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 2
2. Overview 3
3. Basic algebra and geometry of fields 6
4. Projective structures 15
5. Flag maps 19
6. Galois groups 29
7. Valuations 30
8. A dictionary 33
9. Flag maps and valuations 34
10. Galois groups of curves 36
11. Valuations on surfaces 42
12. ℓ-adic analysis: generalities 44
13. ℓ-adic analysis: curves 51
14. ℓ-adic analysis: surfaces 52
15. Proof 55
References 57

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 on $\mathcal{G}_K^a$: a set Σ_K of distinguished (primitive) subgroups which are isomorphic to *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.

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 $\neq \ell$. 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 L is isomorphic to a finite purely inseparable extension of K.

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. We thank the participants of the Algebraic Geometry Seminar at the University of Nice for their comments and suggestions.

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 $\mathcal{G}_K^a$ 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, $\mathcal{G}_K^a$ 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. This projective structure is invariant under *multiplicative* translations by elements of K^*/k^*.

For this we need Galois-theoretic information coming from $\mathcal{G}_K^c$, the maximal pro-ℓ-quotient of

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

This topological group parametrizes those ℓ-extensions of K whose Galois group is a central extension of an abelian ℓ-group.

Our main Galois-theoretic object is a pair $(\mathcal{G}_K^a, \Sigma_K)$, where the *fan* Σ_K is the set of all maximal (by inclusion) topologically noncyclic subgroups $\sigma \subset \mathcal{G}_K^a$ whose set-theoretic preimage in $\mathcal{G}_K^c$ is an abelian group. It turns out that such liftable subgroups σ are *finite-dimensional* $\mathbb{Z}_\ell$-subspaces in $\mathcal{G}_K^a$. Moreover, the maximal $\mathbb{Z}_\ell$-rank of such σ is $\dim(X)$.

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

$$\Psi : (\mathcal{G}_K^a, \Sigma_K) \to (\mathcal{G}_L^a, \Sigma_L)$$

then $k \simeq l$, Y is a surface and L is isomorphic to a purely inseparable extension of K.

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. 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 nonarchimedian divisorial valuation. Its abelian decomposition group $\mathcal{D}_\nu^a \subset \mathcal{G}_K^a$ is a (noncanonical) direct product of the inertia subgroup $\mathcal{I}_\nu^a \simeq \mathbb{Z}_\ell$ and the group $\mathcal{G}_{k(D)}^a$ of the field $k(D)$. Now a subgroup $\sigma \subset \mathcal{D}_\nu^a$ of $\mathbb{Z}_\ell$-rank 2 is liftable if and only if it contains $\mathcal{I}_\nu^a$. Thus Σ_K^{div} contains all liftable subgroups of $\mathbb{Z}_\ell$-rank 2 which are contained in groups $\mathcal{D}_\nu^a$.

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 $\mathcal{D}_\nu^a$, for different $\nu = \nu_D$. This gives an purely group-theoretic description of the groups $\mathcal{D}_\nu^a$: the nontrivial intersection of two liftable groups σ, σ' is always $\mathcal{I}_\nu^a$, for some divisorial valuation $\nu = \nu_D$, and $\mathcal{D}_\nu^a$ "centralizes" $\mathcal{I}_\nu^a$, it consists of all those elements in $\mathcal{G}_K^a$ which commute with $\mathcal{I}_\nu^a$, after lifting to $\mathcal{G}_K^c$.

The proof is based on Kummer theory and the interpretation of $\mathcal{G}_K^a$ 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 $\mathcal{D}_{\nu_D}^a, \mathcal{I}_{\nu_D}^a$ inside $\mathcal{G}_K^a$, or, vaguely speaking, we recovered "all curves" on all models X of K (and Y of L). Next we recover the "points" on D, as inertia groups $\mathcal{I}_w^a \subset \mathcal{G}_{k(D)}^a$, using various subgroups $\mathcal{I}_{\nu_{D'}}^a$ as follows: the image of $\mathcal{I}_w^a$ under any homomorphism of $\mathcal{G}_K^a$ to a finite group, which is trivial on $I_{\nu_D}^a$, coincides with the image of some $\mathcal{I}_{\nu_{D'}}^a$ (see Section 10). Conversely, for any $\gamma \in \mathcal{D}_{\nu_D}^a \setminus \mathcal{I}_w^a$, 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 $\mathcal{I}_{\nu_{D'}}^a$.

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.

We switch our attention to the dual space $\hat{K}^*$ of $\mathcal{G}^a_K$. We seek to recover the subset $L^*/l^* \subset \hat{K}^* = \hat{L}^*$ using Galois-theoretic data. This is done in several steps, each time obtaining a smaller subgroup:

- $\mathcal{FS}(K) \subset \hat{K}^*$ - elements in $\hat{K}^*$ with finite nonrational support,
- $K^*/k^* \otimes \mathbb{Z}_\ell \subset \mathcal{FS}(K)$ and
- $K^*/k^* \otimes \mathbb{Z}_{(\ell)}$.

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. The subgroup $\mathcal{FS}(K) \subset \hat{K}^*$ consists of elements whose support contains only finitely many nonrational divisors (characterized above). Of course, $\mathcal{FS}(K)$ contains K^*/k^* and L^*/l^* but it is still rather big - elements in $\mathcal{FS}(K)$ may have infinite rational "tails" if X contains infinitely many rational curves.

Next we use an ℓ-adic analog of a symbol $(f,g) \mod \ell^n \in \mathrm{K}_2(K)/\ell^n$. Notice that $(f,g) \mod \ell^n = 0$ for any $n \in \mathbb{N}$ if f, g belong to the same one-dimensional subfield in K. In particular, for any $f \in K \setminus k$ 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. This allows us to characterize

$$K^*/k^* \otimes \mathbb{Z}_\ell = L^*/l^* \otimes \mathbb{Z}_\ell \subset \mathcal{FS}(K)$$

as the subgroup generated by elements satisfying this property and having a "sufficiently big" support.

The next step involves a normalization. Inside $K^*/k^* \otimes \mathbb{Z}_\ell$ we cannot Galois-theoretically distinguish $L^*/l^* \otimes \mathbb{Z}_{(\ell)}$ from $a \cdot K^*/k^* \otimes \mathbb{Z}_{(\ell)}$, for $a \in \mathbb{Z}_\ell^*$. 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 (arbitary) irreducible divisor on a model X of K then $L^*/l^* \otimes \mathbb{Z}_{(\ell)}$ is naturally identified inside $K^*/k^* \otimes \mathbb{Z}_\ell$. Thus, after multiplication by $a \in \mathbb{Z}_\ell^*$, we can assume that $L^*/l^* \subset K^*/k^* \otimes \mathbb{Z}_{(\ell)}$.

Now we have K^*/k^* and L^*/l^* inside $K^*/k^* \otimes \mathbb{Z}_{(\ell)} = L^*/l^* \otimes \mathbb{Z}_{(\ell)}$. We also know that subgroups generated by elements f, g with pairwise trivial symbol $(f, g) = 0$ correspond to one-dimensional subfields in K, L, respectively. 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 $k(x)^*/k^* \otimes \mathbb{Z}_{(\ell)} = l^*(t)/l^* \otimes \mathbb{Z}_{(\ell)} \subset K^*/k^* \otimes \mathbb{Z}_{(\ell)}$, for some $t \in L$.

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

Now we add the projective structure over k, l, respectively. We notice that 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 is compatible with a unique projective structure on the (multiplicative) groups K^*/k^* and L^*/l^* - namely the one coming from the field structure. This defines a unique additive structure and finishes the proof of our main result.

3. Basic algebra and geometry of fields

NOTATIONS 3.1. — 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*).

In this paper we use extensively 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.

We assume familiarity with

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

LEMMA 3.2. — *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. — 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 X/k be a surface, $C_1, \ldots, C_s$ a finite set of (pairwise distinct) curves on X and $f_i \in k(C_i)^*$, for $i = 1, \ldots, s$. Then there exists an $f \in k(X)^*$ whose restriction to C_i is defined and equal to f_i, for all i.*

Proof. — Well known. □

LEMMA 3.4. — *For some ample smooth curve $i : C \hookrightarrow X$ the restriction $i^* : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(C)$ is an injection of abstract groups (of k-points).*
In particular, every element in $\mathrm{Pic}^0(X)$ is torsion.

Proof. — Let H be a polarization on X. There exists an $n \in \mathbb{N}$ such that for all pairs $L, L' \in \mathrm{Pic}^0(X)$ one has $H^1(X, -(L - L' + nH)) = 0$. Indeed, the property

$$H^1(X, -(L - L' + mH)) = 0$$

is open in $\mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X) \setminus \Delta$ (where Δ the diagonal subgroup), since $\mathrm{Pic}^0(X)$ is an algebraic group scheme. Denote by

$$U_{mH} \subset (\mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X) \setminus \Delta)$$

the corresponding subset. If we consider a increasing sequence

$$U_{n_iH},\ n_i \in \mathbb{Z},\ U_{mH} \subset U_{nH}, \text{ for } m < n,$$

the union of all U_{n_iH} is equal to $\mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X) \setminus \Delta$. Then there is an $n \in \mathbb{N}$ such that $U_{nH} = \mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X) \setminus \Delta$ (due to algebraicity of $\mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X) \setminus \Delta$ and all U_{n_iH}).

Exact sequence in cohomology implies that:

$$H^0(X, -L + L') = H^0(C_n, -L + L'),$$

where C_n is a smooth curve in the class $[nH]$. Since $H^0(X, -L + L') = 0$, for $L \neq L'$, the same holds for their restrictions. In particular,

$$i^* : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(nH)$$

is a set-theoretic embedding (on the set of k-points). □

REMARK 3.5. — A more delicate analysis shows that for $n \gg 0$ the map $i^* : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(nH)$ is an embedding of algebraic groups. Note that over a closure of a finite field the map

$$i : \mathrm{Pic}(X) \to \mathrm{Pic}(C)$$

is never an embedding if $\mathrm{rk}\,\mathrm{NS}(X) > 1$ (in contrast with characteristic zero).

LEMMA 3.6. — *Let X/k be a smooth projective surface, $C \subset X$ an irreducible curve and Q a finite set of points on C. Then there exists a diagram*

$$\begin{tikzcd} \tilde{C} \subset \tilde{X} \arrow[r, "\pi"] \arrow[d, "\tilde{\pi}"] & Y \\ C \subset X & \end{tikzcd}$$

where $\tilde{X} = \mathrm{Bl}(X) \to X$ is a blowup of X with center supported in $C \setminus Q$ and π is an isomorphism on $\tilde{X} \setminus \tilde{C}$ (the strict transform of C under $\tilde{\pi}$) which maps $\tilde{C}$ to a point on Y.

Proof. — There is a polarization H on X such that $H - C$ restricted to $X \setminus C$ is very ample (induces an embedding of $X \setminus C$ into a projective space). Let $\mathbb{P}^r_C$ be the projective space spanned by C under the embedding $X \subset \mathbb{P}^n$ by H. By our choice of H, $r < n$. A generic hyperplane $\mathbb{P}^{r-1} \subset \mathbb{P}^r_C$ intersects C transversally in finitely many smooth points $q_1, \ldots, q_s$ which are contained in $C \setminus Q$ (here we use Bertini's theorem for embedded curves, which in this case is evident over any algebraically closed field). The projection from this $\mathbb{P}^{r-1}$ (inside $\mathbb{P}^n$) induces a proper map from the blowup $\tilde{X}$ of X with center in $\cup q_i$ onto a projective surface $Y \subset \mathbb{P}^{n-r}$. Note that the image of C under the projection is a point $q \in Y$.

By construction, $\mathbb{P}^r_C$ intersects X exactly in C. Hence, the proper preimage of q in $\tilde{X}$ is $\tilde{C}$. Any other $\mathbb{P}^r \subset \mathbb{P}^n$ intersects $X \setminus C$ in at most one point and transversally (by assumption on $H^0(X, H-C)$). It follows that the projection induces an isomorphism between $\tilde{X} \setminus \tilde{C}$ and $Y \setminus q$. □

LEMMA 3.7. — *Let X/k be a smooth projective surface, $C \subset X$ a curve and $Q \subset C(k)$ a finite set. Let $\mathcal{L}$ be a line bundle on X whose restriction to C is trivial ($\mathcal{L}_C \simeq \mathcal{O}_C$). Then there exists a diagram*

$$\begin{tikzcd}
\tilde{C} \subset \tilde{X} \arrow[r, "\pi"] \arrow[d, "\tilde{\pi}"] & Y \\
C \subset X &
\end{tikzcd}$$

where $\tilde{X} = \mathrm{Bl}(X) \to X$ is a blowup with center supported in finitely many points on $C \setminus Q$ and π is a proper map as in Lemma 3.6 (contracting $\tilde{C}$) such that the pullback $\tilde{\mathcal{L}} = \tilde{\pi}^*\mathcal{L}$ is induced from Y.

Proof. — By Lemma 3.6, we may assume that C is (already) contractible. Since $\mathcal{L}$ is trivial on C we have $\mathcal{L} \simeq \mathcal{O}(R_1 - R_2)$, where R_1, R_2 are divisors on X intersecting C transversally, and

$$R_1 \cap C = R_2 \cap C \subset C \setminus Q.$$

Indeed, we can find a polarization H, so that $\mathcal{L} + H$ is also a polarization, giving surjective maps

$$\begin{array}{ccc} H^0(X, \mathcal{L}+H) & \to & H^0(C, (\mathcal{L}+H)_C) \\ H^0(X, H) & \to & H^0(C, H_C). \end{array}$$

Let $i_C : (\mathcal{L}+H)_C \xrightarrow{\sim} H_C$ be an isomorphism. We can find a pair of sections

$$\mathsf{s}_1 \in H^0(X, \mathcal{L}+H), \ \ \mathsf{s}_2 \in H^0(X, H)$$

with $i_C(\mathsf{s}_1)_C = (\mathsf{s}_2)_C$. Let R_i be the zero divisor of s_i. Then $\mathcal{O}(R_1 - R_2) \simeq \mathcal{L}$ and R_1, R_2 intersect C transversally with

$$R_1 \cap C = R_2 \cap C \subset C \setminus Q,$$

as claimed.

Consider the smooth surface $\tilde{\pi} : \tilde{X} \to X$ obtained by blowing up $R_i \cap C$. The proper preimages $\tilde{R}_i$ of R_i in $\tilde{X}$ don't intersect the proper preimage $\tilde{C} \subset \tilde{X}$ of C. The divisor of $\pi^*\mathcal{L} = \pi^*(R_1 - R_2)$ doesn't contain components which are exceptional curves lying over points in C. Hence $\pi^*\mathcal{L}$ is trivial on the open quasi-projective neighborhood $\tilde{X} \setminus \mathrm{supp}(\pi^*(R_1 - R_2))$ containing $\tilde{C}$. Therefore, the bundle $\mathcal{L}$ is induced from Y (as in Lemma 3.6). □

LEMMA 3.8. — *Let K/k be the function field of a surface, C/k a smooth curve on a model of K and $Q = \{q_0, \dots, q_s\} \subset C(k)$ a finite set of points. Then there exist a model X of K, irreducible divisors D_j, H_j, H'_j on X, with $j = 0, \dots, s$, 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 $j = 1, \dots, s$;*
(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. — Let X be a smooth projective model of K containing C as a smooth curve. Choose divisors $D_j \subset X$ passing (transversally) through q_j (for all $j = 0, \dots, s$). Blowing up points in $C \setminus Q$ we can insure that the (strict transform of) C becomes contractible and that the image of the surface under a contracting morphism is *projective* (by Lemma 3.6).

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 3.2, 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 open neighborhood of C in some model X (using Lemma 3.7).

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.

More precisely, choose classes $[H_i]$ so that

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

provide an embedding of Y into a projective space. Consider an embedding of Y into a projective space defined by one of the series $[H_j], [H'_j]$. For any finite set of irreducible divisors in Y we find a hyperplane section intersecting the union of these divisors transversally and not containing the given finite set of points in Y. Using induction on j we find representatives of $[H_j], [H'_j]$ satisfying the lemma. ☐

LEMMA 3.9. — *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 3.10. — *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 3.11. — 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 3.12. — *For any subfield $E \subset K$ there is a sequence*

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

where

- *π_E is rational 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 3.12, with $k(Y) = k(x)$. 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.

PROPOSITION 3.13. — *Let $K = k(X)$ be the function field of a smooth surface, $C \subset X$ a smooth irreducible curve and $f_1, \dots, f_s \in K^*$ rational functions on X, restricting nontrivially to C. Then there exists a model $\tilde{X}$ of K (a blowup of X) such that for every point q in (the strict transform) of $C \subset \tilde{X}$ there exists an irreducible divisor $D_q \subset \tilde{X}$ (possibly the zero divisor) with the property that for all $i = 1, \dots, s$ the order of D_q in the divisor of f_i is equal to the order of f_i in q.*

Proof. — Consider the divisors C and $\mathrm{div}(f_i)$, $i = 1, \dots, s$ and a model $\tilde{X}$ of K such that the total preimage $\tilde{D} \subset \tilde{X}$ of the union of all these divisors in $\tilde{X}$ has strict normal crossings (resolution of singularities for surfaces). After further blowups we can assume that each irreducible component of $\tilde{D}$ (distinct from C) intersects (the strict transform of) C in at most one point. For each $q \in C \cap (\tilde{D} \setminus C)$ let D_q be this component. For all other q let D_q be the zero divisor. These divisors have the required properties. □

LEMMA 3.14. — *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 3.15. — *Let X be a model of K containing a rational curve C and $x \in K^*$ a function such that its restriction x_C to C is defined and such that $k(C) = k(x_C)$. 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 $k(x_C)$ 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 $k(C)$ the subfield $\mathfrak{K}$ is 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 subsets in K^*.

DEFINITION 3.16. — *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 3.17. — 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 3.18. — *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 3.19. — *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 $x \in K^*$ 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 3.9).

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 3.12). 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 $z\in\mathfrak{K}$. $\square$

REMARK 3.20. — 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 $r \in \mathbb{N}$.

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 $s_1, \ldots, s_n$ 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

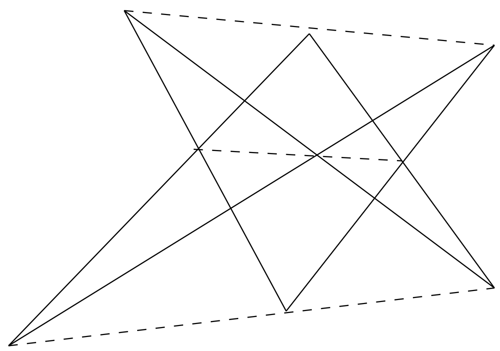
- $\langle S'' \rangle \subset T$ for every finite set $S'' \subset S'$;

– 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 $|S'| - 1$.

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 field* k *such that* $S = \mathbb{P}_k^n$. *This field is unique, up to isomorphism.*

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/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

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

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 $\mathbb{P}^1_k$ $(= \mathfrak{l}_1)$ stabilizing one point (the intersection $\mathfrak{l}_1 \cap \mathfrak{l}_2$). A choice of an additional point $s \in \mathbb{P}^2 \setminus \mathfrak{l}_1 \cup \mathfrak{l}_2$ trivializes this homogeneous space to the group of affine transformations of an affine line over k and 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 (nonzero) $c'(x, y) \in k'$ such that

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

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

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

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. $\square$

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 3.10) 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

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

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 $\mathbb{P}(A) = (A \setminus 0)/\mathbb{F}^*$ its projectivization;
- $\mathcal{M}(A)$ the set of maps from A 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.

DEFINITION 5.2. — *An $\mathbb{F}$-flag on a vector space $A \in \mathrm{Vect}_{\mathbb{F}}$ is a collection of $\mathbb{F}$-subspaces $(A_n)_{n=0,\dots,d}$ such that*

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

The flag is called complete *if $d = \dim(A)$.*

DEFINITION 5.3. — *A map $\mu \in \mathcal{M}(A)$ will be called $\mathbb{F}^*$-homogeneous if for all $a \in A$ and all $\kappa \in \mathbb{F}^*$ one has*

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

DEFINITION 5.4. — *A map μ on a (possibly infinite-dimensional) vector space A will be called an $\mathbb{F}$-flag map, if*

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

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* $\mathbb{F}$*-subspace* B_1 *is called the subspace of* nongeneric *elements. The set of* $\mathbb{F}$*-flag maps will be denoted by* $\Phi_{\mathbb{F}}(A)$*.*

EXAMPLE 5.5. — Let $K = k(X)$ be a function field. We can consider it as a vector space over k or over any of the 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 5.6. — *Let* A *be an* $\mathbb{F}$*-algebra (without zero-divisors). A map* $\mu \in \mathcal{M}(A)$ *will be called logarithmic if*

- μ *is* $\mathbb{F}^*$*-homogeneous and*
- $\mu(a \cdot a') = \mu(a) + \mu(a')$*, for all* $a, a' \in A \setminus 0$.

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

DEFINITION 5.7. — *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 5.8. — *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 5.17);
- reduction to linear spaces over prime fields, resp. $\mathbb{F}_4$, see Lemma 5.19: if $\mu \notin \Phi_{\mathbb{F}'}(A)$, for a finite field $\mathbb{F}'$, and μ is $\mathbb{F}^*$-homogeneous 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: for any rank two $\mathbb{Z}_\ell$-module $\sigma = \langle \mu, \mu' \rangle$ of logarithmic maps generated by a c-pair $\mu, \mu' \in \mathcal{L}_{\mathbb{F}}(A)$, not containing a flag map there is a subgroup $B = B_\sigma \simeq \mathbb{F}_p^3 \subset A$ (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 (resp. $\mathbb{F}_4$): for any σ spanned by a c-pair μ, μ' on B there is a $\mu'' \in \sigma$ such that $\mu'' \in \Phi_{\mathbb{F}}(B)$ - this shows the existence of the desired flag map on A.

□

LEMMA 5.9. — *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 $\mathbb{F}^*$-homogeneous, A_{n+1} is an $\mathbb{F}$-vector space. Indeed, for $a, a' \in A_{n+1}$ and $\kappa, \kappa' \in \mathbb{F}^*$ write

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

with finite I, J. Since

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

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 5.10. — The flag property does not depend on the value of an $\mathbb{F}$-flag map μ in $0 \in A$. Since μ is $\mathbb{F}^*$-homogeneous, 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 a family of $\mathbb{F}^*$-homogeneous maps on A, differing only by their value in $0 \in A$. 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* (resp. nongeneric) elements of $\mathbb{P}_{\mathbb{F}}(A)$ the image of generic (resp. nongeneric) elements from A.

NOTATIONS 5.11. — 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 5.12. — *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 5.13. — *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 $\mathbb{P}(A_1) \in \hat{\mathbb{P}}(A)$). □

We need the following elementary

LEMMA 5.14. — *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 $\mathbb{F}$. Then 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 $\mathbb{F}$) which is not contained in any of the above hyperplanes and which does not intersect 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 5.15. — *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 $\mathbb{F}^*$-homogeneous 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 $\#\{\mu^{\mathrm{gen}}(B_i)\} \geq 3$ or*
(2) $\mu^{\mathrm{gen}}(B_1) = \mu^{\mathrm{gen}}(B_2) \neq \mu^{\mathrm{gen}}(B_3) = \mu^{\mathrm{gen}}(B_4)$.

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 5.14, 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 5.16. — *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 5.15, 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 5.17. — *Let $A \in \mathrm{Vect}_{\mathbb{F}}$, with $\#\mathbb{F} \geq 11$, and $\mu \in \mathcal{M}(A)$ be an $\mathbb{F}^*$-homogeneous 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 5.16, 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 $\mu^{\mathrm{gen}}(B) \neq \hat{\mu}$, contradicting the assumption that $\hat{\mu}$ is constant. Otherwise, put $A_1 := B$. By the inductive assumption, $\mu \in \Phi_{\mathbb{F}}(B)$ 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 $\mu^{\mathrm{gen}}(B)$. Choose an $\mathbb{F}$-basis $b_1, \ldots, b_{n-1}$ in B such that $\mu(b_i) = \mu^{\mathrm{gen}}(B)$. 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 $\mu^{\mathrm{gen}}(B') \neq$ the generic value of $\hat{\mu}$, contradicting the uniqueness of B. It follows that μ is constant on $A \setminus B$. □

REMARK 5.18. — 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 $\mathbb{F}^*$-homogeneous, then $\mu \in \Phi_{\mathbb{F}}(A)$. Indeed, by Lemma 5.9, 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 5.19. — *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 $\mathbb{F}^*$-homogeneous 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

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

where $\#\mathbb{F}' = q$. Similarly, there are at most $(q+1)^2$ such nongeneric $c \in A$ 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 $\mathbb{F}^*$-homogeneous it follows that μ takes two values, and not three as we assumed. Contradiction. □

LEMMA 5.20. — *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 $C_\mu \subset B$, $\dim_{\mathbb{F}'} C_\mu = 2$ with the property that $\mu_{C_\mu} \notin \Phi_{\mathbb{F}'}(C_\mu)$.

Proof. — We will consider K as an $\mathbb{F}$-vector space as well as an $\mathbb{F}'$-vector space.

Let μ be an $\mathbb{F}^*$-homogeneous map on K. If μ were an $\mathbb{F}'$-flag map on every two-dimensional $\mathbb{F}'$-subspace of K then, by Lemma 5.19, 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 5.17 and conclude that $\mu \in \Phi_{\mathbb{F}}(K)$.

Thus, since $\mu \notin \Phi_{\mathbb{F}}(K)$-map, 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, by the logarithmic property. For $s \neq 0$, we have $s\tilde{\mu} + s'\tilde{\mu}' \notin \Phi_{\mathbb{F}'}(C)$. Otherwise, $s\tilde{\mu} + s'\tilde{\mu}' \notin \Phi_{\mathbb{F}'}(\frac{c}{c'} \cdot C')$. □

A detailed analysis of c-pairs on projective planes as above shows that $\langle \mu', \mu'' \rangle_{\mathbb{Z}_\ell}$ on any such space contains a flag map. This will complete the proof of the main theorem.

LEMMA 5.21 (Lemma 4.3.2 in [**3**]). — *Let $B = \mathbb{F}^3$ and $\mu, \mu' \in \mathcal{M}(B)$ be a c-pair of $\mathbb{F}^*$-homogeneous maps. Then the image of $\mathbb{P}(B)$ under map*

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

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

Proof. — Observe that the image of every $\mathbb{P}^1 \subset \mathbb{P}(B)$ is contained in an affine line in $\mathbb{Z}_\ell^2$. This is simply the geometric interpretation of the condition for μ, μ' to be a c-pair.

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 q and, by the first observation, $\varphi(q)$ must lie on both $\mathfrak{l}$ and $\mathfrak{l}'$).

We claim that any subset $V \subset \mathbb{Z}_\ell^2$ with this property is either infinite or contained in a union of a line and a point.

We imbed $\mathbb{A}^2(\mathbb{Z}_\ell)$ into the projective space $\mathbb{P}^2(\mathbb{Q}_\ell)$. Assume that there are 4 distinct points in V, no three of which are on one line. We saw that V contains the intersection points of any two lines through these points. Then there is a projective transformation of $\mathbb{P}^2(\mathbb{Q}_\ell)$ with the property that (the image of) V contains points with homogeneous coordinates

$$(1, 0, 0), (1, 0, 1), (0, 0, 1), (0, 1, 1), (0, 1, 0).$$

Computing the coordinates of intersections of lines through points in V we find that V contains points with coordinates $(1/2^n, 0, 1), (0, 1/2^n, 1)$, for all $n \in \mathbb{N}$. Thus V is infinite, while $\mathbb{P}(B)$ is finite, contradiction.

If in every subset of four points in V three are collinear then all points but one are collinear. Indeed, assume this holds for a subset $V_n \subset V$ consisting of $n \geq 4$ points, let $\mathfrak{l}$ be a line in $\mathbb{P}^2(\mathbb{Q}_\ell)$ containing the $n - 1$ aligned points in V_n and assume that $x \in V_n \setminus \mathfrak{l}$. Let $V_{n+1} = V_n \cup y$, with $y \notin \mathfrak{l}$, write $\mathfrak{l}(x, y)$ for the line through x, y and put $u = \mathfrak{l} \cap \mathfrak{l}(x, y) \in V$. Then there are two more points $z, t \in V_n$, with $z, t \neq u$, (since $\mathfrak{l}$ contains at least 3 points in V_n). Now all six lines

$$\mathfrak{l}(x, y), \mathfrak{l}(x, t), \mathfrak{l}(x, z), \mathfrak{l}(y, z), \mathfrak{l}(y, t), \mathfrak{l}(z, t) = \mathfrak{l}$$

are different, contradicting the assumption. $\square$

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 5.20,*
- B *is as in Lemma 5.20, and in particular, there exist two-dimensional* $C, C' \subset B$ *so that* $\mu_C \notin \Phi_{\mathbb{F}}(C), \mu'_{C'} \notin \Phi_F(C')$ *and* $\mu_{C'} = \mu'_C = 0$.

We can also 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* $\mathfrak{l} \in \mathbb{P}(B)$*; 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) $\varphi(\mathbb{P}(B))$ *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. Assume that* $\varphi(\mathfrak{l}), \varphi(\mathfrak{l}')$ *are contained in the same affine line in* $\mathbb{Z}_\ell^2$*. Then* $\varphi(\mathfrak{l}) = \varphi(\mathfrak{l}')$*. Moreover, every point* $x \in \mathbb{P}^2$ *with* $\varphi(x) \notin \varphi(\mathfrak{l})$ *induces a projective isomorphism* $\pi_{x,\mathfrak{l}'} : \mathfrak{l} \to \mathfrak{l}'$ *such that for all* $y \in \mathfrak{l}$ *one has* $\varphi(y) = \varphi(\pi_{x,\mathfrak{l}'}(y))$.

Proof. — Choose a $y \in \mathfrak{l}$ and an $x \in \mathbb{P}^2$ such that $\varphi(x) \notin \varphi(\mathfrak{l})$, this is possible by (1), and consider the line $\mathfrak{l}(x, y)$. Define $\pi_{x,\mathfrak{l}'}(y) := \mathfrak{l}(x, y) \cap \mathfrak{l}'$. By Lemma 5.21, $\varphi(\pi_{x,\mathfrak{l}'}(y))$ is contained in the intersection of $\varphi(\mathfrak{l}') = \varphi(\mathfrak{l})$ and $\varphi(\mathfrak{l}(x, y))$, so that $\varphi(\pi_{x,\mathfrak{l}'}(y)) = \varphi(y)$. ☐

COROLLARY 5.24. — *Assume that* $\varphi(\mathfrak{l}) = \varphi(\mathfrak{l}')$ *for distinct lines* $\mathfrak{l}, \mathfrak{l}' \subset \mathbb{P}^2_{\mathbb{F}}$ *and let* $x, y \in \mathbb{P}^2_{\mathbb{F}}$ *be points such that* $\varphi(x), \varphi(y) \notin \varphi(\mathfrak{l})$*. Then the projective isomorphisms* $\pi_{x,\mathfrak{l}'}, \pi_{y,\mathfrak{l}'} : \mathfrak{l} \to \mathfrak{l}'$ *have the following property: the composition*

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

is a nontrivial translation, preserving $\mathfrak{l} \cap \mathfrak{l}'$ *and the level sets of* φ*. In particular, if* $\mathbb{F} = \mathbb{F}_p$ *(the prime field) then 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 to* $\mathfrak{l} \setminus (\mathfrak{l} \cap \mathfrak{l}')$

is a union of two (two point) orbits of this translation and φ is constant on each orbit.

Proof of Theorem 5.8. — We keep the Assumptions 5.22. Put $\mathbb{P}^2 = \mathbb{P}(B)$ and $\mathfrak{l} = \mathbb{P}^1 = \mathbb{P}(C), \mathfrak{l}' = \mathbb{P}^1 = \mathbb{P}(C')$. For every $\mathbb{P}^1 \subset \mathbb{P}^2$ its image $\varphi(\mathbb{P}^1)$ spans a unique affine line. Assume there exists a $q \in \mathbb{P}^2 \setminus \mathfrak{l}$ such that $\varphi(q)$ is contained in the affine line L spanned by $\varphi(\mathfrak{l})$. Since $\mu_{\mathfrak{l}} \notin \Phi(\mathfrak{l})$, there is an $r \in \mathfrak{l}$ such that $\varphi(r) \neq \varphi(q)$. Put $\mathfrak{l}'' = \mathfrak{l}(q, r)$. Then $\varphi(\mathfrak{l})$ and $\varphi(\mathfrak{l}'')$ are both contained in L; and since $\mu' \notin \Phi(\mathfrak{l}')$ there exist two distinct points $x, y \in \mathfrak{l}'$ such that $\varphi(x), \varphi(y)$ are not contained in L. Now we use Lemma 5.23 and Corollary 5.24: If $\mathbb{F} = \mathbb{F}_p$ then μ is transitive on $\mathfrak{l} \setminus r$ and preserves φ. Thus $\mu_{\mathfrak{l}}$ is constant on $\mathfrak{l} \setminus r$, contradiction to $\mu_{\mathfrak{l}} \notin \Phi(L)$.

For $\mathbb{F} = \mathbb{F}_4$ we have

$$\mathfrak{l} = r \cup (t_1 \cup t_2) \cup (s_1 \cup s_2),$$

with

$$\varphi(t_1) = \varphi(t_2) \ \text{ and } \ \varphi(s_1) = \varphi(s_2).$$

Since $\mathfrak{l}$ and $\mathfrak{l}''$ are projectively (and φ-invariantly) equivalent we have

$$\mathfrak{l}'' = r \cup (t_1'' \cup t_2'') \cup (s_1'' \cup s_2''),$$

with

$$\varphi(t_1'') = \varphi(t_2'') \ \text{ and } \ \varphi(s_1'') = \varphi(s_2'').$$

Since $\varphi(\mathfrak{l}(t_1'', s_1))$ and $\varphi(\mathfrak{l}(s_1'', t_1))$ are again both contained in the same affine line L we get translations on $\mathfrak{l}$ on the complement to both s_1 and t_1. It follows that

$$\varphi(r) = \varphi(t_1) = \varphi(s_1)$$

contradiction to the assumption that $\mu \notin \Phi(\mathfrak{l})$.

We conclude that $\varphi(\mathfrak{l})$ consists of two points. Otherwise, by Lemma 5.21, $\mathbb{P}^2 \setminus \mathfrak{l}$ is mapped to the unique point outside L (spanned by $\varphi(\mathfrak{l})$), contradicting Assumption 5.22 (3). Applying the same argument to $\mathfrak{l}'$ we find that $\varphi(\mathfrak{l}')$ also consists of two points and that no points $q \in \mathbb{P}^2 \setminus (\mathfrak{l} \cup \mathfrak{l}')$ are mapped to the union of affine lines $L \cap L'$ spanned by $\varphi(\mathfrak{l})$ and $\varphi(\mathfrak{l}')$.

In particular, the image of all lines $\mathfrak{l}'' \neq \mathfrak{l}, \mathfrak{l}'$ is contained in the same affine line L''. Since $\mu \notin \Phi(\mathfrak{l})$ there must be two distinct points $x, y \in \mathfrak{l}$ with $\varphi(x), \varphi(y) \notin L''$. Applying Lemma 5.23 and Corollary 5.24 one more time we find a φ-invariant translation on all $\mathfrak{l}''$ mapped to L''. In particular, either

$\varphi^{-1}(\varphi(\mathfrak{l}\cap\mathfrak{l}''))$ or $\varphi^{-1}(\varphi(\mathfrak{l}'\cap\mathfrak{l}''))$ contains more than one point, contradiction. □

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, $\mathcal{G}_K^a$ 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. In our situation, $\mathcal{G}_K^a$ is a torsion-free $\mathbb{Z}_\ell$-module.

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. — *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 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). — *For every* $n \in \mathbb{N}$ *we have a pairing*

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

which extends to a nondegenerate pairing

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

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

Proof. — Let $\sigma \subset \mathcal{G}^a_E$ be a subgroup with $\mathrm{rk}_{\mathbb{Z}_\ell}\sigma = 2$. Let $\hat{\sigma}$ be the primitive hull of σ in $\mathcal{G}^a_E$ and fix an $n > \#\hat{\sigma}/\sigma$. Assume that σ lifts to an abelian subgroup $\sigma^c \subset \mathcal{G}^c_E$. Then there exist $f, g \in K^*/(K^*)^{\ell^n} = H^1(\mathcal{G}^a_E, \boldsymbol{\mu}_{\ell^n})$ so that $f \wedge g \in H^2(\mathcal{G}^a_E, \boldsymbol{\mu}_{\ell^n})$ is a generator of $H^2(\hat{\sigma}, \boldsymbol{\mu}_{\ell^n})$. In particular, it gives a nontrivial element upon restriction to $H^2(\sigma, \boldsymbol{\mu}_{\ell^n})$. Consider the surjections $\mathcal{G}_E \xrightarrow{p_c} \mathcal{G}^c_E \xrightarrow{p_a} \mathcal{G}^a_E$ and the induced sequence

$$H^2(\mathcal{G}^a_E, \boldsymbol{\mu}_{\ell^n}) \xrightarrow{p_a^*} H^2(\mathcal{G}^c_E, \boldsymbol{\mu}_{\ell^n}) \xrightarrow{p_c^*} H^2(\mathcal{G}_E, \boldsymbol{\mu}_{\ell^n}).$$

Since H^2 classifies central extensions,

$$\mathrm{Ker}(p_c^* \circ p_a^*) \subset \mathrm{Ker}(p_a^*).$$

Since the lift σ^c is abelian there is a section $s : \sigma \to \mathcal{G}^c_E$, with $p^a_c \circ s = id$. Thus if $f \wedge g \in H^2(\mathcal{G}^a_E, \boldsymbol{\mu}_{\ell^n})$ restricts nontrivially to σ^c then $p_a^*(f \wedge g) \neq 0$. However, $p_c^* \circ p_a^*(f \wedge g) = 0$, since $H^2(\mathcal{G}_E, \boldsymbol{\mu}_{\ell^n}) = 0$ (by [**10**], Ch. 2, Prop. 11). Contradiction. □

7. Valuations

In this section we recall basic results concerning valuations and valued fields (we follow [**4**]). Most of this material 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 (nonarchimedian)* 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 $K = k(X)$, with k as above, and ν be a nonarchimedian 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 $\mathcal{G}^a_K$, called an inertia element of the valuation ν. The subgroup generated by such elements is $\mathcal{I}^a_\nu \subset \mathcal{G}^a_K$.

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

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

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

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 (nonarchimedian) 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 $C \subset X$ defines a valuation ν_C on K with value group $\mathbb{Z}$ and every valuation ν on K with value group $\mathbb{Z}$ 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 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. $\square$

8. A dictionary

Write

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

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 $\mu, \mu' \in \mathcal{G}^a_K$ form a commuting pair then the corresponding maps $\mu, \mu' \in \mathcal{L}_K$ form a c-pair (in the sense of Definition 5.7).

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, $\mu, \mu' \in \mathcal{G}^a_K$ define a rank 2 liftable subgroup in $\mathcal{G}^a_{k(x)}$. Such subgroups don't exist since $\mathcal{G}_{k(x)}$ is a free pro-ℓ-group. $\square$

EXAMPLE 8.2. — If $\mu \in \mathcal{D}^a_\nu$ and $\alpha \in \mathcal{I}^a_\nu$ 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, $\alpha \in \mathcal{I}^a_\nu$ (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), $\alpha \in \mathcal{I}^a_\nu$. ☐

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

Proof. — By Theorem 5.8, 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*

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

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. □

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 inertial 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

ν 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. $\square$

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

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

with the identifications

- $\mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}_\ell) = \mathbb{Z}_\ell(\Delta)$ (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, 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

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

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. 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 $\mathcal{I} \subset \mathcal{G}_E^a$ 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 10.2. — *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*

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

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 (10.2), 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

$$\iota(q_{s_1}) \neq \iota(q_{s_2}). \tag{10.4}$$

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 $\mathrm{Div}^0_Q(C)$ be the abelian group of degree zero divisors on C supported in Q. By Lemma 3.2, there is an $n = n_Q \in \mathbb{N}$ such that nD is principal for every $D \in \mathrm{Div}^0_Q(C)$. 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)

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

Notice that $[\mathcal{I}^a_w, f] = 0$ 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 (10.4) 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

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

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

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

satisfies the required properties. □

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 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,

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

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, $\psi(\mathcal{G}^a_{k(C)}) = \psi(\mathcal{I}^a_{k(C)})$). 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 3). 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

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

We consider two cases

(1) there exist two points $q, q' \in C(k)$ such that $\mathcal{I} \subset \langle \mathcal{I}^a_w, \mathcal{I}^a_{w'}\rangle$;
(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 10.2, 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

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

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 3.8. 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. □

LEMMA 10.4. — *Let $E = k(C)$ be the function field of a curve. Then $\mathrm{g}(C) \geq 1$ 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 (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

The next stage of the recognition process leads us to the following problem: How to characterize subgroups $\widehat{k(C)}^* \subset \hat{K}^*$? In this section we recall a geometric argument (used in algebraic K-theory) characterizing pairs of functions $f, g \in K^*$ which are contained in $k(C)^* \subset K^*$, for some curve C (such curves correspond to projections $X \to C$).

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

$$\begin{array}{ccc} K^* \times K^* & \to & \boldsymbol{K}^*_\nu / k^* \\ f, g & \mapsto & f^{\nu(g)}/g^{\nu(f)}. \end{array} \tag{11.1}$$

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

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

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 $f, g \in K^*$*

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

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, $\varrho_\nu(f,g) = 1$ 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 $\varrho_\nu(f,g) = 1$.

($\Rightarrow$) 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 $\varrho_D(f,g) \neq 0$ 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 $\pi_f = \pi_g$. $\square$

12. ℓ-adic analysis: generalities

Hypothetically, surjective homomorphisms $\mathcal{G}_K^a \to \mathcal{G}_{k(C)}^a$ (or dually, inclusions $\widehat{k(C)^*} \subset \hat{K}^*$) are characterized as follows: assume, we have a commutative diagram

$$\begin{tikzcd} \mathcal{G}_K^c \arrow[r] \arrow[d] & A^c \arrow[d] \\ \mathcal{G}_K^a \arrow[r, "\psi"'] & A \end{tikzcd}$$

where the abelian group A is a rank two torsion-free $\mathbb{Z}_\ell$-module and A^c is its free central extension. Then there exists a unique field $k(C) \subset K$ and a factorization of ψ:

$$\mathcal{G}_K^a \to \mathcal{G}_{k(C)}^a \to A.$$

Here we solve a dual problem. We distinguish, Galois-theoretically, a certain subgroup inside $\hat{K}^*$ which contains K^*/k^*. The main result is the Galois-theoretic determination of pairs $\hat{f}, \hat{g}$ of elements of this subgroup which are contained in the completion $\widehat{E}^*$ of the same one-dimensional field.

In detail, to every $f \in K^*$ one associates its divisor $D = D_f$ on X. Conversely, D (uniquely) determines the image of $f \in K^*/k^*$. Recall that the Galois group $\mathcal{G}_K^a$ determines $\hat{K}^*$, a group substantially bigger than K^*/k^*. The goal is to detect the ℓ-adic subspace $K^*/k^* \otimes \mathbb{Z}_\ell \subset \hat{K}^*$.

We start with the theory of divisors with $\mathbb{Z}_\ell$-adic coefficients associated to elements in $\hat{K}^*$. Such an element is, in general, represented by a divisor with infinite support on X, with rapidly decreasing coefficients (in the ℓ-adic topology on Z_ℓ). The Galois datum $(\mathcal{G}_K^a, \Sigma_K)$ allows us to distinguish between rational and nonrational irreducible divisors (via the corresponding valuations) and to characterize intrinsically a subspace $\mathcal{FS}(K) \subset \hat{K}^*$ (of divisors with finite nonrational support, see 12.2 and 12.3), containing $K^*/k^* \otimes \mathbb{Z}_\ell$.

In order to further shrink $\mathcal{FS}(K)$ using Galois data we use the fact that for any nontrivial $f \in K^*$ there are many other $g \in \hat{K}^*$ with $\hat{\rho}(f, g) = 0$ (where $\hat{\rho}(f, g) = 0$ is the ℓ-adic generalization of $\rho(f, g) = 0$). Those are arbitrary elements $g \in \hat{E}^*, E = \overline{k(f)}^K$. However, for a sufficiently generic element $\hat{f} \in \hat{K}^*$ the element g with $\rho(f, g) = 0$ is equal to $f^a, a \in \mathbb{Z}_\ell$.

Thus the property that for $f \in \hat{K}^*$ the set of $g \in \hat{K}^*$ with $\hat{\rho}(f, g) = 0$ contains many elements different from $f^a, a \in \mathbb{Z}_\ell$ can be used to select a smaller subgroup $\mathcal{FS}_X(K) \subset \mathcal{FS}(K)$, containing K^*/k^*. Elements in $\mathcal{FS}_X(K)$ have finite support on every model X. We show in Section 14 that $\rho(f, g) = 0, f, g \in \mathcal{FS}_X(K)$ implies that $f, g \subset \hat{E}^*, E = \bar{k}(x)^K$ for some $x \in K^*$.

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. We identify an $f \in K^*/k^*$ 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

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

  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

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

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

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

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

and a residue map

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

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 (11.1).

DEFINITION 12.1. — *We say that distinct $\hat{f}, \hat{g} \in \hat{K}^*$ commute if $\hat{\varrho}_\nu(\hat{f},\hat{g}) = 0$, for all divisorial ν. We say that they have disjoint support if for all divisorial valuations $\nu \in \mathcal{DV}_K$*

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

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 12.2. — We put

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

DEFINITION 12.3. — *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 set of such elements.

DEFINITION 12.4. — *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 12.5. — *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 only of rational curves. □

COROLLARY 12.6. — *Let* K *be the function field of a surface* X *containing only finitely many rational curves. Then*

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

This gives 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 $\widehat{\mathrm{Div}}_{\mathrm{nr}}(X') = \widehat{\mathrm{Div}}_{\mathrm{nr}}(X)$. Under this identification

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

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
- $\rho_C(f_C) \neq 0 \mod \ell$.

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

LEMMA 12.7. — *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 exists an $f \in \mathcal{F}(K)$ with*

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

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. (Notice that such y generate K^*.) Using such y we construct $\mathcal{F}(K)$ as follows.

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

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

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

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

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, $\rho_{\nu'_j}(\hat{f}, \hat{g}) = 0$, 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. $\square$

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 we denote by $\mathrm{Pic}(X)_\ell$ the quotient group $\widehat{\mathrm{Div}}(X)/\hat{K}^*$. Write

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

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

LEMMA 12.8. — *Let X/k be a smooth projective surface, M a* finite *set and*

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

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 $i \in I$

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

and

$$D = \sum a_i b_i \mathrm{div}(f_i), b_i \in \mathbb{Q}.$$

If $\mathrm{NS}(X) = \mathrm{Pic}(X)$ *then we can take all* $b_i = 1$.

Proof. — We have a diagram

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

The group Λ is finitely generated and its image in $\mathrm{NS}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X)$ has the same rank as Λ (since $\mathrm{Pic}^0(X)$ is a torsion group):

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

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, if $\varphi_\ell(D) = 0$, we can find a representation

$$D = \sum_i a_i \mathrm{div}(f_i^{b_i}),$$

with $b_i \in= \mathbb{Q}$ and $a_i \in \mathbb{Z}_\ell$, linearly independent over $\mathbb{Z}$ (passing to a subset of I, if necessary). □

COROLLARY 12.9. — *There is an exact sequence*

$$1 \to K^*/k^* \otimes \mathbb{Z}_\ell \to \mathcal{FS}_X(K) \to \mathrm{Pic}^0(X)[\ell] \to 1$$

where $\mathrm{Pic}^0(X)[\ell] \subset \mathrm{Pic}^0(X)$ *is the* ℓ*-power torsion subgroup.*

Proof. — If suffices to recall that elements in $\mathrm{Pic}^0(X)[\ell]$, are represented, in our description, by elements f^{1/ℓ^n}, for some $n \in \mathbb{N}$, which define unramified ℓ-power cyclic covering of a model X. □

Lemma 12.7 and Lemma 12.8 allow us to define $\mathcal{FS}_X(K)$ intrinsically. Namely, for every

$$\bar{f} \in \mathcal{FS}(K)/\ell = K^*/\ell = \hat{K}^*/\ell$$

denote by $F_{\bar{f}} \subset \mathcal{FS}(K)$ the group $\mathbb{Z}_\ell$-generated by $(\hat{f}/\hat{f}')^{1/\ell}$, where $\hat{f}$ and $\hat{f}'$ are elements which have nontrivial commutators and which both reduce to $\bar{f}$ modulo ℓ. Then define

$$\mathcal{FS}_0(K) = \cap_{\bar{f} \in K^*/\ell} F_{\bar{f}}.$$

Note that for all $\bar{f} \in \mathcal{F}(K)/\ell$ and every model X of K one has

$$F_{\bar{f}} \subset \mathcal{FS}_X(K).$$

Lemma 12.8 implies that, conversely

$$\mathcal{FS}_X(K) \subset F_{\bar{f}},$$

for every $\bar{f}$. In particular, for every $f \in \mathcal{F}(K)$, with $\bar{f} = f \mod \ell$, both sets coincide. Therefore,

$$\mathcal{FS}_0(K) = \mathcal{FS}_X(K), \tag{12.2}$$

for all models X.

Moreover, notice that elements in $K^*/k^* \otimes \mathbb{Z}_\ell \subset \mathcal{FS}_X(K)$ are Galois-theoretically characterized as elements whose projection to $\mathrm{Pic}^0(X)$ is trivial.

As a group, $K^*/k^* \otimes \mathbb{Z}_\ell$ is generated by elements whose ν-values (for $\nu \in \mathcal{DV}_K$) are not all divisible by ℓ.

13. ℓ-adic analysis: curves

In this section we begin the process 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 13.1. — *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*

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

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

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}_\ell(\Delta_{C(\tilde{k})}) \arrow[r] & \mathcal{M}(C(\tilde{k})) \arrow[r] & \mathcal{G}^a_E \arrow[r] \arrow[d] & \mathbb{Z}_\ell^{2\mathrm{g}} \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{Z}_\ell(\Delta_{\mathbb{P}^1(k)}) \arrow[r] & \mathcal{M}(\mathbb{P}^1(k)) \arrow[r] & \mathcal{G}^a_{k(\mathbb{P}^1)} \arrow[r] & 0 &
\end{tikzcd}$$

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

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

where $a \in \mathbb{Z}_\ell^*$. □

14. 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 11.1 .

PROPOSITION 14.1. — *Let $\hat{f}, \hat{g} \in \mathcal{FS}_0(K)$ be such that*

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

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

Proof. — By Lemma 12.8,

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

where

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

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 $D \in \mathrm{supp}(\hat{f}) \cup \mathrm{supp}(\hat{g})$. By assumption, if $D \in \mathrm{supp}(\hat{f})$ then $D \notin \mathrm{supp}(\hat{g})$ (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 $\mathbb{Q}$ 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 11.1, all f_i, g_j belong to the same 1-dimensional field $E \subset K$ and hence $\hat{f}, \hat{g} \in \hat{E}^*$. □

REMARK 14.2. — 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 14.1.

PROPOSITION 14.3. — *Let $\mathfrak{K}^* \subset \mathcal{FS}_0(K) \subset \hat{K}^*$ 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*

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

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

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 $\mathcal{I}^a_{\nu_0}$ 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 $E' = k(x')$ and $E'' = k(x'')$. □

COROLLARY 14.4. — *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 3.10 and Definition 4.7).

LEMMA 14.5. — *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 3.19 and 14.3. 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. □

COROLLARY 14.6 (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 10.1 and Lemma 10.2 give a Galois-theoretic characterization of the notion "support in 2 points". By Corollary 14.4 we can Galois-theoretically distinguish zeroes and poles of $y \in \mathfrak{K}^*/k^*$. It remains to apply Lemma 14.5. □

15. 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 $\neq \ell$, 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 have $\Sigma_K^{\mathrm{div}} = \Sigma_L^{\mathrm{div}}$ and 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 $\sigma \in \Sigma_K^{\mathrm{div}} \subset \Sigma_K$ 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). 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 10.3).

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 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 12.7 we show that many 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, we prove that

$$\mathcal{FS}_0(K) = K^*/k^* \otimes \mathbb{Z}_\ell = L^*/l^* \otimes \mathbb{Z}_\ell$$

(up to an ℓ-torsion group related to $\mathrm{Pic}^0(X)$, for some model X of K), where $\mathcal{FS}_0(K) \subset \mathcal{FS}(K) \subset \hat{K}^*$ has an intrinsic Galois-theoretic description.

Step 6. For every pair of elements $\hat{f}, \hat{g} \in \mathcal{FS}_0(K)$ 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 14.1).

Step 7. Proposition 13.1 identifies E^*/k^* inside $\hat{E}^*$, up to conformal equivalence, for all one-dimensional $E = k(x)$, which are integrally closed in K.

Step 8. Proposition 14.3 identifies $\mathfrak{K}^* := K^*/k^* \cap L^*/l^*$ (as a multiplicative group) with a multiplicative subgroup of $K^*/k^* \otimes \mathbb{Z}_{(\ell)}$.

Step 9. By Proposition 3.19, $\mathfrak{K}^*$ is isomorphic to K_1^*/k^*, and L_1^*/l^*, where K_1/K and L_1/L are finite purely inseparable extensions. Therefore, $\mathfrak{K}^*$ carries two structures of an abstract projective space compatible with the multiplicative structure (see Example 4.5).

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

Step 11. Lemma 14.5 and Corollary 14.6 give a Galois-theoretic characterization of generating elements and primary lines in $\mathfrak{K}^*$. These define a (unique) partial projective structure on $\mathfrak{K}^*$ (in particular, the projective structures induced by $\mathbb{P}(K_1)$ and $\mathbb{P}(L_1)$ coincide). In particular, the fields K_1 and L_1 both contain k and are isomorphic.

Step 12. If follows that K and L 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] 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.