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

Introduction

We fix two primes p and ℓ. We will assume that $\ell \neq p$ and $p \neq 2$. Let $k = \overline{\mathbb{F}}_p$ 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. We will refer to X as a *model* of K. Let $\mathrm{Pic}(X)$ be the Picard group, $\mathrm{NS}(X)$ the Néron-Severi group of X and $\mathcal{G}_K^a$ 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 on $\mathcal{G}_K^a$: a set Σ_K of distinguished (primitive) subgroups which are isomorphic to *finite rank* (torsion free) $\mathbb{Z}_\ell$-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.

We will call Σ_K a fan. The main theorem of this paper is

THEOREM 1. — *Let K and L be function fields over algebraic closures of finite fields of characteristic $\neq 2, \ell$. Assume that $K = k(X)$ is a function field of a surface X/k such that*

(1) $\mathrm{Pic}(X) = \mathrm{NS}(X)$;
(2) *there exists an isomorphism*

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

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

$$\Sigma_K = \Sigma_L.$$

Then L is a finite purely inseparable extension of K.

The conditions on X do not depend on a choice of a model, which we can assume to be smooth (by resolution of singularities in dimension two). We chose to treat in detail a class of surfaces for which the proof of Theorem 1 is most transparent. The assumption (1) is not necessary; we have included it since it allows us to avoid certain geometric technicalities.

In this paper 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 [8], [7] and [5]).

2. Basic algebra and geometry of fields

In this section we collect some technical results about function fields.

NOTATIONS 2.1. — Throughout, k is an algebraic closure of the finite field $\mathbb{F} = \mathbb{F}_p$ and $K = k(X)$ the function field of an algebraic variety X/k over k (its *model*).

We assume familiarity with
– basic notions of field theory (transcendence degree, purely inseparable extensions);
– basic notions of algebraic geometry (models X of a field K, k-rational points $X(k)$, Picard group $\mathrm{Pic}(X)$, Néron-Severi group $\mathrm{NS}(X)$).

LEMMA 2.2. — *Let C/k be a smooth curve and $Q \subset C(k)$ a finite set. Then there exists an $n = n_Q \in \mathbb{N}$ such that for every degree zero divisor D with support in Q the divisor nD is principal.*

Proof. — Every finitely generated subgroup of a torsion group is finite. Since the group of degree zero divisors $\mathrm{Pic}^0(C)$ (over any finite field) is a torsion group and its subgroup of divisors with support in a finite set of points $Q \subset C(k)$ is finitely generated, the claim follows. □

LEMMA 2.3. — *Let K/k be the function field of a surface, C/k a smooth curve on a model of K and $Q = \{q_0, ..., q_s\} \subset C(k)$ a finite set of points. Then there exist a model X of K, irreducible divisors D_j, H_j, H'_j on X (with $j = 0, ..., s$) and a positive integer $n = n_Q$ such that:*
  (1) X *is smooth and contains C;*

(2) $D_j \cap C = q_j$ *for all* $j = 1, ..., s$;

(3) $n(D_j - D_0)$ *restricted to* C *is a principal divisor;*

(4) $n(D_j - D_0) + (H_j - H'_j)$ *is a principal divisor on* X;

(5) *the divisors* D_j *are pairwise disjoint;*

(6) *all intersections between* D_j, H_i *and* H'_i *are transversal, pairwise distinct and outside* C;

(7) H_j, H'_j *don't intersect* C.

Proof. — On a model X containing C as a smooth curve choose any divisors $D_j \subset X$ passing (transversally) through q_j (for all $j = 0, ..., s$). Blowing up points in $C(k) \setminus Q$ we can insure that the (strict transform of) C becomes contractible and that the image of the surface under a contracting morphism is *projective*. Blowing up again (if necessary) and removing components of exceptional divisors, we can insure that the (strict transforms) $D_j \cap C = q_j$ (for all j). By Lemma 2.2, there exists an $n = n_Q$ such that the restriction of $n(D_j - D_0)$ to C is a principal divisor. We continue to blow up (outside Q) so that each $n(D_j - D_0)$ becomes a trivial line bundle on some affine neighborhood of C in some model X. Throughout, C remains contractible and we write

$$\pi : X \to Y$$

for the corresponding blow-down. Now $n(D_j - D_0)$ is induced from a line bundle on Y (which is projective). In particular, there exist *ample* classes $[H_j], [H'_j] \in \mathrm{Pic}(Y)$ such that

$$[n(D_j - D_0)] + ([H_j] - [H'_j])$$

is a principal divisor on X (here we identified $[H_j], [H'_j]$ with their full transforms in X). Finally, we can choose representatives $H_j, H'_j \subset Y$ of these classes which are disjoint from $\pi(C)$, irreducible and satisfy all required transversality assumptions.   □

LEMMA 2.4. — *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 2.5. — *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 2.6. — 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 2.7. — *For any subfield $E \subset K$ there is a canonical sequence*

$$X \xrightarrow{\pi_E} Y' \xrightarrow{\rho_E} Y,$$

where

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

For generating $x \in K$ we write

$$\pi_x : X \to Y$$

for the morphism from Lemma 2.7, with $k(Y) = k(x)$. For $y \in K \setminus k(x)$ we 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 the projection π_y.

PROPOSITION 2.8. — *Let X/k be a smooth surface. Then*

(1) *if X contains finitely many rational curves then the same holds for every model X' of K;*
(2) *if $\mathrm{Pic}(X) = \mathrm{NS}(X)$ then for every 1-dimensional subfield $E \subset K = k(X)$ such that $E = \overline{E}^K$ one has $E = k(x)$ for some $x \in K$;*
(3) *for every curve $C \subset X$ and every finite set of irreducible divisors $D_1, ..., D_s$ of X not containing C, there exists a blowup*

$$\pi : \tilde{X} \to X$$

such that every branch in the strict transform $\pi^{-1}(C)$ intersects at most one irreducible component of the full transform of $\cup_{j=1}^s D_j$ and these intersections are transversal.

Proof. — Property (1) is evident. Property (2) follows from the fact that every such 1-dimensional field corresponds to a dominant map $X \to C$ onto a curve. If $\mathrm{Pic}(X) = \mathrm{NS}(X)$ then $\mathrm{Pic}^0(X) = 0$ and X admits no such maps onto curves of genus ≥ 1. The last property follows from resolution of singularities for surfaces. ☐

LEMMA 2.9. — *Assume that* $\mathrm{Pic}(X) = \mathrm{NS}(X)$ *and let* $x, y \in k(X) \setminus k$ *be such that*

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

Then y *is generating:* $k(y) = \overline{k(y)}^K$.

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

PROPOSITION 2.10. — *Let* X/k *be an algebraic variety of dimension* ≥ 2 *such that* $\mathrm{Pic}(X) = \mathrm{NS}(X)$. *If* $t \in K = k(X)$ *is not generating then there exist* $y, y' \in K$ *such that for all* $\kappa_1, \kappa_2, \kappa_1', \kappa_2' \in k^*$ *the elements*

$$(2.1) \qquad y, y/(t + \kappa_1), (y + \kappa_2)/t \text{ and } y', y'/(t + \kappa_1'), (y' + \kappa_2')$$

are generating and the elements

$$(2.2) \qquad\qquad\qquad 1, y, y', t$$

are linearly independent over k.

Proof. — Write $E := \overline{k(t)}^K$. By Proposition 2.8 (2), there exists an $x \in K$ such that $E = k(x)$ (so that $t = t(x)$). We have a dominant morphism

$$\pi_x \,:\, X \to \mathbb{P}^1$$

with irreducible generic fiber. Choose two algebraically independent y and y' so that

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

and

$$1, y, y', t$$

are linearly independent (linear independence can be checked, for example, by restricting to a fiber of π_x). By Lemma 2.9, both y and y' are generating.

It suffices to observe that all elements in (2.1) have the same degree on the generic fiber of π_x. □

The next proposition is a characterization of multiplicative groups of subfields $\mathfrak{K} \subset K$. 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 2.11. — *Let X be an algebraic variety of dimension ≥ 2 such that every 1-dimensional subfield $E \subset K = k(X)$ has the form $E = k(x)$ for some $x \in K^*$. Let $\mathfrak{K}^* \subset K^*$ be a subset such that*

(1) *$\mathfrak{K}^*$ is closed under multiplication;*
(2) *for every $E = k(x) \subset K$ with $E = \overline{E}^K$ there exists an $r = r(x) \in \mathbb{N}$ such that*
$$\mathfrak{K}^* \cap E^* = (E^*)^r;$$
(3) *there exists a $y \in K \setminus k$ with $r(y) = 1$ such that y is not a power.*

Then $\mathfrak{K} := \mathfrak{K}^* \cup 0$ is a field 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 $x \in K^*$ is either in $\mathfrak{K}^*$ or some power of it 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 2.4).

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.

Now consider $x \in \mathfrak{K}^*$ with $r(x) > 1$. We claim that there exists a $\kappa \in k$ such that
$$z := \frac{x + y + \kappa}{y + \kappa - 1} \in \mathfrak{K} \text{ and } r(z) = 1.$$
This implies that
$$z - 1 = (x + 1)/(y + \kappa - 1) \in \mathfrak{K}^* \text{ and } x + 1 \in \mathfrak{K}^*,$$
(by multiplicativity).

To prove the claim, choose a model X of K and consider the morphisms
$$\begin{aligned} \pi_x : X &\to \mathbb{P}^1 = (x : 1) \\ \pi_y : X &\to \mathbb{P}^1 = (y : 1) \end{aligned}$$

(as in Lemma 2.7). 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.

Then

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

since $y + \kappa = -1$ on $y + \kappa - 1$ and x is nonconstant on these fibers (where div_0 is the divisor of zeroes). It follows that *both*

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

are not powers so that $r(t) = r(z) = 1$. 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 $z \in \mathfrak{K}$. $\square$

3. Projective structures

In this section we explain the connection between fields and axiomatic projective geometry. We follow closely the exposition in [6].

DEFINITION 3.1. — *Let S be a (nonempty) set and $\mathfrak{L} = \mathfrak{L}(S)$ a collection of subsets $\mathfrak{l} \subset S$ 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*

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

Such a pair $(S, \mathfrak{L})$ is called a projective structure *on S and the elements $\mathfrak{l} \in \mathfrak{L}$ are called* lines.

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 $s_1, \ldots, s_n$ define

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

(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 ≥ 2 is called a projective *subspace* of dimension $|S'| - 1$.

A projective structure $(S, \mathfrak{L})$ satisfies *Pappus' axiom* if for all 2-dimensional subspaces and every configuration of six points and lines in these subspaces as below
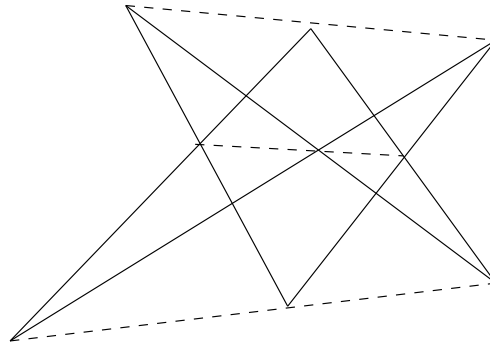
the intersections are collinear. The main theorem of abstract projective geometry is:

THEOREM 3.2. — *Let $(S, \mathfrak{L})$ be a projective structure of dimension $n \geq 2$ which satisfies Pappus' axiom. Then there exists a field k such that $S = \mathbb{P}_k^n$. This field is unique, up to isomorphism.*

Proof. — See [6], Chapter 6.   □

DEFINITION 3.3. — *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 3.4. — 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 natural projective structure: the set of lines is the set of usual projective lines $\mathbb{P}_k^1 \subset \mathbb{P}_k^n$. Every (not necessarily finite) extension of fields K/k induces a morphism of projective structures: $\mathbb{P}_k^n \to \mathbb{P}_K^n$.

DEFINITION 3.5. — *Let S be an abelian group. A projective structure* $(S, \mathfrak{L})$ *on S will be called* compatible *with the group structure if for all $s \in S$ and $\mathfrak{l} \in \mathfrak{L}$ one has*

$$s \cdot \mathfrak{l} \in \mathfrak{L}(S).$$

EXAMPLE 3.6. — Let K/k be a field extension (not necessarily finite). Then

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

carries a natural projective structure which is compatible with multiplication in the abelian group K^*/k^*.

THEOREM 3.7. — *Let K/k and K'/k' be field extensions of degree ≥ 4 and*

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

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

$$k \simeq k' \ \ and \ \ K \simeq K'.$$

Proof. — Choose a plane $\mathbb{P}^2 \subset S$ containing the identity $e \in S$, and two lines $\mathfrak{l}_1, \mathfrak{l}_2$ in this plane passing through e. The set of all points $\mathbb{P}^2 \setminus \{\mathfrak{l}_1, \mathfrak{l}_2\}$ is a principal homogeneous space under the group of projective automorphisms of $\mathbb{P}_k^1$ ($= \mathfrak{l}_1$) stabilizing one point (the intersection $\mathfrak{l}_1 \cap \mathfrak{l}_2$). A choice of an additional point $s \in \mathfrak{P}$ outside $\mathfrak{l}_1 \cup \mathfrak{l}_2$ trivializes this homogeneous space to the group of affine transformations of an affine line over k. In particular, it determines both the additive and the multiplicative structure on k. This implies that k is isomorphic to k' and that for every finite-dimensional space $V \subset K$ there exists a unique k'-linear space $V' \subset K'$ such that the map

$\bar{\phi}_V \ : \ \mathbb{P}_k(V) \to \mathbb{P}_{k'}(V')$ lifts to a (k, k')-linear map $\phi_V \ : \ V \to V'$. Such a lift is unique modulo multiplication by a nonzero scalar in k on the left (resp. k' on the right). We can identify V with $\mathbb{P}(V) \times k^* \cup \{0\}$ (as a set). If V is such that $e \in \mathbb{P}(V)$ then there is a unique lift ϕ_V with the property $\bar{\phi}_V(e) = e' \in S'$.

Let $x, y \in K \setminus k$ be any elements projecting to $\bar{x}, \bar{y} \in \mathbb{P}_k(K)$ and $V \subset K$ a k-vector subspace containing

$$1, x, y, xy.$$

Fix $\phi = \phi_V$ as above. Since $\bar{\phi}$ is an isomorphism of abelian groups there is a $c(x, y) \in k^*$ such that

$$\phi(x \cdot y) = \phi(x)\phi(y)c(x, y).$$

We need to show that $c(x, y) = 1$. For any $a \in k^*$ we have

$$\phi((a + x) \cdot y) = \phi(a \cdot y + c(x, y) \cdot x \cdot y) = a' \cdot y' + c'(x, y) \cdot x' \cdot y' \in V' \subset K',$$

by (k, k')-linearity of ϕ. Since $\bar{\phi}$ preserves products, the right side must be k'-proportional to

$$a' \cdot y' + x' \cdot y'.$$

On the other hand, y' and $x' \cdot y'$ are k'-linearly independent (since $x' \notin k'$). This implies that $c'(x', y') = 1$, as claimed. $\qquad\square$

DEFINITION 3.8. — *A partial projective structure is a pair* $(S, \mathfrak{P})$*, where* $\mathfrak{P}$ *is a set of subsets of* S *(lines) such that for every triple of pairwise distinct elements* $r, s, t \in S$ *there exist distinct elements*

$$x, y, x', y' \in S$$

(pairwise distinct from r, s, t*) and lines*

$$\mathfrak{l}(y, r), \mathfrak{l}(y, s), \mathfrak{l}(t, x), \mathfrak{l}(y', r), \mathfrak{l}(y', s), \mathfrak{l}(t, x'), \mathfrak{l}(y, y') \in \mathfrak{P}$$

with the property that

$$\begin{aligned}
&r, x, y \in \mathfrak{l}(y, r), r, x', y' \in \mathfrak{l}(y', r),\\
&y, s \in \mathfrak{l}(y, s), y', s \in \mathfrak{l}(y', s),\\
&t, x \in \mathfrak{l}(t, x), t, x' \in \mathfrak{l}(t, x'),\\
&\mathfrak{l}(t, x) \cap \mathfrak{l}(y, s) \neq \emptyset, \mathfrak{l}(t, x') \cap \mathfrak{l}(y', s) \neq \emptyset,\\
&\mathfrak{l}(y, y') \cap \mathfrak{l}(t, x) = \mathfrak{l}(y, y') \cap \mathfrak{l}(t, x') = \emptyset.
\end{aligned}$$
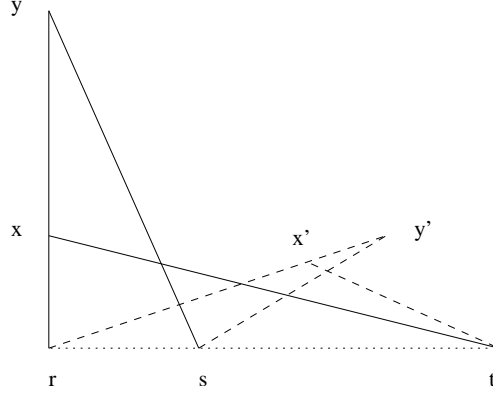
REMARK 3.9. — Of course, a projective structure on a projective space of dimension ≥ 3 is also a partial projective structure.

EXAMPLE 3.10. — Let K/k be the function field of an algebraic variety X of dimension ≥ 2. We have seen in Example 3.6 that $S := \mathbb{P}_k(K)$ carries a projective structure compatible with multiplication. Let $\mathfrak{P}$ be the set of all lines passing through 1 and a generating element of K (see Definition 2.5) and all their translates by elements in S (under multiplication). Proposition 2.10 implies that $(S, \mathfrak{P})$ is a partial projective structure. Indeed, (after translation) we can assume that $r = 1, s = t + \kappa$ etc. The lines in $\mathfrak{P}$ containing 1 will be called *primary*.

PROPOSITION 3.11. — *Let $(S, \mathfrak{L})$ and $(S, \mathfrak{L}')$ be two projective structures on S of dimension ≥ 3 and assume that the intersection $\mathfrak{L} \cap \mathfrak{L}'$ contains a subset $\mathfrak{P}$ such that $(S, \mathfrak{P})$ is a partial projective structure on S. Then $\mathfrak{L} = \mathfrak{L}'$.*

Proof. — For any tuple of points (r, s) we need to show that the line $\mathfrak{l}(r, s) \in \mathfrak{L}$ is also in $\mathfrak{L}'$ (and vice versa). Let t be any point distinct from r and s. There exist points x, y, x', y' as in Definition 3.8 together with corresponding lines in $\mathfrak{P}$. Moreover, $t \in \mathfrak{l}(r, s)$ iff t lies both in the plane spanned by $\mathfrak{l}(y, r)$ and $\mathfrak{l}(y, s)$ and in the plane spanned by $\mathfrak{l}(y', r)$ and $\mathfrak{l}(y', s)$ (which are distinct by the assumption that $\mathfrak{l}(y, y')$ intersects neither $\mathfrak{l}(t, x)$ not $\mathfrak{l}(t, x')$). These conditions are satisfied by the assumptions on the lines $\mathfrak{l}(t, x)$, resp. $\mathfrak{l}(t, x')$. Thus $t \in \mathfrak{l}(r, s)$ iff $t \in \mathfrak{l}'(r, s)$. $\qquad\square$

4. Flag maps

NOTATIONS 4.1. — We fix two prime numbers ℓ and $p \neq 2, \ell$. Let

- $\mathbb{F} = \mathbb{F}_p$ be the finite field with p elements;
- $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ its multiplicative group;
- A a vector space over $\mathbb{F}$ of dimension $\dim(A) \in \mathbb{N} \cup \infty$;
- $\mathbb{P}(A) = (A \setminus 0)/\mathbb{F}^*$ its projectivization;
- $\mathcal{M}(A, S)$ the set of maps from A to a set S;
- for $\mu \in \mathcal{M}(A, S)$ and $B \subset A$, μ_B the restriction of μ to B.

DEFINITION 4.2. — *A (complete)* flag *on a finite-dimensional A is a collection of subspaces $(A_n)_{n=0,..,\dim(A)}$ such that*

- *$A_0 = A$;*
- *$A_n \supsetneq A_{n+1}$ for all $n = 0, ..., \dim(A) - 1$.*

In particular, $A_n \setminus A_{n+1} \neq \emptyset$, for all n, and $A_{\dim(A)} = \{0\}$.

DEFINITION 4.3. — *A map $\mu \in \mathcal{M}(A, S)$ will be called homogeneous if for all $a \in A$ and all $\kappa \in \mathbb{F}^*$ one has*

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

We think of homogeneous maps as being defined on the projectivization $\mathbb{P}(A)$ and write $\mathcal{M}(\mathbb{P}(A), S)$ for the space of such maps.

DEFINITION 4.4. — *A map $\mu \in \mathcal{M}(A, S)$ will be called a* flag map *if*

- *μ is homogeneous;*
- *every finite-dimensional $\mathbb{F}$-vector space $B \subset A$ has a complete flag $(B_n)_{n=0,...,\dim(B)}$ such that μ is constant on $B_n \setminus B_{n+1}$, for all $n = 0, ..., \dim(B) - 1$.*

The set of flag maps will be denoted by $\mathcal{F}(A, S)$ or $\mathcal{F}(\mathbb{P}(A), S)$.

REMARK 4.5. — The flag property does not depend on the value of μ in $0 \in A$. Thus we will generally work on $A \setminus 0$ and $\mathbb{P}(A)$.

DEFINITION 4.6. — *Let S be a ring and A an $\mathbb{F}$-algebra. A map $\mu \in \mathcal{M}(\mathbb{P}(A), S)$ will be called logarithmic if*

$$\mu(a \cdot a') = \mu(a) + \mu(a'),$$

for all $a, a' \in A \setminus 0$. The set of such maps will be denoted by $\mathcal{L}(\mathbb{P}(A), S)$.

REMARK 4.7. — In our applications, A and S are endowed with topologies. We will always consider *continuous* maps, so that the notations $\mathcal{M}, \mathcal{F}, \mathcal{L}$ etc. stand for spaces of continuous maps, subject to the above properties.

DEFINITION 4.8. — *Let S be a ring. Two maps $\mu, \mu' \in \mathcal{M}(\mathbb{P}(A), S)$ will be called a c-pair (commuting pair) if*

- *$\mu, \mu' \in \mathcal{L}(\mathbb{P}(A), S)$;*
- *for all two-dimensional $\mathbb{F}$-subspaces $B \subset A$ there exist constants s, s', s'' (depending on B) with $(s, s') \neq (0, 0)$ such that for all $b \in B$ one has*

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

THEOREM 4.9. — *Let A be an $\mathbb{F}$-algebra and $\mu, \mu' \in \mathcal{L}(\mathbb{P}(A), \mathbb{Z}_\ell)$ non-proportional maps forming a c-pair. Then there exist constants $c, c' \in \mathbb{Z}_\ell$, $(c, c') \neq (0, 0)$ such that $c\mu + c'\mu' \in \mathcal{F}(\mathbb{P}(A), \mathbb{Z}_\ell)$.*

Proof. — This is a special case of the main theorem of [3]. We outline its proof, since the result is crucial for our applications.

Step 1. (Lemma 3.1.2 in [3]) $\mu \in \mathcal{F}(\mathbb{P}(A), S)$ iff for all $h : S \to \mathbb{Z}/2\mathbb{Z}$ one has $h \circ \mu \in \mathcal{F}(\mathbb{P}(A), \mathbb{Z}/2\mathbb{Z})$.

Step 2. (Lemma 3.2.1 and Proposition 2.6.1 in [3]) $\mu \in \mathcal{F}(\mathbb{P}(A), S)$ iff for all $B \subset A$ with $\dim(B) \leq 2$ the restriction $\mu_B \in \mathcal{F}(\mathbb{P}(B), S)$.

Step 3. (Proposition 4.3.1 in [3]) Assume that $\dim(A) \geq 3$ and that $\mu', \mu'' \in \mathcal{L}(\mathbb{P}(A), \mathbb{Z}_\ell)$ is a c-pair such that $\langle \mu', \mu'' \rangle_{\mathbb{Z}_\ell}$ does not contain an $\mathcal{F}$-map. Then there is a $B \subset A$ with $\dim(B) = 3$ such that there exist no (nonzero) $\mathcal{F}$-maps $\mu_B \in \langle \mu'_B, \mu''_B \rangle_{\mathbb{Z}_\ell}$.

Step 4. (Lemma 4.3.2 in [3]) Let $B = \mathbb{F}^3$ and $\mu', \mu'' \in \mathcal{M}(\mathbb{P}(B), \mathbb{Z}_\ell)$ be a c-pair. Then the map

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

has the following property: the image of every $\mathbb{P}^1 \subset \mathbb{P}(B)$ is contained in an affine line in $\mathbb{A}^2(\mathbb{Z}_\ell)$. By affine geometry constructions in Section 4.1 of [3], the image $\varphi(\mathbb{P}(B))$ is contained in a union of an affine line and (possibly) one more point. Using this, and assuming that there are no nonzero $\mathcal{F}$-maps $\mu \in$

$\langle \mu', \mu'' \rangle_{\mathbb{Z}_\ell}$, we conclude that there exist nonconstant (and nonproportional) maps $\phi', \phi'' \in \langle \mu', \mu'', 1 \rangle_{\mathbb{Z}_\ell}$ and an $h : \mathbb{Z}_\ell \to \mathbb{Z}/2\mathbb{Z}$ such that *neither* of the three maps

$$h \circ \phi',$$
$$h \circ \phi'',$$
$$h \circ \phi' + h \circ \phi''$$

is an $\mathcal{F}$-map on B (with values in $\mathbb{Z}/2\mathbb{Z}$).

Step 5. Rename the three maps to $\mu', \mu'', \mu' + \mu'' \in \mathcal{M}(\mathbb{P}(B), \mathbb{Z}/2\mathbb{Z})$. The image $\varphi(\mathbb{P}(B))$ is contained in 3 points $((0,0), (0,1)$ and $(1,0))$. Consequently, $\mathbb{P}(B)$ contains lines of (at most) three types $((00), (01), (10))$. We may assume that there are at least two lines of each type and each line contains at least two points of each type (otherwise, it is easy to find an $\mathcal{F}$-map among $\mu', \mu'', \mu' + \mu''$, leading to a contradiction). We may also assume that μ', resp. $\mu'', \mu' + \mu''$, is constant on lines of type (00), resp. (01), (10). The projective geometry constructions in Section 4.2 of [3] show that one of the three maps has the following property: on every line $\mathbb{P}(C) \subset \mathbb{P}(B)$ (where it is nonconstant) it satisfies the functional equation of Step 6.

Step 6. (Lemma 2.5.6 in [3]) Let $C = \mathbb{F}^2$ and $\mu \in \mathcal{M}(\mathbb{P}(C), \mathbb{Z}/2\mathbb{Z})$ be such that C has a basis (c, b) with $\mu(c) = \mu(c + \kappa b) \neq \mu(b)$, for all $\kappa \in \mathbb{F}$. Then $\mu \in \mathcal{F}(\mathbb{P}(C), \mathbb{Z}/2\mathbb{Z})$.

Indeed, since μ is homogeneous, the functional equation implies that

$$\mu(\kappa c + \kappa' b) = \mu(c)$$

for all $\kappa, \kappa' \in \mathbb{F}^*$. Thus μ is constant on $C \setminus \mathbb{F}b$.

Thus at least one of the maps $\mu', \mu'', \mu' + \mu''$ is an $\mathcal{F}$-map on *all* lines in $\mathbb{P}(B)$, hence an $\mathcal{F}$-map on the whole $\mathbb{P}(B)$, contradiction to Step 4. $\qquad\square$

5. Galois groups

Let k be an algebraic closure of $\mathbb{F}$, $K = k(X)$ the function field of an algebraic variety X over k, $\mathcal{G}_K^a$ the abelianization of the pro-ℓ-quotient $\mathcal{G}_K$ of the Galois group 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. By our assumptions, $\mathcal{G}_K^a$ is a torsion free $\mathbb{Z}_\ell$-module.

DEFINITION 5.1. — *We say that $h, h' \in \mathcal{G}_K^a$ form a* commuting pair *if for some (and therefore any) of their preimages $\tilde{h}, \tilde{h}'$ one has $[\tilde{h}, \tilde{h}'] = 0$. A subgroup $\mathcal{H}$ of $\mathcal{G}^a$ is called* liftable *if any two elements in $\mathcal{H}$ form a commuting pair.*

DEFINITION 5.2. — *A fan $\Sigma_K = \{\sigma\}$ on $\mathcal{G}_K^a$ is the set of all those 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 5.3. — Even though the group $\mathcal{G}_K^c$ depends on the choice of a separable closure of K, the fan Σ_K does not.

REMARK 5.4. — For function fields E/k of curves there are no topologically noncyclic liftable subgroups of $\mathcal{G}_E^a$ and $\Sigma_E = \emptyset$. For function fields K/k of surfaces all groups $\sigma \in \Sigma_K$ are isomorphic to (torsion free) $\mathbb{Z}_\ell$-modules of rank 2 (see Section 8).

NOTATIONS 5.5. — Let

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

and

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

be the Tate twist of $\mathbb{Z}_\ell$. Write

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

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

THEOREM 5.6 (Kummer theory). — *For every $n \in \mathbb{N}$ we have a pairing*

$$\begin{array}{rcl} \mathcal{G}_K^a/\ell^n \times K^*/(K^*)^{\ell^n} & \to & \boldsymbol{\mu}_{\ell^n} \\ (\mu, f) & \mapsto & [\mu, f]_n := \mu(f)/f \end{array}$$

which extends to a nondegenerate pairing

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

REMARK 5.7. — Since k is algebraically closed and $\ell \neq p$ we can choose a noncanonical isomorphism

$$\mathbb{Z}_\ell \simeq \mathbb{Z}_\ell(1).$$

From now on we will fix such a choice.

6. Valuations

In this section we recall basic facts concerning valuations and valued fields (we follow [4]).

NOTATIONS 6.1. — A *value group* is a totally ordered (torsion free) abelian group. We will denote by Γ a value group, use the additive notation $''+''$ for the group law and $\geq$ for the order. We have

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

We put $\Gamma_\infty = \Gamma \cup \{\infty\}$ and make it to a totally ordered group through the conventions

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

EXAMPLE 6.2. — A standard value group is $\mathbb{Z}^n$ with the *lexicographic* ordering.

DEFINITION 6.3. — *A (nonarchimedean) valuation $\nu = (\nu, \Gamma_\nu)$ on a field K is a pair consisting of a totally ordered abelian group Γ_ν (the value group) and a map*

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

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 6.4. — 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 $\Gamma = \{0\}$. In our applications, $K = k(X)$, where k is an algebraic closure of the finite field $\mathbb{F}$ and X is an algebraic variety over k (a *model* for K). Since every element in k is torsion, every valuation of K restricts to a trivial valuation on k.

NOTATIONS 6.5. — 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:

(6.1) $$1 \to \mathfrak{o}_\nu^* \to K^* \to \Gamma_\nu \to 1$$

and

(6.2) $$1 \to (1 + \mathfrak{m}_\nu) \to \mathfrak{o}_\nu^* \to \boldsymbol{K}_\nu^* \to 1.$$

NOTATIONS 6.6. — We denote by $\mathcal{I}_\nu^a \subset \mathcal{D}_\nu^a \subset \mathcal{G}_K^a$ the images of the inertia and the decomposition group of the valuation ν in $\mathcal{G}_K^a$. There is a (canonical) isomorphism

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

DEFINITION 6.7. — *Let K be the function field of an algebraic variety over k. A valuation ν of K is* positive-dimensional *if its residue field $\boldsymbol{K}_\nu$ is the function field of an algebraic variety of dimension ≥ 1. It is* divisorial *if*

$$\operatorname{tr deg}_k \boldsymbol{K}_\nu = \dim(X) - 1.$$

NOTATIONS 6.8. — We let $\mathcal{V}_K$ be the set of all nontrivial (nonarchimedean) valuations of K and $\mathcal{DV}_K$ the subset of its divisorial valuations. If $\nu \in \mathcal{DV}_K$ is realized by a divisor on a model X of K (see Example 6.10) we sometimes write $\mathcal{I}_D^a$, resp. $\mathcal{D}_D^a$, for the corresponding inertia, resp. decomposition group.

EXAMPLE 6.9. — Let C be a smooth curve over k and $E = k(C)$. Every point $q \in C$ 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 6.10. — Let X be a smooth surface over k and $K = k(X)$.

– Every curve $C \subset X$ defines a valuation ν_C on K with value group $\mathbb{Z}$. Conversely, every valuation ν on K with value group isomorphic to $\mathbb{Z}$ defines a curve on *some* model X' of K.

– Every flag (C, q), (curve, point on this curve), defines a valuation $\nu_{C,q}$ on K with value group $\mathbb{Z}^2$.
– There exist (analytic) valuations on K with value group a subgroup of $\mathbb{Z}^2$ and center supported in a point (on every model).

REMARK 6.11. — Every (nontrivial) positive-dimensional valuation on the function field of a surface X/k is divisorial.

DEFINITION 6.12. — *We say that two valuations (ν_1, Γ_1) and (ν_2, Γ_2) are* compatible *if there exists a valuation (ν, Γ) and two surjective order-preserving homomorphisms of value groups* $\mathrm{pr}_j : \Gamma \to \Gamma_j$ *($j = 1, 2$) such that for all* $\kappa \in K^*$

$$\nu_j(\kappa) = \mathrm{pr}_j(\nu(\kappa)).$$

Two valuations (ν_1, Γ_1) and (ν_2, Γ_2) are equivalent *if there exists an order preserving isomorphism of value groups $\Gamma_1 \to \Gamma_2$ commuting with the homomorphisms ν_1, ν_2.*

We will not distinguish equivalent valuations.

LEMMA 6.13. — *Let K be any field and ν', ν'' two valuations on K. Then either*

– *ν' and ν'' are compatible and there exists a valuation ν with maximal ideal $\mathfrak{m}_\nu = \mathfrak{m}_{\nu'} + \mathfrak{m}_{\nu''}$ or*
– *ν', ν'' are incompatible,*

$$K = \mathfrak{m}_{\nu'} + \mathfrak{m}_{\nu''} \text{ and } K^* = (1 + \mathfrak{m}_{\nu'}) \cdot \mathfrak{o}_{\nu''}^*.$$

Proof. — See [9]. □

7. A dictionary

Write

$$\begin{aligned}
\mathcal{L}_K &:= \mathcal{L}(\mathbb{P}(K), \mathbb{Z}_\ell(1)), \\
\mathcal{F}_K &:= \mathcal{F}(\mathbb{P}(K), \mathbb{Z}_\ell(1)).
\end{aligned}$$

PROPOSITION 7.1. — *One has the following identifications:*

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

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 4.8).

Proof. — The first identification is a consequence of Kummer theory 5.6. For the second and third identification we use the sequences (6.1) and (6.2). 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. $\qquad \square$

EXAMPLE 7.2. — If $\mu \in \mathcal{D}_\nu^a$ and $\alpha \in \mathcal{I}_\nu^a$ then μ and α form a commuting pair.

PROPOSITION 7.3. — *Let K be a field and $\alpha \in \mathcal{F}_K \cap \mathcal{L}_K$. Then there exists a unique valuation $\nu = (\nu_\alpha, \Gamma_{\nu_\alpha})$ (up to equivalence) and a homomorphism $\mathrm{pr} : \Gamma_{\nu_\alpha} \to \mathbb{Z}_\ell$ 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 7.1).

Proof. — Assume that $\alpha(f) \neq \alpha(f)$ for some $f, f' \in K$ and consider the projective 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 (6.1), $\alpha \in \mathcal{I}_\nu^a$. $\qquad \square$

COROLLARY 7.4. — *Every (topologically) noncyclic liftable subgroup of $\mathcal{G}_K^a$ contains an inertia element of some valuation.*

Proof. — By Theorem 4.9, every such liftable subgroup contains an $\mathcal{F}$-map, which by Proposition 7.3 belongs to some inertia group. $\square$

8. Flag maps and valuations

LEMMA 8.1. — *Let* $\alpha \in \mathcal{F}_K \cap \mathcal{L}_K$, $\nu = \nu_\alpha$ *the associated valuation and* $\mu \in \mathcal{L}_K$. *Assume that* α, μ *form a c-pair. Then*

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

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

Proof. — 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 κ and m as above;
(3) $\mathfrak{m}_\nu$ is 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 $\mu(1 + m) = \mu(1)$.

If $\alpha(m) = 0$ then there exists $m', m'' \in \mathfrak{m}_\nu$ such that $m = m' + m''$ and $\alpha(m') = \alpha(m'') \neq 0$. Indeed, there exists an $m' \in \mathfrak{m}_\nu$ such that $m > m' > 1$ and $\alpha(m') \neq \alpha(1) = 0$. Since α takes only two values on the subgroup $\langle m', m \rangle \subset \mathfrak{m}_\nu$ we have

$$\alpha(m'') = \alpha(-m' + m) = \alpha(m').$$

Therefore,

$$0 = \mu(1 + m') + \mu(1 + m'') = \mu(1 + m + m'm'').$$

Put $\kappa = 1 + m + m'm''$ and observe that $\alpha(-m'm'') = -2\alpha(m') \neq 0$. By the argument above

$$\mu(\kappa - m'm'') = \mu(\kappa) = \mu(1 + m' + m'') = \mu(1 + m),$$

as claimed. $\square$

LEMMA 8.2. — *Assume that* $\alpha, \alpha' \in \mathcal{G}_K^a \cap \mathcal{F}_K$ *form a c-pair. Then the associated valuations* ν *and* ν' *are compatible.*

Proof. — If ν and ν' are incompatible then, by Lemma 6.13,

$$K^* = \mathfrak{o}_\nu^* \cdot (1 + \mathfrak{m}_{\mu'}).$$

By Lemma 8.1,

$$\alpha(1 + \mathfrak{m}_{\nu'}) = 0 \ \text{ and } \ \alpha(\mathfrak{o}_\nu^*) = 0.$$

This implies that α, and similarly, α' vanish on K^*.   □

COROLLARY 8.3. — *Let K/k be the function field of a surface. Then for every $\sigma \in \Sigma_K$ one has*

$$\mathrm{rk}_{\mathbb{Z}_\ell} \sigma = 2.$$

Proof. — Otherwise, by Lemma 8.1, we would get a topologically noncyclic liftable subgroup in $\mathcal{G}_{\boldsymbol{K}_\nu}^a$ (for some $\nu \in \mathcal{V}_K$). Since $\boldsymbol{K}_\nu$ is either k or the function field of some curve, we get a contradiction.   □

PROPOSITION 8.4. — *Let $K = k(X)$ be the function field of a surface and $\sigma, \sigma' \in \Sigma_K$ be two distinct maximal liftable (topologically noncyclic) subgroups of $\mathcal{G}_K^a$ such that $\sigma \cap \sigma' \neq 0$. Then there exists a unique divisorial valuation ν of K such that*

- *$\sigma \cap \sigma' = \mathcal{I}_\nu^a$;*
- *both σ and σ' are contained in $\mathcal{D}_\nu^a$.*

Moreover, for every divisorial valuation ν of K there exist $\sigma, \sigma' \in \Sigma_K$ as above.

Proof. — First of all, every $\alpha \in \sigma \cap \sigma'$ is an $\mathcal{F}$-map and therefore an inertial element for some valuation ν. It commutes only with the associated $\mathcal{D}_\nu^a$. Since in our case every (nontrivial) valuation ν is geometric, its center $\mathfrak{c}(\nu)$ is a subvariety on some model X of K. If $\mathfrak{c}(\nu)$ is a point then the rank of $\mathcal{D}_\nu^a$ is at most 2. However, $\sigma \cup \sigma \subset \mathcal{D}_\nu^a$ and has rank 3, contradiction. Hence $\dim(\mathfrak{c}(\nu)) = 1$ and ν is divisorial.   □

9. Galois groups of curves

Throughout this section E/k is a 1-dimensional field and C a smooth curve of genus g with $k(C) = E$. 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

$$(9.1) \qquad 0 \to \mathbb{Z}_\ell(\Delta) \to \mathcal{M}(C(k), \mathbb{Z}_\ell) \to \mathcal{G}_E^a \to \mathbb{Z}_\ell^{2\mathbf{g}} \to 0,$$

with the identifications

- $\mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}_\ell) = \mathbb{Z}_\ell$ (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 $C(k) \to \mathbb{Z}_\ell$;
- $\mathbb{Z}_\ell^{2\mathbf{g}} = \mathrm{Ext}^1(\mathrm{Pic}^0(C), \mathbb{Z}_\ell)$.

Using this model and the results in Section 5, we can interpret

$$(9.2) \qquad\qquad \mathcal{G}_E^a \subset \mathcal{M}(C(k), \mathbb{Q}_\ell)/\text{constant maps}$$

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

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

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

$$(9.3) \qquad \begin{array}{rcl} \mathcal{M}(C(k), \mathbb{Q}_\ell) \times E^*/k^* & \to & \mathbb{Q}_\ell \\ (\mu, f) & \mapsto & [\mu, f] := \sum_q \mu(q) f_q, \end{array}$$

where $\mathrm{div}(f) = \sum_q f_q q$. In detail, let $\gamma \in \mathcal{G}_E^a$ be an element of the Galois group. By Kummer theory, γ is a homomorphism $K^*/k^* \to \mathbb{Z}_\ell = \mathbb{Z}_\ell(1)$. 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. 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 $\mathcal{I}_w^a \subset \mathcal{G}_E^a$ corresponds to a "delta"-map (constant outside the point q_w). Each $\mathcal{I}_w^a$ 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 (9.1) is then given by

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

DEFINITION 9.1. — *We say that the support of a subgroup $\mathcal{I} \subset \mathcal{G}_E^a$ is $\leq s$ and write*

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

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

$$\mathcal{I} \subset \langle \mathcal{I}_{w_1}^a, ..., \mathcal{I}_{w_s}^a \rangle_{\mathbb{Z}_\ell} \subset \mathcal{G}_E^a.$$

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

LEMMA 9.2. — *Let $\mathcal{I} \subset \mathcal{G}_E^a$ be a topologically cyclic subgroup such that $|\mathrm{supp}(\mathcal{I})| > s \geq 2$. Then there exist a finite set $\{f_j\}_{j \in J} \subset E^*$ and an $m \in \mathbb{N}$ such that the map*

$$\begin{array}{rcl} \psi : \ \mathcal{G}_E^a & \to & V := \oplus_{j \in J} \mathbb{Z}/\ell^m \\ \mu & \mapsto & ([\mu, f_j]_m)_{j \in J} \end{array}$$

has the following property: for every set $\{w_1, ..., w_s\} \subset \mathcal{V}_E$

$$\psi(\mathcal{I}) \not\subset \langle \psi(\mathcal{I}_{w_1}^a), ..., \psi(\mathcal{I}_{w_s}^a) \rangle_{\mathbb{Z}_\ell}.$$

Proof. — Let $\iota \in \mathcal{G}_E^a \subset \mathcal{M}(C(k), \mathbb{Q}_\ell)$ be a *representative*, as in (9.2), of a topological generator of $\mathcal{I}$, where $\mathrm{supp}(\mathcal{I}) > s$. There are three possibilities:

(1) $\iota(C(k)) \subset \mathbb{Q}_\ell$ is infinite;
(2) there is a $b \in \iota(C(k)) \subset \mathbb{Q}_\ell$ such that $\iota^{-1}(b)$ is infinite *and* there exist at least $s + 1$ distinct points $q_{s+2}, \ldots, q_{2s+2} \in C(k)$ such that $\iota(q_j) \neq b$ for all $j = s + 2, \ldots, 2s + 2$;
(3) otherwise: $\iota(C(k))$ is finite, there is a b with $\iota^{-1}(b)$ infinite and there are at most s distinct points with values differing from b.

In Case (3), $|\mathrm{supp}(\mathcal{I})| \leq s$.

In Case (1), choose any set $Q = \{q_1, ..., q_{2s+2}\} \subset C(k)$ of points with pairwise distinct values. In Case (2) choose distinct $q_1, ..., q_{s+1} \in \iota^{-1}(b)$ and put $Q := \{q_1, ..., q_{2s+2}\}$. In both cases, if $Q' \subset Q$ is any subset of cardinality $|Q'| = s$ then ι is *nonconstant* on $Q \setminus Q'$. In particular, there exist points $q_{s_1}, q_{s_2} \in Q \setminus Q'$ such that

$$(9.4) \qquad\qquad \iota(q_{s_1}) \neq \iota(q_{s_2}).$$

We may assume that $\iota(Q) \subset \mathbb{Z}_\ell$ (replacing ι by a sufficiently high multiple, if necessary). Now we choose an $m'' \in \mathbb{N}$ such that all values of ι on Q remain pairwise distinct modulo $\mathbb{Z}/\ell^{m''}$. Let $\mathrm{Div}_Q^0(C)$ be the abelian group of degree zero divisors on C supported in Q. By Lemma 2.2, there is an $n = n_Q \in \mathbb{N}$ such that nD is principal for every $D \in \mathrm{Div}_Q^0(C)$. In particular, for every $q_{s_1}, q_{s_2} \in Q$ there is a function $f \in E^*$ such that $\mathrm{div}(f) = n(q_{s_1} - q_{s_2})$. Write $n = \ell^{m'} \bar{n}$, with $\gcd(\bar{n}, \ell) = 1$, and put $m = m' + m''$.

We have a pairing (Kummer theory)

$$\begin{aligned}
\mathcal{G}_E^a \times n\mathrm{Div}_Q^0(C) &\rightarrow \mathbb{Z}/\ell^m \\
(\mu, f) &\mapsto [\mu, f]_m.
\end{aligned}$$

Notice that $[\mathcal{I}_w^a, f] = 0$ for all w with $q_w \notin Q$ and all $f \in E^*$ supported in Q. Further, for every $Q' \subset Q$ with $|Q'| = s$ and points $q_{s_1}, q_{s_2} \in Q \setminus Q'$ as in (9.4) there is an $f \in E^*$ with divisor $\mathrm{div}(f) = n(q_{s_1} - q_{s_2})$ such that

$$[\iota, f] = n \cdot (\iota(q_{s_1}) - \iota(q_{s_2})) \neq 0 \mod \ell^m$$

and

$$[\mathcal{I}_{w'}^a, f] = 0$$

for all $\mathcal{I}_{w'}^a$ of $q' \in Q'$. Let $\{f_j\}_{j \in J}$ be a basis for $\ell^m \cdot \mathrm{Div}_Q^0(C)$, with $f_j \in E^*$. The map

$$\begin{aligned}
\psi : \mathcal{G}_E^a &\rightarrow \oplus_{j \in J} \mathbb{Z}/\ell^m \\
\mu &\mapsto ([\mu, f_j]_m)_{j \in J}
\end{aligned}$$

satisfies the required properties. $\qquad\square$

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

$$\mathcal{I}_w^a \subset \mathcal{D}_\nu^a / \mathcal{I}_\nu^a = \mathcal{G}_{k(C)}^a.$$

We have a projection

$$\pi_\nu : \mathcal{G}_K^a \rightarrow \mathcal{G}_K^a / \mathcal{I}_\nu^a$$

and an inclusion

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

PROPOSITION 9.3. — *Let ν be a divisorial valuation of K. A subgroup*

$$\mathcal{I} \subset \mathcal{D}_\nu^a / \mathcal{I}_\nu^a$$

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

$$\psi : \mathcal{G}_K^a / \mathcal{I}_\nu^a \rightarrow V$$

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

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

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

$$\mathcal{I} = \mathcal{I}_w^a \subset \mathcal{D}_\nu^a/\mathcal{I}_\nu^a$$

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

$$\psi \,:\, \mathcal{G}_K^a/\mathcal{I}_\nu^a \to V$$

a homomorphism onto a finite abelian group. Since $\mathcal{G}_K^a$ 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. Moreover, f_j are not simultaneously constant on C (otherwise, $\psi(\mathcal{G}_{k(C)}^a) = \psi(\mathcal{I}_{k(C)}^a)$). Changing the model $\tilde{X} \to X$, if necessary, 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

(see Section 2). Then the image of $\mathcal{I}_D^a$ under ψ is equal to the image of $\mathcal{I}_w^a$.

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

$$\psi \,:\, \mathcal{G}_K^a/\mathcal{I}_\nu^a \to V$$

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

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

We consider two cases

(1) there exist two points $q, q' \in C(k)$ such that $\mathcal{I} \subset \langle \mathcal{I}_w^a, \mathcal{I}_{w'}^a \rangle$;
(2) otherwise.

Case 1. There exists a rational map $\pi : X \to \mathbb{P}^1$ such that its restriction

$$\pi : C \to \mathbb{P}^1$$

is surjective, unramified at q, q' and $\pi(q) \neq \pi(q')$. Under the induced map of Galois groups

$$\pi_*(\mathcal{I}) \subset \langle \mathcal{I}^a_{\pi(w)}, \mathcal{I}^a_{\pi(w')} \rangle$$

but is not contained in either $\mathcal{I}^a_{\pi(q)}$ or $\mathcal{I}^a_{\pi(q')}$. Thus there exist a finite abelian group V and a map $\psi : \mathcal{G}^a_{k(\mathbb{P}^1)} \to V$ such that $\psi(\mathcal{I}) \notin \psi(\mathcal{I}^a_{w''})$ for any $q'' \in \mathbb{P}^1$. It follows that

$$\psi \circ \pi_*(\mathcal{I}) \notin \psi \circ \pi_*(\mathcal{I}^a_\nu)$$

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

Case 2. By Lemma 9.2, there exist a finite set of functions $\bar{f}_j \in k(C)$, with support in a finite set $Q = \{q_0, ..., q_s\} \subset C(k)$, and an $m \in \mathbb{N}$ such that the homomorphism

$$\begin{aligned} \bar{\psi} : \mathcal{G}^a_{k(C)} &\to V = \oplus_{j \in J} \mathbb{Z}/\ell^m \\ \mu &\mapsto ([\mu, \bar{f}_j]_m)_{j \in J} \end{aligned}$$

has the property that for all $w, w' \in \mathcal{DV}_{k(C)}$

$$\psi(\mathcal{I}) \notin \langle \psi(\mathcal{I}^a_w), \psi(\mathcal{I}^a_{w'}) \rangle_{\mathbb{Z}_\ell}.$$

Next we choose a model for X and C as in Lemma 2.3. In particular, there exist functions g_j with divisor

$$\mathrm{div}(g_j) = n \cdot (D_j - D_0) + (H_j - H'_j)$$

such that all the divisors are irreducible, with transversal intersections and $\mathrm{div}(g_j)|C = n(q_j - q_0)$. These functions g_j define a homomorphism

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

If D is a divisor on X then $\psi \circ \pi_\nu(\mathcal{I}^a_D) = 0$ unless $D = D_j$ for some j. In this case $\psi \circ \pi_\nu(\mathcal{I}^a_{D_j}) = \psi(\mathcal{I}^a_{w_j})$.

Let $\nu' \in \mathcal{DV}_K$ and $\mathfrak{c}(\nu') \subset X$ be its center on X. There are three cases:

- $\mathfrak{c}(\nu') \not\subset D_j$ for any j: then $\psi \circ \pi_\nu(\mathcal{I}^a_{\nu'}) = 0$;
- $\mathfrak{c}(\nu') \in D^0_j$, where $D^0_j = D_j \setminus (\cup_{j' \neq j} D_j \cap D_{j'})$: then

$$\psi \circ \pi_\nu(\mathcal{I}^a_{\nu'}) \subset \psi(\mathcal{I}^a_{w_j});$$

– $\mathfrak{c}(\nu') \in D_j \cap D_{j'}$ for some j, j': then

$$\psi \circ \pi_\nu(\mathcal{I}^a_{\nu'}) \subset \langle \psi(\mathcal{I}^a_{w_j}), \psi(\mathcal{I}^a_{w_{j'}})\rangle_{\mathbb{Z}_\ell}.$$

All three possibilities contradict our assumptions. $\qquad\square$

LEMMA 9.4. — *Let C/k be a curve and $E = k(C)$ its function field. Then* $\mathsf{g}(C) \geq 1$ *iff there exists a 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 (9.1)). $\qquad\square$

REMARK 9.5. — Combining this with Proposition 9.3 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*.

10. Valuations on surfaces

Let X be a smooth surface over k, $K = k(X)$ its function field and ν a divisorial valuation of K. We have a well-defined (bilinear, with respect to multiplication) residue map

$$(10.1) \qquad \begin{array}{ccc} K^* \times K^* & \to & \boldsymbol{K}_\nu/k^* \\ f, g & \mapsto & f^{\nu(g)}/g^{\nu(f)}. \end{array}$$

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

$$(10.2) \qquad \varrho_\nu = \varrho_D \,:\, K^* \times K^* \to \boldsymbol{K}_\nu/k^*$$

as follows:

 – $\varrho_\nu(f, g) = 0$ if both f, g are invertible on D;
 – $\varrho_\nu(f, g) = f^m_D$ 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.

LEMMA 10.1. — *For $f, g \in K^*$*

$$\varrho_\nu(f, g) = 0 \ \forall \nu \in \mathcal{DV}_K \iff f, g \in E = k(C) \subset K \text{ for some curve } C.$$

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, $\varrho_\nu(f, g) = 0$ if D is not in the fiber of π. If D is in the 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 $\varrho_\nu(f, g) = 0$.

($\Rightarrow$) Assume that $\varrho_\nu(f, g) = 0$ 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, $\nu_D(f) \neq 0$, while $\nu_D(g) = 0$ and g is nonconstant on D. Hence $\varrho_D(f, g) \neq 0$, contradiction. Therefore, all D_q are (multiples of) fibers of π_g and f is induced from C_g. Hence $C_f = C_g$ and $\pi_f = \pi_g$. $\square$

11. ℓ-adic analysis: generalities

Let $K = k(X)$ be the function field of a smooth algebraic variety X over k. We have an exact sequence

(11.1) $$0 \to K^*/k^* \xrightarrow{\rho_X} \mathrm{Div}(X) \xrightarrow{\varphi} \mathrm{Pic}(X) \to 0,$$

where $\mathrm{Div}(X)$ is the group of (Weil or Cartier) divisors of X. We will identify an element $f \in K^*/k^*$ with its image under ρ_X. 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 *rapidly decreasing coefficients*:

- M is a countable set;
- for all $r \in \mathbb{Z}$ the set

$$\{m \mid |\hat{a}_m|_\ell \le r\}$$

   is finite;
- for $D \in \widehat{\mathrm{Div}}_{\mathrm{nr}}(X)$, all D_m are nonrational.

Clearly, the group of *finite ℓ-adic divisors*

$$\mathrm{Div}(X)_\ell := \mathrm{Div}(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \subset \widehat{\mathrm{Div}}(X).$$

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

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

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

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

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

and a residue map

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

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

(10.1). We say that two elements $\hat{f}, \hat{g} \in \hat{K}^*$ commute if $\hat{\varrho}_\nu(\hat{f}, \hat{g}) = 0$, for all divisorial ν.

NOTATIONS 11.1. — We put

$$\begin{aligned} \operatorname{supp}_K(\hat{f}) &:= \{ \quad \nu \in \mathcal{DV}_K \quad | \quad \hat{f} \text{ nontrivial on } \mathcal{I}_\nu^a \}; \\ \operatorname{supp}_X(\hat{f}) &:= \{ \qquad D_m \qquad | \quad \hat{a}_m \neq 0 \}. \end{aligned}$$

DEFINITION 11.2. — *We say that $\hat{f}$ has* finite nonrational support *if the set of nonrational $\nu \in \operatorname{supp}_K(\hat{f})$ is finite (see Lemma 9.4 for the definition and Galois-theoretic characterization of nonrational valuations). Let*

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

be the set of such elements.

DEFINITION 11.3. — *We say that $\hat{f}$ has finite support on the model X if* $\operatorname{supp}_X(\hat{f})$ *is finite. Put*

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

LEMMA 11.4. — *The definition of $\mathcal{FS}_X(K)$ does not depend on the choice of a model X.*

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

COROLLARY 11.5. — *Let K be the function field of a surface X which contains only finitely many rational curves. Then*

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

In particular, we obtain an intrinsic, Galois-theoretic description of $\mathcal{FS}_X(K)$ in this case. We proceed to give such a description in general. 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 $\widehat{\operatorname{Div}}_{\mathrm{nr}}(X') = \widehat{\operatorname{Div}}_{\mathrm{nr}}(X)$. Under this identification

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

Let $\mathcal{F}(K)$ be the set of all $f \in K^*/k^*$ such that $\rho_{X,\mathrm{nr}}(f) \neq 0$ and for every rational divisorial valuation ν and some (equivalently, every) model X of K, where $\nu = \nu_C$ for a rational curve $C \subset X$, either

- $f_C = 1 \in k(C)^*/k^*$ or
- $\rho_C(f_C) \neq 0 \mod \ell$.

LEMMA 11.6. — *The set $\mathcal{F}(K)$ generates K^*/k^*. Moreover, for every pair of commuting elements $\hat{f}, \hat{g} \in \mathcal{FS}(K)$ with disjoint support such that there exist $f, g \in \mathcal{F}(K)$ with*

$$f = \hat{f} \mod (K^*)^\ell \quad and \quad g = \hat{g} \mod (K^*)^\ell,$$

one has $\hat{f} \in \mathcal{FS}_X(K)$ and $\hat{g} \in \mathcal{FS}_X(K)$, for every model X of K.

Proof. — Let $y \in K^*$ be a function such that the generic fiber of the corresponding map $\pi_y : X \to \mathbb{P}^1_y$, from some model X of K, is an irreducible nonrational curve. Such y generate K^*.

For generic quadratic, coprime polynomials $P, Q \in k[y]$, the preimage in X of $(0 \cup \infty) \subset \mathbb{P}^1$ under the composition of π_y with the map

$$\phi : \begin{array}{ccc} \mathbb{P}^1_y & \to & \mathbb{P}^1 \\ y & \mapsto & f(y) := P(y)/Q(y) \end{array}$$

contains at least 4 irreducible smooth fibers of π_y. If f were nonconstant on a rational curve C (on some model X of K) and f_C were an ℓ-th power then the local ramification indices of f and hence of y were divisible by ℓ. Thus we would have a map $\pi_y : C \to \mathbb{P}^1_y$ with all local ramification indices over 4 points divisible by ℓ, and by Hurwitz' theorem, $\mathrm{g}(C) > 0$, which contradicts the rationality of C. It follows that $f \in \mathcal{F}(K)$. Clearly, such elements f generate $k(y)^*$.

Next, write

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

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, $\rho_{\nu'_j}(\hat{f}, \hat{g}) = 0$, for all ν'_j corresponding to C'_j. Since C'_j are rational, this residue equals the residue of f on C'_j, which is nonzero $\mod \ell$,

contradiction. Thus, if $(\hat{f}, \hat{g}) = 0$, then $\mathrm{supp}_X(\hat{g})$ is finite and we may put $\hat{g} = g'$. The restriction of g' to any irreducible component of the divisor of $\hat{f}$ is identically zero. This implies that g' is a product of ℓ-adic powers of elements belonging to the same field $k(y)$ as f. Thus all rational curves in the support of $\hat{f}$ also belong to the fibers of y. There are finitely many such curves since some fibers contain nonrational curves. $\qquad\square$

We have an exact sequence

$$0 \to \hat{K}^* \xrightarrow{\hat{\rho}_X} \widehat{\mathrm{Div}}(X) \xrightarrow{\varphi_\ell} \mathrm{Pic}(X)_\ell \to 0,$$

where $\mathrm{Pic}(X)_\ell := \mathrm{Pic}(X) \otimes \mathbb{Z}_\ell$. We write

$$\widehat{\mathrm{Div}}(X)^0 \subset \widehat{\mathrm{Div}}(X)$$

for the group generated by the image $\hat{\rho}_X(\hat{K}^*)$ and identify an element $\hat{f} \in \hat{K}^*$ with its image.

LEMMA 11.7. — *Let X/k be smooth algebraic with $\mathrm{NS}(X) = \mathrm{Pic}(X)$. Let M be a* finite *set and*

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

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 $i \in I$

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

and

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

Proof. — We have a diagram

$$\begin{array}{ccccccc}
\mathrm{Ker}(\varphi) & \to & \oplus_{m \in M} \mathbb{Z} D_m & \xrightarrow{\varphi} & \Lambda \subset \mathrm{Pic}(X) & \to 0 \\
\downarrow & & \downarrow & & \downarrow & \\
\mathrm{Ker}(\varphi_\ell) & \to & \oplus_{m \in M} \mathbb{Z}_\ell D_m & \xrightarrow{\varphi_\ell} & \Lambda_\ell \subset \mathrm{Pic}(X)_\ell & \to 0.
\end{array}$$

Since $\mathrm{Pic}(X) = \mathrm{NS}(X)$ the map $\mathrm{Pic}(X) \to \mathrm{Pic}(X)_\ell$ is injective and

$$\mathrm{rk}_\mathbb{Z} \Lambda = \mathrm{rk}_{\mathbb{Z}_\ell} \Lambda_\ell \text{ and } \mathrm{rk}_\mathbb{Z} \mathrm{Ker}(\varphi) = \mathrm{rk}_{\mathbb{Z}_\ell} \mathrm{Ker}(\varphi_\ell).$$

In particular, $\mathrm{Ker}(\varphi_\ell)$ has a basis $\{D_i\}_{i \in I}$ (over $\mathbb{Z}_\ell$), where each D_i is a $\mathbb{Z}$-integral linear combinations of D_m (with $m \in M$) and is also in $\mathrm{Ker}(\varphi)$. It

follows that $D_i = \mathrm{div}(f_i)$ for some function $f_i \in K^*$ with support in D. Finally, we can find a representation

$$D = \sum_i a_i D_i,$$

with $a_i \in \mathbb{Z}_\ell$ linearly independent over $\mathbb{Z}$ (passing to a subset of I, if necessary). $\qquad\square$

12. ℓ-adic analysis: curves

PROPOSITION 12.1. — *Let $\tilde{k}$ be the closure of a finite field, $\mathrm{char}(\tilde{k}) \neq p$, C a curve over $\tilde{k}$ of genus g with function field $E = \tilde{k}(C)$ and*

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

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

$$\Phi^* \; : \; \widehat{\tilde{k}(\mathbb{P}^1)}^* \to \hat{E}^*$$

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

Proof. — Recalling the exact sequence (9.1), we have a commuting diagram

$$0 \longrightarrow \mathbb{Z}_\ell \Delta_{C(\tilde{k})} \longrightarrow \mathcal{M}(C(\tilde{k}), \mathbb{Z}_\ell) \longrightarrow \mathcal{G}^a_E \longrightarrow \mathbb{Z}_\ell^{2\mathsf{g}} \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z}_\ell \Delta_{\mathbb{P}^1(k)} \longrightarrow \mathcal{M}(\mathbb{P}^1(k), \mathbb{Z}_\ell) \longrightarrow \mathcal{G}^a_{k(\mathbb{P}^1)} \longrightarrow 0 \longrightarrow$$

Since Φ 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

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

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

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

so that

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

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 $w' \in \mathcal{V}_{\mathbb{P}^1}$. In particular, for the dual groups we have

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

where $a \in \mathbb{Z}_\ell^*$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

13. ℓ-adic analysis: surfaces

Let $K = k(X)$ be a function field of a smooth surface X over k. We will need an ℓ-adic version of Lemma 10.1 .

PROPOSITION 13.1. — *Let* $\hat{f}, \hat{g} \in \mathcal{FS}(K)$ *be such that*

- $\varrho_\nu(\hat{f}, \hat{g}) = 0$ *for every* $\nu \in \mathcal{DV}_K$;
- $\operatorname{supp}_K(\hat{f}) \cap \operatorname{supp}_K(\hat{g}) = \emptyset$.

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

Proof. — By Lemma 11.7,

$$\hat{f} = \prod_{i \in I} f_i^{a_i}, \text{ resp. } \hat{g} = \prod_{j \in J} g_j^{b_j},$$

where

- 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 ν and choose a (smooth) model X so that $\nu = \nu_D$ for some divisor $D \subset X$. Then

$$\varrho_\nu(\hat{f}, \hat{g}) = \prod \varrho_D(f_i, g_j)$$

and we can compute it using only those pairs f_i, g_j which have D in their support. In particular,

$$\hat{f}^{m_g}/\hat{g}^{m_f} = \prod (f_i^{a_i m_j}/g_j^{b_j m_i}),$$

where m_j (resp. m_i) is the order of g_j (resp. f_i) on D. This order vanishes unless $D \in \operatorname{supp}(\hat{f}) \cup \operatorname{supp}(\hat{g})$. By assumption, if $D \in \operatorname{supp}(\hat{f})$ then $D \notin \operatorname{supp}(\hat{g})$ (and $n_j = 0$) so that

$$\varrho_D(\hat{f}, \hat{g}) \in \hat{k}(D)^*.$$

Since the nonzero numbers a_i are linearly independent over $\mathbb{Z}$ the equality $\sum a_i m_i = 0$ implies that $m_i = 0$ (for all i) and that $g_D \in k^*$.

Similarly, $g_D = \prod (g_j)_D^{b_j}$, where b_j are linearly independent over $\mathbb{Z}$, and $g_D \in k^*$ implies that $(g_j)_D \in k^*$ (for all $j \in J$). It follows that

$$\varrho_\nu(f_i, g_j) = 0$$

for all f_i, g_j and every valuation $\nu = \nu_D$. By Lemma 10.1, all f_i, g_j belong to the same 1-dimensional field $E \subset K$ and hence $\hat{f}, \hat{g} \in \hat{E}^*$. $\square$

REMARK 13.2. —   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 13.1.

PROPOSITION 13.3. —   *Let $\mathfrak{K}^* \subset \mathcal{FS}(K) \subset \hat{K}^*$ be a subset with the following properties:*

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

$$\{[\delta_0, \hat{f}] \,|\, \hat{f} \in \mathfrak{K}^*\} \simeq \mathbb{Z}$$

  for a topological generator δ_0 of $\mathcal{I}_{\nu_0}^a$.

Then $\mathfrak{K}^* \subset K^*/k^* \otimes \mathbb{Z}_{(\ell)}$.

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

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

If some (any) topological generator δ_0 of $\mathcal{I}_{\nu_0}^a$ 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

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

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 $E' = k(x')$ and $E'' = k(x'')$. $\qquad\square$

COROLLARY 13.4. — *After a choice of δ_0, for every 1-dimensional $E \subset K$ and every $f \in E^*/k^*$ we can Galois-theoretically distinguish its poles from its zeroes.*

The last essential step is a Galois-theoretic characterization of the partial projective structure on $\mathfrak{K}^*/k^*$, more precisely, the characterization of generating elements and primary lines in $\mathfrak{K}^*/k^*$ (see Definition 2.5 and Example 3.10).

LEMMA 13.5. — *Let $x \in K^*$ be a generating element, $E := k(x)$ and $r = r(x) \in \mathbb{N}$ the smallest positive integer such that $x^r \in \mathfrak{K}^*$. Then*

- *$r = p^m$ for some $m \in \mathbb{N}$ (with $p = \mathrm{char}(k)$);*
- *$(E^*/k^*) \cap (\mathfrak{K}^*/k^*) = (E^{p^m})^*/k^*$;*
- *(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 $K/\mathfrak{K}$ is a finite purely inseparable extension, by Propositions 2.11 and 13.3. Next, we claim that a generator $y \in \mathfrak{K}$ is a p^m-th power of a generator 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 generator $y \in \mathfrak{K}^*$ is in $E^* \cap \mathfrak{K}^*$ (and is the minimal positive power of a generator in E contained in $E^* \cap \mathfrak{K}^*$). This implies the third property: the generators of E^{p^m} are p^m-th powers of the generators of E. $\qquad\square$

COROLLARY 13.6 (Definition). — *Assume that y, y' are primitive elements in $(E^{p^m})^* \subset \mathfrak{K}^*$ such that*

    – y, y' *have support in 2 points;*
    – *the pole of y coincides with the pole of y'.*

Then (the images of) y, y' in $\mathfrak{K}^*/k^*$ are contained in a primary line passing through (the images of) $1, y, y'$.

Proof. — Definition 9.1 and Lemma 9.2 give a Galois-theoretic characterization of the notion "support in 2 points". By Corollary 13.4 we can Galois-theoretically distinguish zeroes and poles of $y \in \mathfrak{K}^*/k^*$. It remains to apply Lemma 13.5. $\qquad\square$

14. Proof

In this section we prove our main theorem: if

$$(\mathcal{G}_K^a, \Sigma_K) = (\mathcal{G}_L^a, \Sigma_L),$$

where L is a function field over an algebraic closure of a finite field of characteristic $\neq 2, \ell$, then K is a purely inseparable extension of L.

Step 1. We have a nondegenerate pairing

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

This implies that $\hat{K}^* = \hat{L}^*$.

Step 2. We identify 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 $\sigma \in \Sigma_K$ 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). This identifies $\mathcal{DV}_K = \mathcal{DV}_L$.

Step 3. For every $\nu \in \mathcal{DV}_K$ we characterize intrinsically

$$\mathcal{I}_w^a \subset \mathcal{D}_\nu^a/\mathcal{I}_\nu^a$$

(see Proposition 9.3).

Step 4. We distinguish divisorial valuations with nonrational centers (see Lemma 9.4 and Remark 9.5).

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 set of elements satisfying the first notion of finiteness. If some (any) model X of K contains only finitely many rational curves, both notions of finiteness of support coincide and one obtains an intrinsic Galois-theoretic characterization of $K^*/k^* \otimes \mathbb{Z}_\ell \subset \hat{K}^*$, as elements in $\mathcal{FS}(K)$. In general, it may happen that some $g \in L^*/l^*$ has an "infinite rational tail" on some (every) model X of K:

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

where C_j are irreducible rational curves on X. In Lemma 11.6 we show that a many (and consequently, all) elements of $L^*/l^* \subset \mathcal{FS}(L) = \mathcal{FS}(K)$ have finite support on every model X of K, and vice versa. In particular, $K^*/k^* \otimes \mathbb{Z}_\ell = L^*/l^* \otimes \mathbb{Z}_\ell$.

Step 6. For every pair of elements $\hat{f}, \hat{g} \in \mathcal{FS}_X(K)$ satisfying

– $\mathrm{supp}_K(\hat{f}) \cap \mathrm{supp}_K(\hat{g}) = \emptyset$;
– $\varrho_\nu(\hat{f}, \hat{g}) = 0$ 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 13.1).

Step 7. Since $\mathrm{Pic}(X) = \mathrm{NS}(X)$ every such subfield $E = k(x)$ for some $x \in K^*$.

Step 8. Proposition 12.1 identifies E^*/k^* inside $\hat{E}^*$, up to conformal equivalence.

Step 9. Proposition 13.3 identifies $\mathfrak{K}^* := K^* \cap L^*$ (as a multiplicative group) with a multiplicative subgroup of $K^*/k^* \otimes \mathbb{Z}_{(\ell)}$.

Step 10. By Proposition 2.11, $\mathfrak{K}^*$ is a multiplicative group of a field so that both K and L are finite purely inseparable extensions of this field. It remains to insure that the additive structure on $\mathfrak{K}^*$ is intrinsically defined.

Step 11. By Theorem 3.7 and Proposition 3.11, the field is uniquely determined by the partial projective structure.

Step 12. Lemma 13.5 and Corollary 13.6 give a Galois-theoretic characterization of generating elements and primary lines in $\mathfrak{K}^*/k^*$. Proposition 2.10 and Example 3.10 show that these define a (unique) partial projective structure on $\mathfrak{K}^*/k^*$ (in particular, the projective structures induced by $\mathbb{P}(K)$ and $\mathbb{P}(L)$ coincide).

Step 13. If follows $K/\mathfrak{K}$ and $L/\mathfrak{K}$ are finite purely inseparable extensions of the *same* field. 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] R. J. MIHALEK – *Projective geometry and algebraic structures*, Academic Press, New York, 1972.

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

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

[9] 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.