinite rational tail" on some (every) model X of K:

$$\rho_X(\Psi^*(g)) = \rho_{X,\mathrm{nr}}(\Psi^*(g)) + \sum_{j\ge 1} n_j C_j,$$

where C_j are irreducible rational curves on X. In Lemma 13.6 we show that Ψ^*-images of many elements of $L^*/l^* \subset \mathcal{FS}(L)$ have finite support on every model X of K, and vice versa. In particular, we obtain a canonical isomorphism

$$\Psi^* \,:\, \mathcal{FS}_Y(L) \to \mathcal{FS}_X(K),$$

where Y is a model of L and X a model of K. Combining the exact sequence (13.1) with Lemma 12.3 we obtain a canonical isomorphism

$$\Psi^* \,:\, L^*/l^* \otimes \mathbb{Z}_\ell \to K^*/k^* \otimes \mathbb{Z}_\ell.$$

Step 7. For every pair of elements $\hat{f}, \hat{g} \in \mathcal{FS}_X(K)$ satisfying

- $\mathrm{supp}_K(\hat{f}) \cap \mathrm{supp}_K(\hat{g}) = \emptyset$;
- $\varrho_\nu(\hat{f}, \hat{g}) = 1$ for all $\nu \in \mathcal{DV}_K$

there exists a subfield $E = k(C) \subset K$ such that $\hat{f}, \hat{g} \in \hat{E}^*$ (Proposition 15.1). This gives canonical isomorphisms between completions of multiplicative groups of normally closed 1-dimensional subfields in K and L, inside $K^*/k^* \otimes \mathbb{Z}_\ell$. This isomorphism preserves the genus of the corresponding curves.

Step 8. Proposition 14.1 identifies E^*/k^* inside $\hat{E}^*$, up to conformal equivalence with respect to multiplication by elements in $\mathbb{Z}_\ell^*$. More precisely, there exist an $c \in \mathbb{Z}_\ell^*$, an $x \in K^* \setminus k^*$ and a $y \in L^* \setminus l^*$ such that

$$c \cdot \Psi^* \, : \, l(y)^*/l^* \to k(x)^*/k^*$$

is an isomorphism of multiplicative groups of subfields of K, resp. L.

Step 9. Let $\mathfrak{M}^* = c\Psi^*(L^*/l^*) \cap K^*/k^*$. By Proposition 3.12, we have finite purely inseparable extensions K/K_1 and L/L_1 such that $\mathfrak{M}^* = K_1^*/k^*$ and $\mathfrak{M}^* = c\Psi^*(L_1^*/l^*)$, as a multiplicative group. Thus, $\mathfrak{M}^*$ carries two structures of an abstract projective space compatible with the multiplicative structure (see Example 4.5), induced from the additive structure on K_1, resp. L_1.

Step 10. By Theorem 4.6 the field is uniquely determined by the partial projective structure on $\mathfrak{M}^*$ consisting of primary lines (see Lemma 4.8 and Lemma 4.9).

Step 11. Corollary 16.3 shows that the map $c\Psi^*$ identifies primary lines of these two structures. This defines a unique projective structure on $\mathfrak{M}^*$, compatible with multiplication. It follows that $c\Psi^*$ induces an isomorphism of fields

$$L \supset L_1 \simeq K_1 \subset K,$$

and of perfect closures of L and K. This concludes the proof of Theorem 1.

References

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

[2] F. A. BOGOMOLOV – "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.

[3] F. A. BOGOMOLOV and Y. TSCHINKEL – "Commuting elements in Galois groups of function fields", in *Motives, Polylogarithms and Hodge theory*, International Press, 2002, p. 75–120.

[4] N. BOURBAKI – *Commutative algebra. Chapters 1–7*, Elements of Mathematics, Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation.

[5] I. EFRAT – "Construction of valuations from K-theory", *Math. Res. Lett.* **6** (1999), no. 3-4, p. 335–343.

[6] O. ENDLER – *Valuation theory*, Springer-Verlag, New York, 1972, To the memory of Wolfgang Krull (26 August 1899–12 April 1971), Universitext.

[7] R. J. MIHALEK – *Projective geometry and algebraic structures*, Academic Press, New York, 1972.

[8] S. MOCHIZUKI – "The local pro-p anabelian geometry of curves", *Invent. Math.* **138** (1999), no. 2, p. 319–423.

[9] F. POP – "On Grothendieck's conjecture of birational anabelian geometry", *Ann. of Math. (2)* **139** (1994), no. 1, p. 145–182.

[10] J.-P. SERRE – *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[11] O. ZARISKI and P. SAMUEL – *Commutative algebra. Vol. II*, Springer-Verlag, New York, 1975, Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.