RECONSTRUCTING FUNCTION FIELDS FROM MILNOR K-THEORY

ANNA CADORET AND ALENA PIRUTKA

Abstract. Let F be a finitely generated regular field extension of transcendence degree ≥ 2 over a perfect field k. We show that the multiplicative group $F^\times/k^\times$ endowed with the equivalence relation induced by algebraic dependence on F over k determines the isomorphism class of F in a functorial way. As a special case of this result, we obtain that the isomorphism class of the graded Milnor K-ring $K_*^M(F)$ determines the isomorphism class of F, when k is algebraically closed or finite.

1. Introduction

This paper is motivated by the following general question.

Question 1. Does the Milnor K-ring $K_*^M(F)$ determine the isomorphism class of the field F?

One may also ask whether or not the above holds in a functorial way, that is, whether or not the Milnor K-ring functor is fully faithfull from the groupoid[1] of fields to the groupoid of $\mathbb{Z}_{\geq 0}$-graded rings.

Question 1 has a negative answer in general. For instance[2], all solvably closed subfields of $\overline{\mathbb{Q}}$ have isomorphic Milnor K-rings. Indeed, let F_1, F_2 be two such fields. To show that $K_*^M(F_1) \simeq K_*^M(F_2)$ it is enough to show that $K_j^M(F_1) \simeq K_j^M(F_2)$, $j = 1, 2$ compatibly with the pairings $\{-,-\} : K_1^M(F_i) \otimes K_1^M(F_i) \to K_2^M(F_i)$, $i = 1, 2$ (See Remark 12). Since every polynomial $T^n - x \in F_i[T]$ is totally split by assumption, $K_2^M(F_i)$ is uniquely divisible torsion-free [2, I, (1.2)]. On the other hand, since $K_2^M(F_i)$ is a quotient of the inductive limit of the $K_2^M(F)$, for $\mathbb{Q} \subset F \subset F_i$ describing the set of all finite field subextensions of $F_i|\mathbb{Q}$ and that $K_2^M(F)$ is an extension of a torsion abelian group by a finitely generated abelian group [2, II, (1.2)], $K_2^M(F_i)$ is trivial. So it is enough to show that $F_1^\times \simeq F_2^\times$. Since $F_i^\times$ is divisible countable, $F_i^\times \simeq (F_i^\times)_{tors} \oplus \mathbb{Q}^{\mathbb{Z}}$ and the assertion follows from $(F_1^\times)_{tors} \simeq (F_2^\times)_{tors} \simeq (\overline{\mathbb{Q}}^\times)_{tors}$.

Also, even when restricted to a class of fields where Question 1 has a positive answer, the naive functorial version of Question 1 still has a negative answer in general, as shown by the example of finite fields F where $K_*^M(F)$ has extra automorphisms induced by $x \to x^u$ for u prime to $|F| - 1$ on $K_1^M(F)$. To get a viable functorial version of Question 1, one should at least kill such extra automorphisms.

Since $K_1^M(F) = F^\times$, Question 1 essentially reduces to reconstructing the additive structure of F from the multiplicative group $F^\times$ endowed with additional data that can be detected by the Milnor

Date: Article submitted on 2018/09/18. Reports received on 2019/07/19. Article resubmitted on 2019/08/28.

[1]Here, given a category $\mathcal{C}$, the groupoid of $\mathcal{C}$ means the category with the same objects as $\mathcal{C}$ and with morphisms the isomorphisms in $\mathcal{C}$.

[2]This counter-example was suggested to us by one of the Referees.

K-ring. Our main result (Theorem 4) asserts that for a finitely generated regular field extension F of transcendence degree ≥ 2 over a perfect field k, the multiplicative group $F^\times/k^\times$ endowed with the equivalence relation induced by algebraic dependence on F over k determines the isomorphism class of F in a functorial way. In Section 2, we show (Theorem 7) that for a finitely generated regular field extension of a field k which is either algebraically closed or finite, the Milnor K-ring detects algebraic dependence. This is a consequence of deep K-theoretic results - the $n = 2$ case of the Bloch-Kato conjecture [12] when k is algebraically closed and of the Bass-Tate conjecture [15] when k is finite. Combined with Theorem 4, this enables us to show that the Milnor K-ring modulo the ideal of divisible elements (resp. of torsion elements) determines in a functorial way finitely generated regular field extensions of transcendence degree ≥ 2 over algebraically closed fields (resp. over finite fields) (see Corollary 10). In particular, this provides a purely K-theoretic description of the group of birational automorphisms of normal projective varieties of dimension ≥ 2 over algebraically closed or finite fields (Corollary 11).

1.1. **Main Result.** Recall that a field extension $F|k$ is *regular* if k is algebraically closed in F and $F|k$ has a separating transcendence basis. If k is perfect, the latter condition is automatic. Let $F|k$ be a regular field extension.

Definition 2. We say that $\overline{x}, \overline{y} \in F^\times/k^\times$ are algebraically dependent and write $\overline{x} \equiv \overline{y}$ if some (equivalenty, every) lifts $x, y \in F^\times$ of $\overline{x}, \overline{y} \in F^\times/k^\times$ are algebraically dependent over k. The relation $\equiv$ is an equivalence relation on $F^\times/k^\times$.

Note that, as $F|k$ is regular, if $\overline{x}, \overline{y} \in F^\times/k^\times$ are algebraically dependent then either $\overline{x} = \overline{y} = 1$ or $1 \neq \overline{x}, \overline{y}$.

Let $F|k$, $F'|k'$ be regular field extensions.

Definition 3. We say that a group morphism $\overline{\psi} : F^\times/k^\times \to F'^\times/k'^\times$ *preserves algebraic dependence* if for every $\overline{x}, \overline{y} \in F^\times/k^\times$ the following holds: $\overline{x} \equiv \overline{y}$ if and only if $\overline{\psi}(\overline{x}) \equiv \overline{\psi}(\overline{y})$.

(In particular, a group morphism preserving algebraic dependence is automatically injective).

For a subfield $E \subset F$, write $\overline{E^F} \subset F$ for the algebraic closure of E in F. Then a group morphism $\overline{\psi} : F^\times/k^\times \to F'^\times/k'^\times$ preserves algebraic dependence if and only if $\overline{k(x)^F}^\times/k^\times = \overline{\psi}^{-1}(\overline{k'(\psi(x))^{F'}}/k'^\times)$ for every $x \in F$ and some (equivalently, every) lift $\psi(x) \in F'$ of $\overline{\psi}(\overline{x})$.

Let $\mathrm{Isom}(F, F')$ denote the set of field isomorphisms $F\tilde{\to}F'$ and

$$\mathrm{Isom}(F|k, F'|k') \subset \mathrm{Isom}(F, F')$$

denote the subset of isomorphisms $F\tilde{\to}F'$ inducing field isomorphisms $k\tilde{\to}k'$.

Let $\mathrm{Isom}(F^\times/k^\times, F'^\times/k'^\times)$ denote the set of group isomorphisms $F^\times/k^\times\tilde{\to}F'^\times/k'^\times$ and

$$\mathrm{Isom}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times) \subset \mathrm{Isom}(F^\times/k^\times, F'^\times/k'^\times)$$

the subset of isomorphisms $F^\times/k^\times\tilde{\to}F'^\times/k'^\times$ preserving algebraic dependence. The group $\mathbb{Z}/2$ acts on the set $\mathrm{Isom}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times)$ by $\overline{\psi} \to \overline{\psi}^{-1}$. Write

$$\overline{\mathrm{Isom}}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times)$$

for the resulting quotient.

Theorem 4. *Let k, k' be perfect fields of the same characteristic $p \geq 0$, and let $F|k$, $F'|k'$ be finitely generated regular field extensions and assume one of them has transcendence degree ≥ 2. Then the canonical map*

$$\mathrm{Isom}(F|k, F'|k') \to \overline{\mathrm{Isom}}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times)$$

is bijective.

1.2. **Comparison with existing results.** Question 1 was considered by Bogomolov and Tschinkel in [3], where they prove (a variant of) Theorem 4 for finitely generated regular extensions of characteristic 0 fields ([3, Thm. 2]) and deduce from it Corollary 10 for finitely generated field extensions of algebraically closed fields of characteristic 0 ([3, Thm. 4]).

Variants of our results were also obtained by Topaz from a smaller amount of K-theoretic information - mod-ℓ Milnor K-rings (for finitely generated field extensions of transcendence degree ≥ 5 over algebraically closed field of characteristic $p \neq \ell$ [16, Thm. B]) and rational Milnor K-rings (for finitely generated field extensions of transcendence degree ≥ 2 over algebraically closed field of characteristic 0 [17, Thm. 6.1]) but enriched with the additional data of the so-called "rational quotients" of $F|k$. See also [17, Rem. 6.2] for some cases where the additional data of rational quotients can be removed.

Our strategy follows the one of Bogomolov and Tschinkel in [3], where the key idea is to parametrize lines in $F^\times/k^\times$ as intersections of multiplicatively shifted (infinite dimensional) projective subspaces of a specific form arising from relatively algebraically closed subextensions of transcendence degree 1. See Subsection 1.3 for details. The strategy of Topaz is more sophisticated and goes through the reconstruction of the quasi-divisorial valuations of F *via* avatars of the theory of commuting-liftable pairs as developped in the framework of birational anabelian geometry. Though not explicitly stated in the literature, it is likely that Theorem 4 and Corollary 10 for finitely generated field extensions of algebraically closed fields of characteristic $p > 0$ could also be recovered from the techniques of birational anabelian geometry as developed by Bogomolov-Tschinkel [4], Pop (*e.g.* [14], [13]) and Topaz.

To our knowledge, Theorem 4 for finitely generated regular extensions of perfect fields of characteristic $p > 0$ and Corollary 10 for finitely generated field extensions of finite fields are new.

1.3. **Strategy of proof.** For simplicity, write $F^p \subset F$ for the subfield generated by k and the x^p, $x \in F$ and $F^\times/p := F^\times/F^{p\times}$.

The proof of Theorem 4 is carried out in Section 3. According to the fundamental theorem of projective geometry (see Lemma 29, for which we give a self-contained proof in the setting of possibly infinite field extensions), it would be enough to show that a group isomorphism $\overline{\psi} : F^\times/k^\times \tilde{\to} F'^\times/k'^\times$ preserving algebraic dependence induces a bijection from lines in $F^\times/k^\times$ to lines in $F'^\times/k'^\times$. This would reduce the problem to describing lines in $F^\times/k^\times$ using only $\equiv$ and the multiplicative structure of $F^\times/k^\times$. This classical approach works well if $p = 0$. The key observation of Bogomolov and Tschinkel in [3] is that every line can be multiplicatively shifted to a line passing through a "good" pair of points and that those lines can be uniquely parametrized as intersections of multiplicatively shifted (infinite dimensional) projective subspaces of a specific form arising from relatively algebraically closed subextensions of transcendence degree 1 [3, Thm. 22]. This is the output of elaborate computations in [3]. Later, Rovinsky suggested an alternative argument using differential forms; this is sketched in [4, Prop. 9].

When $p > 0$, the situation is more involved. The original computations of [3] fail due to inseparability phenomena. Instead, we adjust the notion of "good" for the pair of points (Definition 19) in order to refine the argument of Rovinsky. In particular, we use the field-theoretic notion of "regular" element rather than the group-theoretic notion of "primitive" element used in [3]. To show that every line can be shifted to a line whose image contains a "good" pair of points (Lemma 20), one can invoke Bertini theorems ([7, Cor. 6.11.3] when k is infinite and [5, Thm. 1.6] when k is finite); we also give an alternative, more elementary argument due to Akio Tamagawa in Remark 22. This reduces the problem to show that $\overline{\psi}$ (or $\overline{\psi}^{-1}$) maps every line in $F^\times/k^\times$ whose image contains a good pair of points $(\overline{x}_1, \overline{x}_2)$ isomorphically to a line in $F'^\times/k'^\times$. Actually, we cannot prove this directly when $p > 0$. The issue is that, when $p > 0$, the Bogomolov-Tschinkel parametrization of such line by the set $\mathfrak{I}(\overline{x}_1, \overline{x}_2)$ introduced in Subsection 3.2 is much rougher than in [3, Thm. 22]. More precisely, when $p > 0$, the set $\mathfrak{I}(\overline{x}_1, \overline{x}_2)$ only recovers the line passing through $(\overline{x}_1, \overline{x}_2)$ up to prime-to-p powers and certain affine transformations with F^p-coefficients (Lemma 23); this is due to the apparition of constants in F^p when one integrates differentials forms. Lemma 23 is however enough to show that there exists a unique $m \in \mathbb{Z}$ normalized as

$$\begin{array}{ll} |m| = 1 & \text{if } p = 0, 2 \\ 1 \leq |m| \leq \frac{p-1}{2} & \text{if } p > 2; \end{array} \tag{1.1}$$

such that $\overline{\psi}^m$ induces a bijection from lines in $F^\times/p$ to lines in $F'^\times/p$ (Proposition 27). So Lemma 29 gives a unique field isomorphism $\phi : F \tilde{\rightarrow} F'$ such that the resulting isomorphism of groups $\phi : F^\times \tilde{\rightarrow} F'^\times$ coincides with $\overline{\psi}^m$ on $F^\times/p$. This concludes the proof if $p = 0$. But if $p > 0$, the extension F/F^p is much smaller (finite-dimensional!) and one has to perform an additional descent step (Section 3.6) to show that $m = \pm 1$ and ϕ coincides with $\overline{\psi}^{\pm 1}$ on $F^\times/k^\times$ (not only on $F^\times/p$).

We limited our exposition to function fields, which are those of central interest in algebraic geometry. However, some of our results extend to more exotic fields provided they behave like function fields. For instance, Theorem 4 works for the class of regular field extensions F of transcendence degree ≥ 2 over a perfect field k such that for every subfield $k \subset E \subset F$ of transcendence degree 2 over k, the algebraic closure of E in F is a finite extension of E. We do not elaborate on this.

1.4. **Acknowledgements.** We would like to thank heartfully the referees for their thorough and constructive reports. They pointed out several minor but mathematical inacurracies and made suggestions that helped improve a lot the exposition. The first author was partially supported by the I.U.F. and the ANR grant ANR-15-CE40-0002-01. The second author was partially supported by NSF grant DMS-1601680 and by the Laboratory of Mirror Symmetry NRU HSE, RF Government grant, ag. no. 14.641.31.0001. This project was initiated at the occasion of a working group on geometric birational anabelian geometry at the Courant Institute of Mathematics, NYU. The authors would like to thank F. Bogomolov and Y. Tschinkel for inspiring exchanges, B. Kahn for his explanations concerning the Bass-Tate conjecture and A. Merkurjev, M. Morrow and A. Tamagawa for helpful remarks on a first version of this text. They also thank A. Tamagawa for suggesting the more elementary proof of Lemma 20 presented in Remark 22.

2. Milnor K-rings and algebraic dependence

For a field F, the Milnor K-ring $K_*^M(F)$ is the quotient of the $\mathbb{Z}_{\geq 0}$-graded ring $T^{\otimes *}(F^\times) := \oplus_{n\geq 0}(F^\times)^{\otimes n}$ (with the convention $(F^\times)^{\otimes 0} = \mathbb{Z}$) by the two-sided homogeneous ideal generated by the degree-2 elements $a \otimes (1-a)$, $1 \neq a \in F^\times$. The map $F \to K_*^M(F)$ defines a functor from the groupoids $\mathcal{F}$ of fields to the groupoid $\mathcal{A}$ of associative $\mathbb{Z}_{\geq 0}$-graded anti-commutative rings.

Given a field F and elements $x_1, \dots, x_n \in F^\times$, we write $\{x_1, \dots, x_n\} \in K_n^M(F)$ for the image of $x_1 \otimes \cdots \otimes x_n \in T^{\otimes n}(F^\times)$. Recall (*e.g.* [2, §4]) that given a discrete valuation $v : F^\times \to \mathbb{Z}$ on F, with ring of integers $\mathcal{O}_v$ and residue field $k(v)$ there exists a unique group morphism $\partial_v^* : K_*^M(F) \to K_{*-1}^M(k(v))$ such that for every $x_1 \in F^\times$ and $x_2, \dots, x_n \in \mathcal{O}_v^\times$ with images $\overline{x}_2, \dots, \overline{x}_n$ in $k(v)$,

$$\partial_v^n(\{x_1, x_2, \dots, x_n\}) = \pm v(x_1)\{\overline{x}_2, \dots, \overline{x}_n\} = \pm\{\overline{x}_2^{v(x_1)}, \overline{x}_3, \dots, \overline{x}_n\}.$$

For $p = 0$ or a prime, let $\mathcal{F}_p \subset \mathcal{F}$ denote the full subcategory of fields of characteristic p.

2.1. **Some geometric observations.** Let $F|k$ be a finitely generated regular field extension.

2.1.1. Let $x_1, \dots, x_n \in F$ be such that $k(x_1, \dots, x_n)$ has transcendence degree n over k. Then

Lemma 5. *There exists a divisorial valuation $v : F^\times \to \mathbb{Z}$ of F such that*
- *$v(x_1) \neq 0$, $v(x_2) = \cdots = v(x_n) = 0$;*
- *the images $\overline{x}_2, \dots, \overline{x}_n$ of $x_2, \dots, x_n$ in the residue field $k(v)$ are algebraically independent over k.*

Proof. Fix a normal projective model $X|k$ of $F|k$. Each x_i defines a dominant rational function $x_i : X \dashrightarrow \mathbb{P}_k^1$ such that

$$\underline{x} = (x_1, \dots, x_n) : X \dashrightarrow (\mathbb{P}_k^1)^n$$

is again dominant. Choose any open subscheme $U \subset X$ over which the map $\underline{x} : U \to (\mathbb{P}_k^1)^n$ is defined. Then, up to replacing X by the normalization of the Zariski closure of the graph of $\underline{x}|_U$ in $X \times (\mathbb{P}_k^1)^n$, one may assume that the maps x_i, $i = 1, \dots, n$ and $\underline{x}$ are defined over X, and surjective. Choose an irreducible divisor $D \in Div(X)$ with $v_D(x_1) \neq 0$. Then (since $\underline{x}(D)$ has codimension at most 1 in $(\mathbb{P}_k^1)^n$) the restriction $\underline{x}|_D : D \to (\mathbb{P}_k^1)^n$ surjects onto $0 \times (\mathbb{P}_k^1)^{n-1} \subset (\mathbb{P}_k^1)^n$; in particular the elements $\overline{x}_i := x_i|_D \in k(D)$, $i = 2, \dots, n$ remain algebraically independent over k and $v_D(x_i) = 0$, $i = 2, \dots, n$. □

2.1.2. The abelian group $F^\times/k^\times$ is a free abelian group since it embeds into a free abelian group. This follows from the exact sequence

$$0 \to k^\times \to F^\times \to Div(X),$$

where $X|k$ is any normal projective model $X|k$ of $F|k$, and the fact that $Div(X)$ is a free abelian group.

2.2. **Type.** We say that a field F is a function field over a field k (or with field of constants k) if F is a finitely generated regular field extension of transcendence degree ≥ 1 over k. We say that a function field F over k is of type 1 (resp. of type 2) if k is algebraically closed (resp. finite), in which case k is uniquely determined by F (see Lemma 6 below).

Let $\widetilde{\mathcal{F}} \subset \mathcal{F}$, $\widetilde{\mathcal{F}}_p \subset \mathcal{F}_p$ denote the full subcategories of function fields which are of types 1 and 2.

Lemma 6. *For $F \in \widetilde{\mathcal{F}}$, the type, the multiplicative group $k^\times$ of the field of constants and the characteristic p of F are determined by $F^\times = K_1^M(F)$ as follows.*

Type	*Torsion subgroup of* $F^\times$	$k^\times$	p
1	*Infinite*	*Divisible subgroup of* $F^\times$	0 *or unique* p *such that* $(-)^p : k^\times \to k^\times$ *is an isomorphism*
2	*Finite*	*Torsion subgroup of* $F^\times$	*Unique* p *such that* $\log(\|k^\times\|+1) \in \mathbb{Z}\log(p)$

In the following, we sometimes write $F|k \in \widetilde{\mathcal{F}}$ instead of $F \in \widetilde{\mathcal{F}}$ implicitly meaning that k is the field of constants of F.

2.3. **Detecting algebraic dependence.** For $F \in \mathcal{F}_p$ and a prime $\ell \neq p$, let $DK_*^M(F) \subset K_*^M(F)$ (resp. $TK_*^M(F) \subset K_*^M(F)$) denote the (two-sided) ideal of elements which are infinitely ℓ-divisible (resp. torsion) with respect to the $\mathbb{Z}$-module structure on $K_*^M(F)$ and write

$$\overline{K}_*^{1,M}(F) := K_*^M(F)/DK_*^M(F);$$
$$\overline{K}_*^{2,M}(F) := K_*^M(F)/TK_*^M(F).$$

Then $K_*^M \to \overline{K}_*^{i,M}$ is a morphism of functors from $\mathcal{F}$ to $\mathcal{A}$, $i = 1, 2$.

Theorem 7. *For $F \in \widetilde{\mathcal{F}}_p$ of type i and every $x_1, \ldots, x_n \in F^\times$ consider the following assertions.*

(a) $\{x_1, \ldots, x_n\} = 0$ in $\overline{K}_n^{i,M}(F)$;

(b) the transcendence degree of $k(x_1, \ldots, x_n)$ over k is $\leq n-1$.

Then, (a) $\Rightarrow$ (b) and (b) $\Rightarrow$ (a) if $i = 1$ or if $i = 2$ and $n \leq 2$.

Proof. The assertion for $n = 1$ follows from 2.1.2.

(a) $\Rightarrow$ (b): We proceed by induction on n. Assume $k(x_1, \ldots, x_n)$ has transcendence degree n over k and choose a place v of F as in Lemma 5. By induction hypothesis $\partial_v^n(\{x_1, \ldots, x_n\}) = \pm\{\overline{x}_2^{v(x_1)}, \overline{x}_3, \ldots, \overline{x}_n\} \neq 0$ in $\overline{K}_{n-1}^{i,M}(k(v))$ hence, *a fortiori*, $\{x_1, \ldots, x_n\} \neq 0$ in $\overline{K}_n^{i,M}(F)$.

(b) $\Rightarrow$ (a): Assume $E = k(x_1, \ldots, x_n)$ has transcendence degree $d \leq n-1$ over k. Since $\{x_1, \ldots, x_n\}$ lies in the image of the restriction map $\overline{K}_n^{i,M}(E) \to \overline{K}_n^{i,M}(F)$, it is enough to show that $\overline{K}_n^{i,M}(E) = 0$. If F is of type 1, this follows from Tsen's theorem [9], which ensures that the étale cohomology group $H^n(E, \mathbb{Z}_\ell(n))$ is trivial and from the Bloch-Kato conjecture [18, 19]. If F is of type 2, this follows from the $n = 2$ case of the Bass-Tate conjecture [15, Thm. 1]. □

Let $F, F' \in \widetilde{\mathcal{F}}_p$ of the same type i. For a morphism $\overline{\psi}_* : \overline{K}_*^{i,M}(F) \to \overline{K}_*^{i,M}(F')$ of $\mathbb{Z}_{\geq 0}$-graded rings and integer $n \geq 1$, consider the assertions:

$(\subset, n)$ For every $x_1, \ldots, x_n \in F^\times$, $\overline{\psi}_1(\overline{k(x_1, \ldots, x_n)^F}^\times/k^\times) \subset \overline{k'(\psi_1(x_1), \ldots, \psi_1(x_n))^{F'}}^\times/k'^\times$

$(=, n)$ For every $x_1, \ldots, x_n \in F^\times$, $\overline{\psi}_1(\overline{k(x_1, \ldots, x_n)^F}^\times/k^\times) = \overline{k'(\psi_1(x_1), \ldots, \psi_1(x_n))^{F'}}^\times/k'^\times$

where $\psi_1 : F^\times \to F'^\times$ denotes any set-theoretic lift of $\overline{\psi}_1$.

Corollary 8. *If $\overline{\psi}_*$ is injective in degree $\leq n+1$ (resp. an isomorphism), Assertion $(\subset, n)$ (resp. $(=, n)$) holds for every n if $i = 1$ and for $n \leq 1$ if $i = 2$.*

Proof. The second part of Corollary 8 follows from the first part (applied to $\overline{\psi}_*$ and $\overline{\psi}_*^{-1}$). We prove the first part. An element $x \in F$ is algebraic over $k(x_1, \ldots, x_n)$ if and only if there exists a subset $I \subset \{1, \ldots, n\}$ such that $k(x_i|i \in I)$ and $k(x_i|i \in I, x)$ both have transcendence degree $|I|$ over k. Assume $i = 1$ and $n \geq 1$ is arbitrary or $i = 2$ and $n \leq 1$. Then, from Theorem 7, the condition that $k(x_i|i \in I)$ and $k(x_i|i \in I, x)$ both have transcendence degree $|I|$ over k is equivalent to $\{x_i|i \in I\} \neq 0$ in $\overline{K}^{i,M}_{|I|}(F)$ and $\{x_i|i \in I, x\} = 0$ in $\overline{K}^{i,M}_{|I|+1}(F)$. Since $\overline{\psi}_* : \overline{K}^{i,M}_*(F) \to \overline{K}^{i,M}_*(F')$ is injective, $\{x_i|i \in I\} \neq 0$ in $\overline{K}^{i,M}_{|I|}(F)$ and $\{x_i|i \in I, x\} = 0$ in $\overline{K}^{i,M}_{|I|+1}(F)$ in turn implies $\{\psi_1(x_i)|i \in I\} \neq 0$ in $\overline{K}^{i,M}_{|I|}(F')$ and $\{\psi_1(x_i)|i \in I, \psi_1(x)\} = 0$ in $\overline{K}^{i,M}_{|I|+1}(F')$. Applying again Theorem 7 yields the conclusion. □

Remark 9.
- When F is of type 2 the implication (b) ⇒ (a) of Theorem 7 and the second part of Corollary 8 for every n are predicted by the Bass-Tate conjecture in positive characteristic [2, Question, p.390]. See also [8] for the relation between the Bass-Tate conjecture in positive characteristic and classical motivic conjectures.
- For our applications, we only need the $n = 1$ cases of Corollary 8 (*viz* the $n = 2$ case of Theorem 7). In particular, for function fields of type 1, we only need the $n = 2$ case of the Bloch-Kato conjecture, an earlier theorem of Merkurjev and Suslin [12].

2.4. **Reconstructing function fields.** The $n = 1$ case of Corollary 8 implies that for $i = 1, 2$ and for every $F, F' \in \widetilde{\mathcal{F}}_p$ of type i and isomorphism $\overline{\psi}_* : \overline{K}^{i,M}_*(F) \to \overline{K}^{i,M}_*(F')$ of $\mathbb{Z}_{\geq 0}$-graded rings the induced isomorphism of multiplicative groups $\overline{\psi}_1$ preserves algebraic dependence. This implies the following. For $i = 1, 2$, let

$$\mathrm{Isom}(\overline{K}^{i,M}_*(F), \overline{K}^{M}_*(F'))$$

denote the set of isomorphisms of $\mathbb{Z}$-graded rings $\overline{K}^{i,M}_*(F) \tilde{\to} \overline{K}^{i,M}_*(F')$ and

$$\overline{\mathrm{Isom}}(\overline{K}^{i,M}_*(F), \overline{K}^{i,M}_*(F'))$$

their quotients by the natural action of $\mathbb{Z}/2$.

Corollary 10. *Let $F, F' \in \tilde{\mathcal{F}}$. Then*

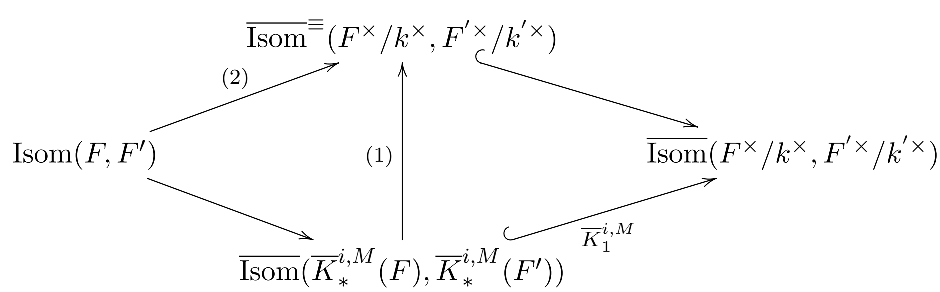
(a) $\mathrm{Isom}(K^M_*(F), K^M_*(F')) \neq \emptyset$ only if F, F' are of the same type i and characteristic p.

(b) If $F, F' \in \tilde{\mathcal{F}}_p$ are of the same type i and have transcendence degree ≥ 2 over their fields of constants then the natural functorial map

$$\mathrm{Isom}(F, F') \to \overline{\mathrm{Isom}}(\overline{K}^{i,M}_*(F), \overline{K}^{i,M}_*(F'))$$

is bijective.

Proof. Part (a) follows from Lemma 6. For Part (b), one has a canonical commutative diagram



where the factorization (1) follows from Corollary 8. So the conclusion follows from the fact that ($\overline{K}_1^{i,M}$ - hence (1) - is injective and) the map (2) is bijective by Theorem 4. □

Corollary 11. *Let $F \in \tilde{\mathcal{F}}$ of type i. Then one has the following group isomorphisms*

$$\mathrm{Aut}(F)\tilde{\to}\overline{\mathrm{Aut}}^{\equiv}(F^\times/k^\times)\tilde{\to}\overline{\mathrm{Aut}}(\overline{K}_*^{i,M}(F))$$

Remark 12. Since $\overline{K}_*^{i,M}(F)$ is a quadratic algebra it is entirely determined by $\overline{K}_{\leq 2}^{i,M}(F)$ (for $i = 1$, one can even replace $\overline{K}_2^{1,M}(F)$ with its ℓ-adic completion $H^2(F, \mathbb{Z}_\ell(2))$). In particular, in Corollary 10, one could replace $\mathrm{Isom}(K_*^M(F), K_*^M(F'))$ by the set of group isomorphisms $\overline{\psi}_{\leq 2}$: $\overline{K}_{\leq 2}^{i,M}(F)\tilde{\to}\overline{K}_{\leq 2}^{i,M}(F')$ such that $\overline{\psi}_2(\{x_1, x_2\}) = \{\overline{\psi}_1(x_1), \overline{\psi}_1(x_2)\}$.

Remark 13. From Lemma 6, one can reconstruct the field of constants k of a function field F in $\tilde{\mathcal{F}}$ from $K_1^M(F)$. In general, one may ask for a relative version of Corollary 10 that is replacing the functor $K_*^M(-)$ with the functor sending a finitely generated field extension F of a perfect field k to the morphism $K_*^M(k) \to K_*^M(F)$.

The remaining part of the paper is devoted to the proof of Theorem 4.

3. Proof of Theorem 4

3.1. **Recollection on differentials.**

We will use repeatedly the following classical facts about differentials.

Lemma 14. *For $x_1, \dots, x_n \in F$, the following are equivalent*

- *$x_1, \dots, x_n \in F$ is a separating transcendence basis for $F|k$ (i.e. $F|k(x_1, \dots, x_n)$ is a finite separable field extension);*
- *$dx_1, \dots, dx_n \in \Omega^1_{F|k}$ is an F-basis of $\Omega^1_{F|k}$.*

If $p > 0$, these are also equivalent to

- *$x_1, \dots, x_n \in F$ is a p-basis of $F|k$.*

See *e.g* [11, §27, Thm 59; §38, Thm. 86] for the proof. Recall that since k is a perfect field, the extension $F|k$ always admits a separating transcendence basis, and that if $p = 0$, every transcendence basis is separating.

Corollary 15. $\ker(d : F \to \Omega^1_{F|k}) = F^p$.

In particular for every $x \in F$, the following are equivalent:

(a) $x \in F \setminus F^p$;
(b) $dx \neq 0$;
(c) x is a separating transcendence basis for $\overline{k(x)}^F|k$.

If $x \in F$ verifies the above equivalent conditions (a), (b), (c), for every $0 \neq f \in \overline{k(x)}^F$ there exists a unique $f' := f'(x) \in \overline{k(x)}^F$ such that $df = f'dx$.

3.2. **Notation and overview of the proof of Theorem 4.**

Let k be a perfect field of characteristic $p \geq 0$ and let $F|k$ be a finitely generated regular field extension of transcendence degree ≥ 2.

For every subfield $k \subset E \subset F$ and $x, y \in F^\times$ such that $\overline{x} \neq \overline{y} \in F^\times/E^\times$, write $\mathfrak{l}_E(x,y) := Ex + Ey \subset F$ (which by assumption is a 2-dimensional E-subspace) and

$$\mathfrak{l}_E(\overline{x},\overline{y}) = ((Ex+Ey)\cap F^\times)/E^\times \subset F^\times/E^\times$$

for the corresponding line in $F^\times/E^\times$.

Definition 16. We say that $\overline{x}, \overline{y} \in F^\times/p$ are *p-multiplicatively dependent* and write $\overline{x} \sim_p \overline{y}$ if either $\overline{x} = \overline{y} = 1$ or $\overline{x}, \overline{y} \neq 1$ and

$$\overline{x}^{\mathbb{Z}} \cap \overline{y}^{\mathbb{Z}} \neq 1$$

We say that $\overline{x}, \overline{y} \in F^\times/k^\times$ are *p-multiplicatively dependent* and write again $\overline{x} \sim_p \overline{y}$ if their images in $F^\times/p$ are p-multiplicatively dependent. The relations $\sim_p$ are equivalence relations on $F^\times/p$ and $F^\times/k^\times$.

Note that, if $p > 0$, $\overline{x} \sim_p \overline{y}$ if and only if $\overline{x}^{\mathbb{Z}} = \overline{y}^{\mathbb{Z}}$ in $F^\times/p$.

For $\overline{x}_1, \overline{x}_2, \overline{y}_1, \overline{y}_2 \in F^\times/k^\times$ and some (equivalently, every) lifts $x_1, x_2, y_1, y_2 \in F^\times$, write

$$\mathcal{I}(\overline{x}_1,\overline{x}_2,\overline{y}_1,\overline{y}_2) := (\overline{k(x_1/x_2)^F}^\times \cdot x_2) \bigcap (\overline{k(y_1/y_2)^F}^\times \cdot y_2)$$

and

$$\mathfrak{I}(\overline{x}_1,\overline{x}_2) = \bigcup_{y_1,y_2} \mathcal{I}(\overline{x}_1,\overline{x}_2,\overline{y}_1,\overline{y}_2)$$

where the union is over all $y_i \in \overline{k(x_i)^F}^\times$, $\overline{y}_i \not\sim_p \overline{x}_i, 1$, $i = 1, 2$.

Let $\overline{\mathcal{I}}(\overline{x}_1,\overline{x}_2,\overline{y}_1,\overline{y}_2)$, $\overline{\mathfrak{I}}(\overline{x}_1,\overline{x}_2)$ denote the images of $\mathcal{I}(\overline{x}_1,\overline{x}_2,\overline{y}_1,\overline{y}_2)$, $\mathfrak{I}(\overline{x}_1,\overline{x}_2)$ in $F^\times/k^\times$ respectively.

For every $\overline{I} \in \overline{\mathfrak{I}}(\overline{x}_1,\overline{x}_2)$ and $i = 1, 2$, set $\{i,j\} = \{1,2\}$ and let $\mathfrak{l}^\circ(\overline{I},\overline{x}_i)$ denote the set of all $y_i \in \overline{k(x_i)^F}^\times$, $\overline{y}_i \not\sim_p 1, \overline{x}_i$ such that for some (equivalently, every) lift $I \in F^\times$ of $\overline{I} \in F^\times/k^\times$, one has $I \in \overline{k(y_1/y_2)^F}^\times \cdot y_2$ for some $y_j \in \overline{k(x_j)^F}$, $\overline{y}_j \not\sim_p 1, \overline{x}_j$. Set also

$$\mathfrak{l}(\overline{I},\overline{x}_i) = \mathfrak{l}^\circ(\overline{I},\overline{x}_i) \cup \{x_i\}$$

and let $\overline{\mathfrak{l}}(\overline{I},\overline{x}_i)$ denote the image of $\mathfrak{l}(\overline{I},\overline{x}_i)$ in $F^\times/k^\times$.

3.2.1. Roughly, $\overline{\mathfrak{I}}(\overline{x}_1,\overline{x}_2)$ and $\overline{\mathfrak{l}}(\overline{I},\overline{x}_i)$, $i = 1, 2$ have to be regarded as approximations - defined only in terms of the multiplicative structure of $F^\times/k^\times$ and the relation $\equiv$ of algebraic dependence on F over k - of $\mathfrak{l}_k(\overline{x}_1,\overline{x}_2)$ and $\mathfrak{l}_k(1,\overline{x}_i)$, $i = 1, 2$ respectively. But actually $\overline{\mathfrak{I}}(\overline{x}_1,\overline{x}_2)$ and $\overline{\mathfrak{l}}(\overline{I},\overline{x}_i)$, $i = 1, 2$ do not distinguish lines from their 'inverse'. More precisely,

Lemma 17. *For every $\overline{x}_1, \overline{x}_2 \in F^\times/k^\times$ such that $\overline{x}_1, \overline{x}_2, \overline{x}_1/\overline{x}_2 \not\sim_p = 1$ and $\epsilon = \pm 1$, one has $\mathfrak{l}_k(\overline{x}_1^\epsilon, \overline{x}_2^\epsilon)^\epsilon \subset \overline{\mathfrak{I}}(\overline{x}_1,\overline{x}_2)$ and for every $\overline{I} \in \mathfrak{l}_k(\overline{x}_1^\epsilon,\overline{x}_2^\epsilon)^\epsilon$, $\overline{I} \neq \overline{x}_1^\epsilon, \overline{x}_2^\epsilon$, one has $\mathfrak{l}_k(1,\overline{x}_i^\epsilon)^\epsilon \subset \overline{\mathfrak{l}}(\overline{I},\overline{x}_i)$, $i = 1, 2$.*

Proof. We perform the proof for $\epsilon = 1$; the proof for $\epsilon = -1$ is similar. We first observe that for every $c \in k^\times$, $\overline{x_i - c_i} \not\sim_p 1, \overline{x}_i$, $i = 1, 2$. Since k is perfect, $\overline{x}_i \not\sim_p 1$ forces $\overline{x_i - c_i} \not\sim_p 1$. If $\overline{x_i - c_i} \sim_p \overline{x}_i$, there would be nonzero integers $a_i, b_i \in \mathbb{Z}$ and $\alpha_i \in \overline{k(x_i)^F}$ such that

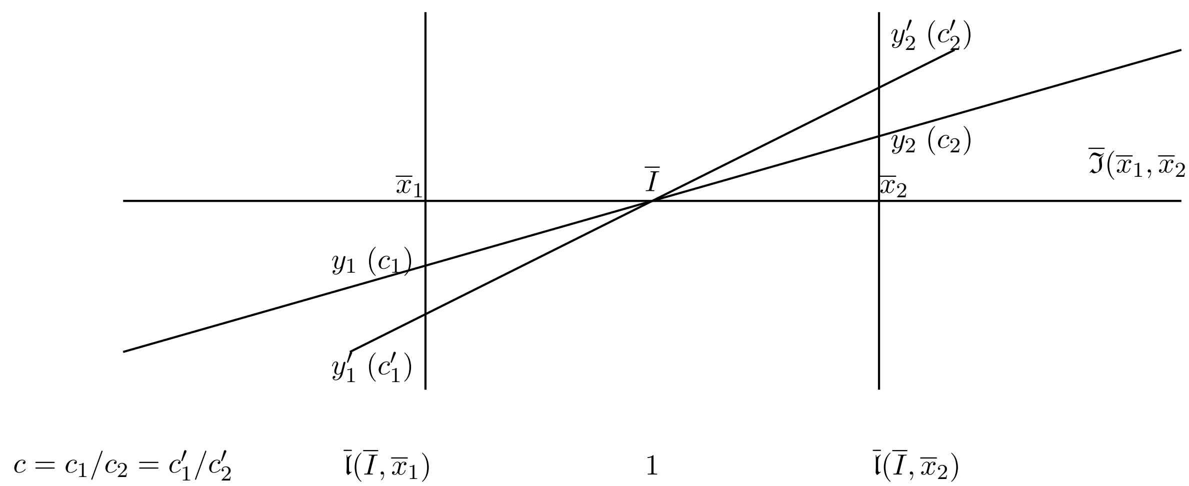
$$\frac{(x_i - c_i)^{b_i - 1} x_i^{a_i - 1}(b_i x_i - a_i(x_i - c_i))}{x_i^{2a_i}} dx_i = d(\frac{(x_i-c_i)^{b_i}}{x_i^{a_i}}) = 0,$$

which forces (here we use again $\overline{x}_i \not\sim_p 1$) $a_i = b_i = 0$: a contradiction.
Fix $c \in k$. On the one hand $x_1 - cx_2 = (\frac{x_1}{x_2} - c)x_2 \in k(x_1/x_2)^\times x_2$ and on the other hand, writing $\{i,j\} = \{1,2\}$, for every $c_i, c_j \in k^\times$ such that $c = c_i/c_j$,

$$x_i - cx_j = (\frac{x_i - c_i}{x_j - c_j} - c)(x_j - c_j) \in k(\frac{x_i - c_i}{x_j - c_j})^\times (x_j - c_j). \tag{3.1}$$

Since $\overline{x_i - c_i} \not\sim_p \overline{x}_i, 1$, $i = 1, 2$, this ensures that $x_1 - cx_2 \in \mathcal{I}(\overline{x}_1, \overline{x}_2, \overline{y}_1, \overline{y}_2) \subset \mathfrak{I}(\overline{x}_1, \overline{x}_2)$. The last part of the assertion also follows from (3.1) since for every $c_j \in k^\times$ one can take $c_i = cc_j$. □

The following picture sums up visually what happens for $\epsilon = 1$.



Provided $(\overline{x}_1, \overline{x}_2)$ satisfies certain properties which are encapsuled in the notion of 'good pair' (see Definition 19) and $p = 0$, the indeterminancy $\epsilon = \pm 1$ is the only one (see Remark 26) but when $p > 0$, it is much rougher. More precisely, when $p > 0$, the set $\mathfrak{I}(\overline{x}_1, \overline{x}_2)$ only recovers the line passing through $(\overline{x}_1, \overline{x}_2)$ up to prime-to-p powers and certain affine transformations with F^p-coefficients. The best one can say in whole generality is stated in Lemma 23, which is the technical core of the paper. The proof of Lemma 23 is sketched in Subsection 3.4.2.

For every $\overline{x}_1, \overline{x}_2 \in F^\times/k^\times$ such that $\overline{x}_1, \overline{x}_2, \overline{x}_1/\overline{x}_2 \not\sim_p = 1$, another key property of $\Omega^\circ := \mathfrak{l}_k(\overline{x}_1, \overline{x}_2) \setminus \{\overline{x}_1, \overline{x}_2\}$ as a subset of $\overline{\mathfrak{I}}(\overline{x}_1, \overline{x}_2)$ is that, for $i = 1, 2$ the intersection

$$\bigcap_{\overline{I} \in \Omega^\circ} \mathfrak{l}(\overline{I}, \overline{x}_i)$$

of the 'parameter spaces' $\mathfrak{l}(\overline{I}, \overline{x}_i)$ contains a non-empty subset $\Delta_i (= \mathfrak{l}_k(1, \overline{x}_i))$ which is not contained in $F^{\times p}\overline{x}_i^{\mathbb{Z}}$. This property, which is only set theoretic and multiplicative hence is preserved by any group isomorphism $\psi : F^\times/k^\times \tilde{\to} F'^\times/k'^\times$, will be used crucially in combination with the easy Lemma 28 (which is completely independent of the rest of the proof) in the proof of Proposition 27.

3.2.2. The injectivity of the map

$$\mathrm{Isom}(F|k, F'|k') \to \overline{\mathrm{Isom}}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times)$$

in Theorem 4 is easy - see the last paragraph of Subsection 3.6. We now summarize the main steps of the proof of the surjectivity in Theorem 4 assuming Lemma 23 (and $p>0$).

Let $\psi : F^\times/k^\times \tilde{\to} F'^\times/k'^\times$ be a group isomorphism preserving algebraic independence. The basic idea is to apply the fundamental theorem of projective geometry (Lemma 29). For this, one should show that for $\epsilon = \pm 1$, ψ^ϵ maps lines in $F^\times/k^\times$ isomorphically onto lines in $F'^\times/k'^\times$. We are not able to do this directly. Instead, we consider first a very small quotient of $\psi : F^\times/k^\times \tilde{\to} F'^\times/k'^\times$, namely

$$\begin{array}{ccc} F^\times/k^\times & \xrightarrow[\psi]{\simeq} & F'^\times/k'^\times \\ \downarrow & & \downarrow \\ F^\times/F^{p\times} & \xrightarrow[\overline{\psi}]{\simeq} & F'^\times/F'^{p\times} \end{array}$$

and show (Proposition 27) that there exists a unique integer $m \in \mathbb{Z}$ satisfying (1.1) such that $\overline{\psi}^m$ maps lines in $F^\times/F^{p\times}$ isomorphically onto lines in $F'^\times/F'^{p\times}$. Using symmetry, multiplicativity and that every line in $F'^\times/k'^\times$ can be shifted to a line passing through a good pair (Lemma 20), it is actually enough to show that there exists a unique integer $m \in \mathbb{Z}$ satisfying (1.1) such that for every $\overline{x}_1 \neq \overline{x}_2 \in F^\times/p$ for which $(\psi(\overline{x}_1), \psi(\overline{x}_2)) \in F'^\times/k'^\times$ is a good pair, $\overline{\psi}(\mathfrak{l}_k(\overline{x}_1, \overline{x}_2))^m \subset \mathfrak{l}_{F'^p}(\psi(\overline{x}_1)^m, \psi(\overline{x}_2)^m)$. From Lemma 17 and the multiplicativity of ψ, one has $\Omega := \psi(\mathfrak{l}_k(\overline{x}_1, \overline{x}_2)) \subset \psi(\mathfrak{I}(\overline{x}_1, \overline{x}_2)) = \mathfrak{I}(\psi(\overline{x}_1), \psi((\overline{x}_2))$ and, for every $\overline{I} \in \mathfrak{l}_k(\overline{x}_1, \overline{x}_2)$, $\overline{I} \neq \overline{x}_1, \overline{x}_2$, one has $\Delta_i := \psi(\mathfrak{l}_k(1, \overline{x}_i)) \subset \psi(\bar{\mathfrak{l}}(\overline{I}, \overline{x}_i)) = \mathfrak{l}(\psi(\overline{I}), \psi(\overline{x}_i))$, $i = 1, 2$. Write $\Omega^\circ := \Omega \setminus \{\psi(\overline{x}_1), \psi(\overline{x}_2)\}$. From Lemma 23 and Lemma 28, one has a stratification $\Omega^\circ = \sqcup_m \Omega^\circ_m$, where m varies among all integers $m \in \mathbb{Z}$ satisfying (1.1) with the property that $\Omega^{\circ m}_m \subset \mathfrak{l}_{F'^p}(\psi(\overline{x}_1)^m, \psi(\overline{x}_2)^m)$ and for every $\omega \in \Omega^\circ_m$, $\bar{\mathfrak{l}}(\omega, \psi(\overline{x}_i))^m \subset \mathfrak{l}_{F'^p}(1, \psi(\overline{x}_i)^m)$, $i = 1, 2$. In particular, one has the inclusions $\Delta_i^m \subset \mathfrak{l}_{F'^p}(1, \psi(\overline{x}_i)^m)$, $i = 1, 2$ which are *independent of* ω. Applying Lemma 28 again, this shows that $\Omega^\circ_m = \emptyset$ for all but one m and then that m is independent of the line $\mathfrak{l}_k(\overline{x}_1, \overline{x}_2)$.

With Proposition 27 in hands, one can apply the fundamental theorem of projective geometry to $\overline{\psi}^m : F^\times/F^{p\times} \tilde{\to} F'^\times/F'^{p\times}$ to obtain a unique field isomorphism $\Phi : F \tilde{\to} F'$ such that the induced group isomorphism $\overline{\phi} : F^\times/F^{p\times} \tilde{\to} F'^\times/F'^{p\times}$ coincides with $\overline{\psi}^m$. To conclude, it remains to show that the group isomorphism $\phi : F^\times/k^\times \tilde{\to} F'^\times/k'^\times$ induced by $\Phi : F \tilde{\to} F'$ coincides with ψ and that $m = \pm 1$. We prove both assertions together in Subsection 3.6. It is the consequence of a slightly tricky computation, which relies on the explicit description of $\psi(\overline{x}_1 + \overline{x}_2)^m$ given by (3.2) and the additivity of Φ.

3.3. **Multiplicatively shifting lines to lines passing through good pairs.**

Let k be a perfect field of characteristic $p \geq 0$ and let $F|k$ be a finitely generated regular field extension of transcendence degree ≥ 2.

Definition 18. We say that $x \in F$ is *$F|k$-regular* if x is transcendental over k and $F|k(x)$ is a regular field extension.

Definition 19. We say that $(\overline{x}_1, \overline{x}_2) \in F^\times/k^\times$ is a *good pair* if for some (equivalently, every) lifts $x_1, x_2 \in F^\times$ of $\overline{x}_1, \overline{x}_2 \in F^\times/k^\times$, x_1 is $F|k$-regular and $dx_1, dx_2 \in \Omega^1_{F|k}$ are linearly independent over F.

Lemma 20. *For every $x \in F^\times \setminus F^{p\times}$, there exists a $F|k$-regular $y \in F^\times$ such that dx, dy are linearly independent over F.*

In particular, for every $\overline{x} \in F^\times/k^\times$, $\overline{x} \neq 1$ in $F^\times/p$ there exists $\overline{y} \in F^\times/k^\times$ such that $(\overline{y}, \overline{xy}) \in F^\times/k^\times$ is a good pair. In particular, for $\overline{x}_1 \neq \overline{x}_2 \in F^\times/k^\times$ and setting $\overline{x} := \frac{\overline{x}_1}{\overline{x}_2} \neq 1$, the line $\mathfrak{l}_k(\overline{x}_1, \overline{x}_2)$ can be shifted multiplicatively to a line passing through a good pair $(\overline{y}, \overline{xy})$ as

$$\overline{x}_1^{-1}\overline{y}\mathfrak{l}_k(\overline{x}_1, \overline{x}_2) = \mathfrak{l}_k(\overline{y}, \overline{xy}).$$

Proof. This follows from Bertini theorems. Since F has finite transcendence degree $r \geq 2$ over k and k is perfect, there exist $x_2, \ldots, x_r \in F^\times$ such that $dx, dx_2, \ldots, dx_r$ are linearly independent over F. Write $E := k(x_2, \ldots, x_r)$. Let $z \in F^\times$ with minimal polynomial

$$P_z = T^d + \sum_{0 \leq i \leq d-1} a_i T^i \in E(x)[T]$$

over $E(x)$. Then dx, dz are linearly dependent over F if and only if $\partial a_i / \partial x_j = 0$, $i = 0, \ldots, d-1$, $j = 2, \ldots r$, or equivalently, $P_z \in E^p(x)[T]$. In particular, any $y \in E(x) \setminus E^p(x)$ will have the property that dx, dy are linearly independent over F. We claim that one can find $y \in E(x) \setminus E^p(x)$ such that y is $F|k$-regular. Fix a normal quasi-projective model $X|k$ of $F|k$ such that $x, x_2, \ldots, x_r$ induce a finite dominant morphism $\underline{x} : X \to \mathbb{P}^r_k$. As $F|k$ is regular, X is geometrically irreducible over k. It is enough to show there exists a homogeneous polynomial $P \in k[x, x_1, \ldots, x_r] \setminus k[x, x_1^p, \ldots, x_r^p]$ such that the fiber at 0 of the composite map

$$y : X \overset{\underline{x}}{\to} \mathbb{P}^r_k \overset{P}{\to} \mathbb{P}^1_k$$

is geometrically irreducible. Viewing y as an element in $E(x)$, we deduce that y is $F|k$-regular, by [6, 9.7]. If k is infinite, the existence of P follows directly from [7, Cor. 6.11.3]. If k is finite, this follows from [5, Thm. 1.6] applied to $\underline{x}_{\overline{k}} : X_{\overline{k}} \to \mathbb{P}^r_{\overline{k}}$ (note that there is no vertical component since $\underline{x}_{\overline{k}} : X_{\overline{k}} \to \mathbb{P}^r_{\overline{k}}$ is finite) and Lemma 21 below. □

Let k be a finite field. Set $S' := k[x, x_2^p, \ldots, x_r^p] \subset k[x, x_2, \ldots, x_r]$ and define the density of S' as

$$\delta(S') = \lim_{d \to +\infty} \frac{|S' \cap S_d|}{|S_d|},$$

where $S_d \subset k[x, x_2, \ldots, x_r]$ denotes the set of homogeneous polynomials of degree d. Then

Lemma 21. $\delta(S') = 0$.

Proof.[3] As $S_{d+p-1} = \oplus_{i=0}^{p-1} x^{p-1-i}(k[x^p, x_2, \ldots, x_r] \cap S_{d+i})$, one has

$$\dim(S_{d+p-1}) \geq p\dim(k[x^p, x_2, \ldots, x_r] \cap S_d) \geq p\dim(S' \cap S_d),$$

so $\dim(S' \cap S_d) \leq \frac{1}{p}\dim(S_{d+p-1})$ and thus, using that $\dim(S_d) = \binom{d+r-1}{d}$,

$$\dim(S' \cap S_d) - \dim(S_d) \leq \frac{1}{p}\dim(S_{d+p-1}) - \dim(S_d) \sim \frac{(d+r-1)!}{d!(r-1)!}(\frac{1}{p} - 1) \to -\infty.$$

This means $\delta(S') = \lim_{d \to +\infty} \frac{|S' \cap S_d|}{|S_d|} = 0$. □

Remark 22. We resorted to Bertini theorems, which provide a conceptually natural proof of Lemma 20 but one can give more elementary arguments. If k is infinite, the Galois-theoretic Lemma [10, Chap. VIII, Lem. in Proof of Thm. 7] already shows there exists (infinitely many) $0 \neq a \in k$ such that $y := ax_2 + x$ is $F|k$-regular; by construction dx, dy are linearly independent over F. If k is finite, Akio Tamagawa suggested the following arguments. Fix a smooth (not necessarily

[3]Our original proof of Lemma 21 was more technical; the following alternative proof was suggested to us by one of the Referees.

proper) model $X|k$ of $F|k$ and a closed point $t \in X$. Let $\widetilde{X} \to X$ denote the blow-up of X at t and $D_t = \mathbb{P}^{n-1}_{k(t)} \subset \widetilde{X}$ the exceptional divisor. Fix a non-empty affine subset $U = \mathrm{Spec}(R) \subset \widetilde{X}$ such that $Z := U \cap D_t$ is non-empty and the rational map $x : \widetilde{X} \to X \dashrightarrow \mathbb{A}^1_k$ given by x is defined over U. We endow Z with its reduced subscheme structure. Since Z is irreducible, one can write $Z = \mathrm{Spec}(R/P)$ for some prime ideal P in R. Pick $y \in R \setminus R \cap F^p\overline{k(x)^F}$ such that $f \mathrm{mod} P \in R/P \setminus k(t)$. Let $\overline{k[y]^F} \subset F$ denote the normal closure of $k[y]$ in $\overline{k(y)^F}/k(y)$. Since R is smooth over k hence normal, $\overline{k[y]^F} \subset R$. Also, by our choice of y, the morphism $\overline{k[y]^F} \hookrightarrow R \twoheadrightarrow R/I$ is injective whence the fraction field $\overline{k(y)^F}$ of $\overline{k[y]^F}$, embeds into the fraction field $k(t)(x_2, \ldots, x_n)$ of R/I. Since $\overline{k(y)^F}/k$ is regular, $k(t) \otimes_k \overline{k(y)^F} \simeq k(t) \cdot \overline{k(y)^F} \subset k(t)(x_2, \ldots, x_n)$. From Lurōth theorem, one thus has $k(t) \otimes_k \overline{k(y)^F} = k(t)(T)$ for some $T \in k(t)(x_2, \ldots, x_n)$ transcendent over $k(t)$. In other words, $\overline{k(y)^F}$ is the function field of a $k(t)/k$ form C_y of $\mathbb{P}^1_k$. Since k is finite hence perfect with trivial Brauer group, $C_y \simeq \mathbb{P}^1_k$. This shows $y \in F$ is $F|k$ regular. Since $y \notin F^p\overline{k(x)^F}$, dx, dy are linearly independent over F.

3.4. **Approximating lines passing through good pairs up to powers.**

3.4.1. *Statement of the main Lemma.* Let k be a perfect field of characteristic $p \geq 0$ and let $F|k$ be a finitely generated regular field extension of transcendence degree ≥ 2.

Lemma 23. *Let $(\overline{x}_1, \overline{x_2}) \in F^\times/k^\times$ be a good pair. Then, for every $I \in \mathfrak{I}(\overline{x}_1, \overline{x}_2)$ there exists $m \in \mathbb{Z}$ (depending a priori on I) satisfying (1.1), $N \in \mathbb{Z}$, $\alpha = \alpha(\frac{x_1}{x_2}) \in \overline{k(\frac{x_1}{x_2})^F}^\times$ and $c \in k^\times$ such that*

$$I^m = \alpha(\frac{x_1}{x_2})^p(x_1^m - c\frac{x_1^{pN}}{x_2^{pN}}x_2^m). \tag{3.2}$$

Furthermore, for every $y_i \in \overline{k(x_i)^F}$, $\overline{y}_i \not\sim_p \overline{x}_i, 1$, $i = 1, 2$ such that $I \in \mathcal{I}(\overline{x}_1, \overline{x}_2, \overline{y}_1, \overline{y}_2)$, one has for $i = 1, 2$

$$y_i^m = \alpha_i^p(x_i^m - c_i x_i^{pN}) \tag{3.3}$$

for some $\alpha_i \in \overline{k(x_i)^F}$, $c_i \in k^\times$ with the condition $c = c_1/c_2$.

Remark 24. In particular, for every $I \in \mathfrak{I}(\overline{x}_1, \overline{x}_2)$ there exists $m \in \mathbb{Z}$ (depending *a priori* on I) satisfying (1.1) such that $\overline{I}^m \in \mathfrak{l}_{F^p}(x_1^m, x_2^m)$ and $\mathfrak{l}(I, x_i)^m \subset \mathfrak{l}_{F^p}(1, x_i^m)$, $i = 1, 2$. But let us point out that (3.2) imposes restrictions on the lifts $I \in F^\times$ of the $\overline{I} \in \mathfrak{l}_{F^p}(x_1^m, x_2^m)^{m^{-1}}$ which lie in $\mathfrak{I}(\overline{x}_1, \overline{x}_2)$. This will be used crucially in Subsection 3.6.

3.4.2. *Main steps of the proof of Lemma 23.* The proof when $p = 0$ is significantly simpler since $\ker(d) = k$ (recall $F|k$ is regular). We carry out the proof for $p > 0$ and just mention the simplifications that occur for $p = 0$. The results for $p = 0$ are similar (recall that, by our convention, $F^p = k$ when $p = 0$).

We are to determine the possible $y_i \in \overline{k(x_i)^F}^\times$, $\overline{y}_i \not\sim_p \overline{x}_i, 1$, $i = 1, 2$ such that $\mathcal{I}(\overline{x}_1, \overline{x}_2, \overline{y}_1, \overline{y}_2) \neq \emptyset$ and for all such y_i, $i = 1, 2$ the elements $I \in \mathcal{I}(\overline{x}_1, \overline{x}_2, \overline{y}_1, \overline{y}_2)$. So assume $\mathcal{I}(\overline{x}_1, \overline{x}_2, \overline{y}_1, \overline{y}_2) \neq \emptyset$ and fix $I \in \mathcal{I}(\overline{x}_1, \overline{x}_2, \overline{y}_1, \overline{y}_2)$.

Note that, as $(\overline{x}_1, \overline{x_2}) \in F^\times/k^\times$ is a good pair and $\overline{y}_i \not\sim_p 1$, $i = 1, 2$, $\overline{y}_1/\overline{y}_2 \not\sim_p 1$. Indeed, otherwise, we would have $y_1'dx_1 = \frac{y_1 y_2'}{y_2}dx_2$ hence $y_1' = y_2' = 0$.

We decompose the proof of Lemma 23 into four steps.

- Step 1. Differentiating the conditions $I/x_2 \in \overline{k(x_1/x_2)^F}^\times$ and $I/y_2 \in \overline{k(y_1/y_2)^F}^\times$, we show that there exists $u \in k^\times$ such that I satisfies an equation of the form
$$\frac{d(I/x_2)}{(I/x_2)} = \frac{f_1(1-f_2)}{f_1-f_2}\frac{d(x_1/x_2)}{x_1/x_2}$$
with, for $i=1,2$, $f_i = \frac{x_i y_i'}{y_i}$ satisfying the equation
$$x_i f_i' = u f_i(1-f_i).$$
This step uses the conditions $\overline{x}_1/\overline{x}_2, \overline{y}_1/\overline{y}_2 \not\sim_p 1$ and that $(\overline{x}_1, \overline{x}_2)$ is a good pair.

- Step 2. Considering the equation $x_i f_i' = u f_i(1-f_i)$ for $i=1$ and using that $x_1 \in F^\times$ is $F|k$-regular, we show that the parameter u necessarily lies $\mathbb{F}_p$ and can be represented[4] by an integer $m \in \mathbb{Z}$ satisfying (1.1). Once this is settled, one can easily solve $x_i f_i' = u f_i(1-f_i)$ for $i=1,2$ and determine y_i^m, $i=1,2$.

- Step 3. Using the relations between I, f_1, f_2 and the expressions of y_i^m, $i=1,2$ obtained in Step 2, we show that
$$I^m = \alpha^p(x_1^m - \frac{\beta_1^p}{\beta_2^p}x_2^m)$$
for some $\alpha \in \overline{k(\frac{x_1}{x_2})^F}$, $\beta_i \in \overline{k(x_i)^F}$, $i=1,2$.

- Step 4. Using that $I/x_2 \in \overline{k(\frac{x_1}{x_2})^F}$, we show that there exists $N \in \mathbb{Z}$ such that $\beta_i = c_i x_i^N$ for some $c_i \in k^\times$, $i=1,2$.

For Step 1 and Step 2 we use the following technical lemma, which we state separately.

Lemma 25. *Let $x \in F^\times \setminus F^{p\times}$ and $y \in \overline{k(x)^F}^\times$. Write $dy = y'dx$. Then*

(a) For $m \in \mathbb{Z}$, $\frac{xy'}{y} = m \Rightarrow y \in F^{p\times}x^m$;

(b) If $y \in k(x)^\times$ and $\frac{xy'}{y} \in F^{p\times}$ then $y \in F^{p\times}x^{\mathbb{Z}}$; in particular, $\overline{x} \sim_p \overline{y}$ (since $\frac{xy'}{y} \in F^{p\times}$ implies $\overline{y} \not\sim_p 1$).

Proof. For (a), just observe that $\frac{xy'}{y} = m$ if and only if
$$d(\frac{y}{x^m}) = \frac{x^m y' - m x^{m-1} y}{x^{2m}} dx = 0.$$
For (b), write $y = \frac{a}{b}A^p$ with $0 \neq a, b \in k[x]$ coprime and with zeros of multiplicities at most $p-1$ and a monic (if $p=0$, just impose $a, b \in k[x]$ to be coprime and a monic). By assumption there exist $u, v \in k[x]$ coprime such that
$$x(a'b - ab')v^p = u^p ab.$$
Assume a has a non-zero root α of multiplicity $1 \leq n_\alpha \leq p-1$. Then, since a and b are coprime, on the left hand side, the multiplicity of α is congruent to $n_\alpha - 1$ (mod p), while, one the right hand

[4]In the following, to simplify the exposition, we usually do not distinguish in the notation an element $m \in \mathbb{Z}$ and its image $m \in \mathbb{F}_p \subset F$; this should cause no confusion.

side, the multiplicity of α is congruent to $n_\alpha \pmod p$: a contradiction. This shows there exists $0 \leq m \leq p-1$ such that $a = x^m$. The equation thus becomes

$$(mb - xb')v^p = u^p b$$

or, equivalently (since $m^p = m$ as $m \in \mathbb{F}_p$),

$$b(mv-u)^p = (mv^p - u^p)b = xb'v^p.$$

Again, considering the multiplicity of a non-zero root of b, one sees that $b \in k^\times x^n$ for some integer $0 \leq n \leq p-1$. As a result $y = \frac{a}{b}A^p \in F^{p\times}x^{\mathbb{Z}}$ as claimed. □

3.4.3. *Step 1.* For $z = x, y$ we have: $I/z_2 \in \overline{k(z_1/z_2)^F}^\times$, so that there exists $A_z \in \overline{k(z_1/z_2)^F}$ with

$$\frac{d(I/z_2)}{I/z_2} = A_z \frac{d(z_1/z_2)}{z_1/z_2}. \tag{3.4}$$

Here, we use $\overline{z}_1/\overline{z}_2 \not\sim_p 1$ (see the third paragraph in 3.4.2) through the remark after Corollary 15. Equivalently,

$$\frac{dI}{I} = \frac{dz_2}{z_2}(1 - A_z) + \frac{dz_1}{z_1}A_z.$$

We deduce

$$A_x \frac{dx_1}{x_1} - A_y \frac{dy_1}{y_1} = (A_x - 1)\frac{dx_2}{x_2} - (A_y - 1)\frac{dy_2}{y_2} \in F dx_1 \cap F dx_2 = 0.$$

Whence, setting $dy_i = y_i' dx_i$ with $y_i' \in \overline{k(x_i)^F}$ (here, we use $\overline{x}_i \not\sim_p 1$) and using that dx_1, dx_2 are linearly independent over F, we obtain

$$A_x = A_y \frac{x_1 y_1'}{y_1} = (A_y - 1)\frac{x_2 y_2'}{y_2} + 1. \tag{3.5}$$

Set

$$f_i := \frac{x_i y_i'}{y_i} \in \overline{k(x_i)^F},\ i = 1, 2. \tag{3.6}$$

We obtain

$$A_x = A_y f_1, \quad A_y(f_1 - f_2) = 1 - f_2. \tag{3.7}$$

Since $y_2 \not\sim_p x_2$, $1 - f_2 = y_2(\frac{x_2}{y_2})' \neq 0$ hence $f_1 - f_2, A_y \neq 0$. As a result the second equation in (3.7) can be rewritten

$$A_y = \frac{1 - f_2}{f_1 - f_2}.$$

So, setting $df_i = f_i' dx_i$ with $f_i' \in \overline{k(x_i)^F}$, $i = 1, 2$ we get

$$\frac{dA_y}{A_y} = \frac{f_1'}{f_2 - f_1}dx_1 + \frac{(1 - f_1)f_2'}{(1 - f_2)(f_1 - f_2)}dx_2.$$

We also have $A_y \in \overline{k(y_1/y_2)^F}^\times$ so that there exists $\alpha \in \overline{k(y_1/y_2)^F}$ with

$$\frac{dA_y}{A_y} = \alpha\left(\frac{y_1'}{y_1}dx_1 - \frac{y_2'}{y_2}dx_2\right).$$

(here we use $\overline{y}_1/\overline{y}_2 \not\sim_p 1$). Since dx_1, dx_2 are linearly independent over F, one gets

$$\alpha = \frac{y_1 f_1'}{y_1'(f_2 - f_1)} = \frac{y_2(1 - f_1)f_2'}{y_2'(1 - f_2)(f_2 - f_1)}$$

whence

$$u := \frac{y_1 f_1'}{y_1'(1-f_1)} = \frac{y_2 f_2'}{y_2'(1-f_2)} \in \overline{k(x_1)^F} \cap \overline{k(x_2)^F} = k.$$

By Lemma 25 (b) (recall that by definition of a good pair x_1 is $F|k$-regular) below and the fact that $y_1 \not\sim_p x_1$, we have $f_1 \notin F^p$ hence $u \neq 0$. Recalling that $f_i := \frac{x_i y_i'}{y_i}$, $i = 1, 2$ we eventually get $x_i f_i' = u f_i (1 - f_i)$ that is,

$$x_i (f_i/(1-f_i))'/(f_i/(1-f_i)) = u. \tag{3.8}$$

3.4.4. *Step 2.* As $x_1(f_1/(1-f_1))'/(f_1/(1-f_1)) = u$ and k is perfect, Lemma 25 (b) applied to $y := f_1/(1-f_1) \in k(x_1)^\times$ (here we use that x_1 is $F|k$-regular) implies that $u \in \mathbb{F}_p$. As $u \neq 0$, it can be represented by an integer $m \in \mathbb{Z}$ satisfying (1.1). But then, by Lemma 25 (a), (3.8) yields $(1-f_i)/f_i = x_i^{-m}\beta_i^p$ for some $\beta_i \in \overline{k(x_i)^F}$ or, equivalently,

$$\frac{x_i y_i'}{y_i} = f_i = \frac{x_i^m}{x_i^m + \beta_i^p}.$$

Whence

$$\frac{(x_i^m + \beta_i^p)'}{x_i^m + \beta_i^p} = m\frac{x_i^{m-1}}{x_i^m + \beta_i^p} = \frac{(y_i^m)'}{y_i^m}$$

and

$$d\Big(\frac{y_i^m}{(x_i^m + \beta_i^p)}\Big) = 0$$

that is

$$y_i^m = \alpha_i^p (x_i^m + \beta_i^p) \tag{3.9}$$

for some $\alpha_i \in \overline{k(x_i)^F}$.

Remark 26. ($p = 0$ case) If $p = 0$, we obtain that there exists $0 \neq m \in \mathbb{Z}$ such that $y_1^m = \alpha_1(x_1^m + \beta_1)$ for some $\alpha_1, \beta_1 \in k^\times$. Then the factoriality of $k[x_1]$ and the fact that $x_1 \not\sim_0 y_1$ yields $m = \pm 1$.

3.4.5. *Step 3.* Then,

$$A_y = \frac{1-f_2}{f_1 - f_2} = \frac{\beta_2^p(x_1^m + \beta_1^p)}{\beta_2^p x_1^m - \beta_1^p x_2^m}$$

and

$$A_x = A_y f_1 = \Big(1 - \frac{\beta_1^p}{\beta_2^p}\Big(\frac{x_1}{x_2}\Big)^{-m}\Big)^{-1}.$$

So, writing $\beta := \frac{\beta_1}{\beta_2}$, $x := \frac{x_1}{x_2}$ and $J = J(x) := \frac{I}{x_2}$ and using (3.4) one gets

$$\frac{(J^m)'}{J^m} = \frac{m x^{m-1}}{x^m - \beta^p} = \frac{(x^m - \beta^p)'}{x^m - \beta^p}$$

Whence

$$J^m = \alpha^p (x^m - \beta^p)$$

for some $\alpha \in \overline{k(\frac{x_1}{x_2})^F}$ and

$$I^m = \alpha^p (x_1^m - \beta^p x_2^m) = \alpha^p \Big(x_1^m - \frac{\beta_1^p}{\beta_2^p} x_2^m\Big)$$

with $\alpha \in \overline{k(\frac{x_1}{x_2})^F}$ and $\beta_i \in \overline{k(x_i)^F}$, $i = 1, 2$.

3.4.6. *Step 4.* The assumption $I/x_2 \in \overline{k(\frac{x_1}{x_2})^F}$ forces $\beta = \frac{\beta_1}{\beta_2} \in \overline{k(\frac{x_1}{x_2})^F}^\times$. This in turn imposes $\beta_1 \in k^\times x_1^N, \beta_2 \in k^\times x_2^N$ for some $N \in \mathbb{Z}$.

Indeed, write again $x := \frac{x_1}{x_2}$. Up to replacing β with βx^N (hence β_i with $\beta_i x_i^N$, $i = 1, 2$) for some $N \in \mathbb{Z}$, one may assume that β_1 (as a function in x_1) is regular and has no zero at 0. We are going to show that, necessarily, $\beta_1, \beta_2 \in k^\times$. Let

$$P_\epsilon(x, T) = T^d + \sum_{0 \le i \le d-1} a_{\epsilon,i}(x) T^i \in k(x)[T]$$

be the monic minimal polynomial of β^ϵ over $k(x)$ for $\epsilon = \pm 1$. If $\beta_1 \notin k^\times$, then β_1 or β_1^{-1} admits at least one zero distinct from 0. So the relations

$$\beta_2^{-d} + \sum_{0 \le i \le d-1} a_{1,i}(x)(\beta_1^{-1})^{d-i}\beta_2^{-i} = 0$$

$$\beta_2^{d} + \sum_{0 \le i \le d-1} a_{-1,i}(x)\beta_1^{d-i}\beta_2^{i} = 0$$

yield $\beta_2^{-d} = 0$ or $\beta_2^d = 0$: a contradiction. This shows that $\beta_1 \in k^\times$. Then, as x_2 and x are algebraically independent, $\beta_2 \in \overline{k(x)^F} \cap \overline{k(x_2)^F} = k$.

This concludes the proof of Lemma 23.

3.5. **Recovering lines in $F^\times/p$, $F'^\times/p$ up to powers.** Let k, k' be perfect fields of characteristic $p \geq 0$, let $F|k$, $F'|k'$ be finitely generated regular field extensions of transcendence degree ≥ 2 and let

$$\psi : F^\times/k^\times \tilde{\to} F'^\times/k'^\times$$

be a group isomorphism preserving algebraic dependence. Write

$$\overline{\psi} : F^\times/p \tilde{\to} F'^\times/p$$

for the group isomorphism induced by ψ.

Proposition 27. *There exists $m \in \mathbb{Z}$ satisfying (1.1) such that for every $\overline{x}_1 \neq \overline{x}_2 \in F^\times/p$,*

$$\overline{\psi}(\mathfrak{l}_{F^p}(\overline{x}_1, \overline{x}_2))^m = \mathfrak{l}_{F'^p}(\overline{\psi}(\overline{x}_1)^m, \overline{\psi}(\overline{x}_2)^m)$$

Proof. For simplicity, write $\overline{x}' := \overline{\psi}(\overline{x})$. We proceed in two steps.

- Step 1: We first show there exists $m \in \mathbb{Z}$ satisfying (1.1) such that for every $\overline{x}_1 \neq \overline{x}_2 \in F^\times/p$,

$$\overline{\psi}(\mathfrak{l}_{F^p}(\overline{x}_1, \overline{x}_2))^m \subset \mathfrak{l}_{F'^p}(\overline{x}_1'^m, \overline{x}_2'^m)$$

By (the comment after) Lemma 20, one may assume $(\overline{x}_1', \overline{x}_2') \in F'^\times/k'^\times$ is a good pair. More precisely, as $\overline{x}_2/\overline{x}_1 \not\sim_p 1$, $\overline{x}_2'/\overline{x}_1' \not\sim_p 1$ hence there exists $\overline{z}' \in F'^\times/k'^\times$ such that $(\overline{z}', \overline{z}'\overline{x}_2'/\overline{x}_1')$ is a good pair in $F'^\times/k'^\times$. Write $\overline{z} := \psi^{-1}(\overline{z}') \in F^\times/k^\times$. Then, observing that

$$\mathfrak{l}_{F^p}(\overline{x}_1, \overline{x}_2) = \overline{x}_1/\overline{z}\,\mathfrak{l}_{F^p}(\overline{z}, \overline{z}\overline{x}_2/\overline{x}_1),$$

one has

$$\overline{\psi}(\overline{x}_1/\overline{z})^m \overline{\psi}(\mathfrak{l}_{F^p}(\overline{z}, \overline{x}_2/\overline{x}_1))^m = \overline{\psi}(\mathfrak{l}_{F^p}(\overline{x}_1, \overline{x}_2))^m \subset \mathfrak{l}_{F'^p}(\overline{x}_1'^m, \overline{x}_2'^m) = (\overline{x}_1'/\overline{z}')^m \mathfrak{l}_{F'^p}(\overline{z}'^m, \overline{x}_2'^m/\overline{x}_1'^m)$$

if and only $\overline{\psi}(\mathfrak{l}_{F^p}(\overline{z},\overline{x}_2/\overline{x}_1))^m\subset\mathfrak{l}_{F'^p}(\overline{z}'^m,\overline{x}_2'^m/\overline{x}_1'^m)$. Similarly, $\overline{\psi}(\mathfrak{l}_{F^p}(\overline{x}_1,\overline{x}_2))^m=\mathfrak{l}_{F'^p}(\overline{x}_1'^m,\overline{x}_2'^m)$ if and only $\overline{\psi}(\mathfrak{l}_{F^p}(\overline{z},\overline{x}_2/\overline{x}_1))^m=\mathfrak{l}_{F'^p}(\overline{z}'^m,\overline{x}_2'^m/\overline{x}_1'^m)$. Since

$$\mathfrak{l}_{F^p}(\overline{x}_1,\overline{x}_2)=\bigcup_{\alpha\in F^\times}F^{p\times}\mathfrak{l}_k(\overline{x}_1,\overline{\alpha}^p\overline{x}_2)$$

and for every $\alpha\in F^\times$, $(\overline{x}_1',\overline{\alpha}^p\overline{x}_2')\in F'^\times/k'^\times$ is again a good pair, it is enough to prove that there exists $m\in\mathbb{Z}$ satisfying (1.1) such that for every $\overline{x}_1\neq\overline{x}_2\in F^\times/p$ for which $(\overline{x}_1',\overline{x}_2')\in F'^\times/k'^\times$ is a good pair, one has

$$\overline{\psi}(\mathfrak{l}_k(\overline{x}_1,\overline{x}_2))^m\subset\mathfrak{l}_{F'^p}(\overline{x}_1'^m,\overline{x}_2'^m).$$

Write

$$\mathfrak{I}(\overline{x}_1',\overline{x}_2')_m:=\{I'\in\mathfrak{I}(\overline{x}_1',\overline{x}_2')\mid I'^m\in\mathfrak{l}_{F'^p}(\overline{x}_1'^m,\overline{x}_2'^m)\}.$$

From Lemma 23 (here we use that $(\overline{x}_1',\overline{x}_2')$ is a good pair) and Lemma 28 below, one has

$$\mathfrak{I}(\overline{x}_1',\overline{x}_2')=\{\overline{x}_1',\overline{x}_2'\}\bigsqcup\bigsqcup_m(\mathfrak{I}(\overline{x}_1',\overline{x}_2')_m\setminus\{\overline{x}_1',\overline{x}_2'\}),$$

where the union is over all $m\in\mathbb{Z}$ satisfying (1.1) and for every $I'\in\mathfrak{I}(\overline{x}_1',\overline{x}_2')_m$, one has

$$\bar{\mathfrak{l}}(\overline{I'},\overline{x}_i')^m\subset\mathfrak{l}_{F'^p}(1,\overline{x}_i'^m),\ i=1,2.$$

From Lemma 17, $\mathfrak{l}_k(\overline{x}_1,\overline{x}_2)\subset\overline{\mathfrak{I}}(\overline{x}_1,\overline{x}_2)$ so that $\overline{\psi}(\mathfrak{l}_k(\overline{x}_1,\overline{x}_2))\subset\overline{\mathfrak{I}}(\overline{x}_1',\overline{x}_2')$. Fix $\overline{I}\in\mathfrak{l}_k(\overline{x}_1,\overline{x}_2)$, $\overline{I}\neq\overline{x}_1,\overline{x}_2$ in $F^\times/p$ and let $m:=m(\overline{x}_1,\overline{x}_2,\overline{I})\in\mathbb{Z}$ be the unique integer satisfying (1.1) such that $I'\in\mathfrak{I}(\overline{x}_1',\overline{x}_2')_m$. From Lemma 17, for $i=1,2$, one has $\mathfrak{l}_k(1,\overline{x}_i)\subset\bar{\mathfrak{l}}(\overline{I},\overline{x}_i)$ hence

$$\overline{\psi}(\mathfrak{l}_k(1,\overline{x}_i))^m\subset\overline{\psi}(\bar{\mathfrak{l}}(\overline{I},\overline{x}_i))^m=\bar{\mathfrak{l}}(\overline{I'},\overline{x}_i')^m\subset\mathfrak{l}_{F'^p}(1,\overline{x}_i'^m).$$

By Lemma 28 below, this characterizes m as the unique integer satisfying (1.1) such that

$$\overline{\psi}(\mathfrak{l}_k(1,\overline{x}_i))^m\subset\mathfrak{l}_{F'^p}(1,\overline{x}_i'^m).$$

Hence m is uniquely determined by any of the two sets $\overline{\psi}(\mathfrak{l}_k(1,\overline{x}_i))$, $i=1,2$ and, in particular, does not depend on $\overline{I}$. As a result:

$$\overline{\psi}(\mathfrak{l}_k(\overline{x}_1,\overline{x}_2))^m\subset\mathfrak{l}_{F'^p}(\overline{x}_1'^m,\overline{x}_2'^m).$$

In fact, m does not depend on the line $\mathfrak{l}_k(\overline{x}_1,\overline{x}_2)$ either. Indeed, let $\mathfrak{l}_k(\overline{y}_1,\overline{y}_2)$ be any other line such that $(\overline{y}_1',\overline{y}_2')\in F'^\times/k'^\times$ is a good pair and let $n\in\mathbb{Z}$ satisfying (1.1) be the attached integer. Then, necessarily, at least one of the two pairs $(\overline{x}_1',\overline{y}_1')$, $(\overline{x}_1',\overline{y}_2')$ - say $(\overline{x}_1',\overline{y}_1')$ - is a good pair; let $r\in\mathbb{Z}$ satisfying (1.1) be the attached integer. Then, by considering $\overline{\psi}(\mathfrak{l}_k(1,\overline{x}_1))$, one has $m=r$ and by considering $\overline{\psi}(\mathfrak{l}_k(1,\overline{y}_1))$, one has $n=r$.

- Step 2: Since the situation is symmetric in $F^\times/k^\times$ and $F'^\times/k'^\times$ (here, we use that ψ preserves algebraic dependence if and only if ψ^{-1} does, by the very definition of 'preserving algebraic dependence'), there exists $m'\in\mathbb{Z}$ satisfying conditions (1.1), such that for every $\overline{x}_1',\overline{x}_2'\in F'^\times/k'^\times$ with $\overline{x}_1'\neq\overline{x}_2'$ in $F'^\times/p$ one also has

$$\overline{\psi}^{-1}(\mathfrak{l}_{F'^p}(\overline{x}_1',\overline{x}_2'))^{m'}\subset\mathfrak{l}_{F^p}(\overline{\psi}^{-1}(\overline{x}_1')^{m'},\overline{\psi}^{-1}(\overline{x}_2')^{m'})\tag{3.10}$$

in $F^\times/p$. As a result

$$\mathfrak{l}_{F^p}(\overline{x}_1,\overline{x}_2)^{mm'}=\overline{\psi}^{-1}(\overline{\psi}(\mathfrak{l}_{F^p}(\overline{x}_1,\overline{x}_2))^m)^{m'}\subset\overline{\psi}^{-1}(\mathfrak{l}_{F'^p}(\overline{\psi}(\overline{x}_1)^m,\overline{\psi}(\overline{x}_2)^m))^{m'}\subset\mathfrak{l}_{F^p}(\overline{x}_1^{mm'},\overline{x}_2^{mm'})$$

In particular, if $\overline{x}_1,\overline{x}_2\in F^\times/k^\times$ are such that dx_1,dx_2 are linearly independent over F, we obtain

$$(x_1+x_2)^{mm'}=a_1^px_1^{mm'}+a_2^px_2^{mm'}\text{ for some }a_1,a_2\in F^\times$$

hence

$$mm'(x_1+x_2)^{mm'-1}(dx_1+dx_2) = mm'(a_1^p x_1^{mm'-1}dx_1 + a_2^p x_2^{mm'-1}dx_2)$$

and

$$(x_1+x_2)^{mm'-1} = a_1^p x_1^{mm'-1} = a_2^p x_2^{mm'-1}.$$

This forces

$$mm' \equiv 1\,(mod\,p).$$

Now, let $\overline{x}_1, \overline{x}_2 \in F^\times/k^\times$ with $\overline{x}_1 \neq \overline{x}_2$ in $F^\times/p$ and apply (3.10) to $\overline{x}'_i = \overline{\psi}(\overline{x}_i)^m$, $i=1,2$. Using $mm' \equiv 1\,(mod\,p)$, we obtain

$$\overline{\psi}^{-1}(\mathfrak{l}_{F'^p}(\overline{\psi}(\overline{x}_1)^m, \overline{\psi}(\overline{x}_2)^m)) \subset \mathfrak{l}_{F^p}(\overline{x}_1, \overline{x}_2)^m$$

in $F^\times/p$. This concludes the proof of Proposition 27.

□

Lemma 28. *For every $\overline{x} \in F^\times/k^\times$ such that $\overline{x} \neq 1$ in $F^\times/p$ and for $m \neq n \in \mathbb{Z}$ satisfying (1.1),*

$$\mathfrak{l}_{F^p}(1, \overline{x}^m)^n \cap \mathfrak{l}_{F^p}(1, \overline{x}^n)^m \subset \{1\} \cup F^{p\times} x^{mn}.$$

Proof. If $\mathfrak{l}_{F^p}(1, \overline{x}^m)^n \cap \mathfrak{l}_{F^p}(1, \overline{x}^n)^m \setminus \{1\} \neq \emptyset$, there exist $\alpha, \beta, \gamma, \delta \in F$, $\beta \neq 0 \neq \delta$, such that

$$(\alpha^p + \beta^p x^m)^n = (\gamma^p + \delta^p x^n)^m.$$

Taking the logarithmic differentials and using that $dx \neq 0$, one gets

$$\frac{\beta^p x^{m-1}}{\alpha^p + \beta^p x^m} = \frac{\delta^p x^{n-1}}{\gamma^p + \delta^p x^n},$$

hence $\gamma^p \beta^p x^{m-1} = \alpha^p \delta^p x^{n-1}$, which is only possible if $m = n$ or $\gamma\beta = \alpha\delta = 0$. But, in turn, $\gamma\beta = \alpha\delta = 0$ is possible only if $\alpha = \gamma = 0$. □

3.6. **End of the proof of Theorem 4.**

From Proposition 27 and Lemma 29 (b), applied to the field extensions F/F^p and F'/F'^p, there exist an integer $m \in \mathbb{Z}$ satisfying conditions (1.1), and a unique field isomorphism $\Phi : F \tilde{\to} F'$ such that the following diagram

$$\begin{array}{ccc} F^\times & \xrightarrow{\Phi} & F'^\times \\ \downarrow & & \downarrow \\ F^\times/p & \xrightarrow[\overline{\psi}^m]{} & F'^\times/p \end{array}$$

commutes. This concludes the proof of the surjectivity of the map $\mathrm{Isom}(F|k, F'|k') \to \overline{\mathrm{Isom}}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times)$ for $p = 0$. For $p > 0$, one needs to work more, using the more explicit description of I^m given in (3.2). Write $\phi : F^\times/k^\times \tilde{\to} F'^\times/k'^\times$ and $\overline{\phi}(= \overline{\psi}^m) : F^\times/p \tilde{\to} F'^\times/p$ for the group isomorphisms induced by $\Phi : F \tilde{\to} F'$.

Consider the group morphism

$$\begin{array}{rlcl} \theta: & F^\times/k^\times & \to & F'^{\times p}/k'^\times \\ & \overline{x} & \to & \psi(\overline{x})^m \phi(\overline{x})^{-1}. \end{array}$$

We are to show that $m = \pm 1$ and θ is trivial.

Fix a set-theoretic lift $\Psi : F^\times \to F'^\times$ of $\psi : F^\times/k^\times \to F'^\times/k'^\times$ and set

$$\begin{array}{cccc}\Theta: & F^\times & \to & F'^\times \\ & x & \to & \Psi(x)^m\Phi(x)^{-1}\end{array}$$

Let $x_1, x_2 \in F^\times$ be such that $(\psi(\overline{x}_1), \psi(\overline{x}_2)) \in F'^\times/k'^\times$ is a good pair. From (3.2), one has

$$\overline{\Psi(x_1+x_2)^m} = \overline{\alpha^p(\Psi(x_1)^m + \lambda\frac{\Psi(x_1)^{Np}}{\Psi(x_2)^{Np}}\Psi(x_2)^m)}$$

in $F'^\times/k'^\times$ for some $\alpha \in F'^\times$, $\lambda \in k'^\times$ and $N \in \mathbb{Z}$ (depending on x_1, x_2). Using the definition of Θ and using that $\Phi : F \to F'$ is a field homomorphism (hence is compatible with the additive structure), one has

$$\overline{\Psi(x_1+x_2)^m} = \overline{\Theta(x_1+x_2)\Phi(x_1+x_2)} = \overline{\frac{\Theta(x_1+x_2)}{\Theta(x_1)}\Psi(x_1)^m + \frac{\Theta(x_1+x_2)}{\Theta(x_2)}\Psi(x_2)^m}.$$

in $F'^\times/k'^\times$. This shows that

$$\mu\alpha^p(\Psi(x_1)^m + \lambda\frac{\Psi(x_1)^{Np}}{\Psi(x_2)^{Np}}\Psi(x_2)^m) = \frac{\Theta(x_1+x_2)}{\Theta(x_1)}\Psi(x_1)^m + \frac{\Theta(x_1+x_2)}{\Theta(x_2)}\Psi(x_2)^m$$

for some $\mu \in k'^\times$.

Since $d\Psi(x_1), d\Psi(x_2)$ are linearly independent over F'^p by assumption, and since $p \nmid m$, $\Psi(x_1)^m, \Psi(x_2)^m$ are linearly independent over F'^p so that

$$\overline{\frac{\Theta(x_1+x_2)}{\Theta(x_1)}} = \overline{\alpha^p}, \quad \overline{\frac{\Theta(x_1+x_2)}{\Theta(x_2)}} = \overline{\alpha^p\frac{\Psi(x_1)^{Np}}{\Psi(x_2)^{Np}}}.$$

Combining both equalities one obtains

$$\theta(\overline{x}_1) = \frac{\psi(\overline{x}_1)^{Np}}{\psi(\overline{x}_2)^{Np}}\theta(\overline{x}_2).$$

Now fix two primes $p' \neq p''$ distinct from p and such that $p' \not\equiv 1\,(mod\, p'')$, and apply the above to $x_1, x_2^{p'}$, $x_1, x_2^{p''}$ to get

$$\theta(\overline{x}_1) = \frac{\psi(\overline{x}_1)^{N'p}}{\psi(\overline{x}_2)^{N'p'p}}\theta(\overline{x}_2)^{p'}$$

$$\theta(\overline{x}_1) = \frac{\psi(\overline{x}_1)^{N''p}}{\psi(\overline{x}_2)^{N''p''p}}\theta(\overline{x}_2)^{p''}$$

for some $N', N'' \in \mathbb{Z}$. Since the map $x' \to x'^p$ is injective on $F'^\times/k'^\times$, we deduce

$$(\frac{\psi(\overline{x}_1)^{N-N'}}{\psi(\overline{x}_2)^{N-N'p'}})^{p''-1} = (\frac{\psi(\overline{x}_1)^{N-N''}}{\psi(\overline{x}_2)^{N-N''p''}})^{p'-1}.$$

Since $\psi(\overline{x}_1)$, $\psi(\overline{x}_2)$ are multiplicatively independent, this forces

$$\begin{array}{c}(p''-p')N - (p''-1)N' + (p'-1)N'' = 0 \\ (p''-p')N - p'(p''-1)N' + p''(p'-1)N'' = 0\end{array}$$

Reducing modulo p'' and using that $p' \not\equiv 1\,(mod\, p'')$, one sees that the matrix

$$\left(\begin{array}{ccc}(p''-p') & -(p''-1) & (p'-1) \\ (p''-p') & -p'(p''-1) & p''(p'-1)\end{array}\right)$$

has rank 2. Since $(1,1,1)$ is a solution of the system above, we deduce $N = N' = N''$. This implies

$$\theta(\overline{x_2})^{(p'-1)} = \psi(\overline{x_2})^{Np(p'-1)}, \text{ hence } \theta(\overline{x}_2) = \psi(\overline{x_2})^{Np},$$

and

$$\theta(\overline{x}_1) = \psi(\overline{x}_1)^{Np}.$$

In particular, this shows that N does not depend on x_2. But it does not depend on x_1 either: if $y_1 \in F^\times$ is another element such that $\Psi(y_1)$ is $F'|k'$-regular then either $d\Psi(x_1), d\Psi(y_1)$ are linearly independent over F' and one applies the above with $(x_1, x_2) := (x_1, y_1)$ or one can always find $x_2 \in F^\times$ such that $d\Psi(x_1), d\Psi(x_2)$ and $d\Psi(y_1), d\Psi(x_2)$ are linearly independent over F' and one applies the above with $(x_1, x_2) := (x_1, x_2)$ and $(x_1, x_2) := (y_1, x_2)$ respectively. Since, by Lemma 20, for every $x \in F^\times \setminus F^{p\times}$ there exists $y \in F^\times$ such that $(\overline{y}, \overline{x}) \in F^\times/k^\times$ is a good pair, we deduce

$$\theta(\overline{x}) = \psi(\overline{x})^{Np},\ x \in F^\times \setminus F^{p\times}.$$

But by multiplicativity of θ, ψ this also holds for $x \in F^{p\times} \setminus k^\times$ since such an x can be written as $x = x_0^{p^s}$ for some $x_0 \in F^\times \setminus F^{p\times}$ and integer $s \geq 1$. By definition of θ, this means

$$\psi(\overline{x})^{m-Np} = \phi(\overline{x}),\ \overline{x} \in F^\times/k^\times.$$

Since $\Phi : F \tilde{\to} F'$ is a field isomorphism, this is only possible if $m - Np = \pm 1$ (otherwise, the resulting morphism of groups $\phi : F^\times/k^\times \to F'^\times/k'^\times$ would not be surjective). Since m satisfies conditions (1.1) this forces $N = 0$, $m = \pm 1$, hence

$$\psi(\overline{x}) = \phi(\overline{x})^{\pm 1},\ x \in F^\times$$

as claimed.

This concludes the proof of the surjectivity of the map $\mathrm{Isom}(F|k, F'|k') \to \overline{\mathrm{Isom}}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times)$. The injectivity follows from the unicity in Lemma 29 and the fact that for a field isomorphism $\phi : F \tilde{\to} F'$, the bijective map $F \tilde{\to} F'$, $0 \mapsto 0$, $0 \neq x \mapsto 1/\phi(x)$ is a field isomorphism if and only if $F' = \mathbb{F}_2$ (which is excluded by our assumption on the transcendence degree of $F|k$, $F'|k$).

4. The fundamental theorem of projective geometry

Lemma 29. *Let k, k' be fields and let $F|k$ and $F'|k'$ be field extensions. Let*

$$\phi : F^\times/k^\times \to F'^\times/k'^\times$$

be a group morphism. Assume that:

- *(a) ϕ is injective and preserves collinearity: for any line $L \subset F^\times/k^\times$ there is a line $L' \subset F'^\times/k'^\times$, such that $\phi(L) \subset L'$, or that*
- *(b) ϕ is an isomorphism and preserves lines: for any line $L \subset F^\times/k^\times$ there is a line $L' \subset F'^\times/k'^\times$, such that $\phi(L) = L'$.*

Assume that the image of ϕ is contained in no dimension ≤ 2 projective subspace of $F'^\times/k'^\times$. Then, in case (a) (resp., in case (b)), there is a unique field morphism (resp. isomorphism) $\Phi : F \to F'$ such that $\Phi(k) \subset k'$ (resp. $\Phi(k) = k'$) and the induced group morphism $\overline{\Phi} : F^\times/k^\times \to F'^\times/k'^\times$ coincides with ϕ.

Lemma 29 is elementary and well-known to experts. See for instance [1, Chap. II, Thm. 2.26] for a classical formulation in the setting of finite dimensional vector spaces. For the convenience of the reader, we include here a proof in the setting of (not necessarily finite) field extensions.

Recall that for $x \in F^\times$ we denote by $\overline{x}$ its image $\overline{x} \in F^\times/k^\times$.

4.1. **Definition of Φ.**

4.1.1. *Definition on* $\{0,1\}$. Set $\Phi(0)=0$, $\Phi(1)=1$.

4.1.2. *Definition on* $F\setminus k$. For every $x\in F^\times\setminus k^\times$, we have

$$\phi(\overline{1+x})=(\overline{1+x})\in \mathfrak{l}_{k'}(1,\phi(\overline{1+x})=(\overline{x})),$$

so that there exists a unique $\Phi(x)\in F'^\times$ such that

$$\overline{\Phi(x)}=\phi(\overline{x}) \text{ and } \overline{1+\Phi(x)}=\phi(\overline{1+x}).$$

4.1.3. *Definition on* $k^\times$. For every $x\in F^\times\setminus k^\times$, set $\Phi_x(0)=0$. For every $\alpha\in k^\times$,

$$\overline{\Phi(\alpha x)}=\phi(\overline{x})=\overline{\Phi(x)},$$

so that there exists a unique $\Phi_x(\alpha)\in k'^\times$ such that

$$\Phi(\alpha x)=\Phi_x(\alpha)\Phi(x)$$

Note that by definition $\Phi_x(1)=1$, $\Phi_x(k^\times)\subset k'^\times$.

Lemma 30. *For every* $x,y\in F^\times\setminus k^\times$, $\Phi_x=\Phi_y$.

Proof. Case 1: The elements 1, $\Phi(x)$, $\Phi(y)$ are linearly independent over k'. In particular, for every $\alpha\in k^\times$,

$$\mathfrak{l}_{k'}(\overline{\Phi(x)},\overline{\Phi(y)})\neq \mathfrak{l}_{k'}(\overline{1+\Phi_x(\alpha)\Phi(x)},\overline{1+\Phi_y(\alpha)\Phi(y)}).$$

Since ϕ preserves collinearity and

$$\overline{(1+\alpha x)-(1+\alpha y)}=\overline{x-y}\in \mathfrak{l}_k(\overline{x},\overline{y})\cap \mathfrak{l}_k(\overline{1+\alpha x},\overline{1+\alpha y})$$

we see that

$$\{\phi(\overline{x-y})\}=\mathfrak{l}_{k'}(\overline{\Phi(x)},\overline{\Phi(y)})\cap \mathfrak{l}_{k'}(\overline{1+\Phi_x(\alpha)\Phi(x)},\overline{1+\Phi_y(\alpha)\Phi(y)})$$

is *independent of* α while, on the other hand, a direct computation shows that for every $\alpha\in k^\times$,

$$\{\overline{\Phi_x(\alpha)\Phi(x)-\Phi_y(\alpha)\Phi(y)}\}=\mathfrak{l}_{k'}(\overline{\Phi(x)},\overline{\Phi(y)})\cap \mathfrak{l}_{k'}(\overline{1+\Phi_x(\alpha)\Phi(x)},\overline{1+\Phi_y(\alpha)\Phi(y)}).$$

This forces $\Phi_x(\alpha)=\Phi_y(\alpha)$.

Case 2: The elements 1, $\Phi(x)$, $\Phi(y)$ are linearly dependent over k'. Then, by assumption, there exists $z\in F^\times$ such that 1, $\Phi(x)$, $\Phi(z)$ (equivalently 1, $\Phi(y)$, $\Phi(z)$) are linearly independent over k'. By the above $\Phi_x=\Phi_z$ and $\Phi_y=\Phi_z$.

□

From Lemma 30, we can define Φ on $k^\times$ by setting $\Phi|_{k^\times}=\Phi_x$ for some (equivalently every) $x\in F^\times\setminus k^\times$. Note that for $\alpha=1$, this definition coincides with the one in 4.1.1.

In particular, for every $\alpha,\beta\in k^\times$ and $x\in F^\times\setminus k^\times$, we have

$$\Phi(\alpha\beta)\Phi(x)=\Phi(\alpha\beta x)=\Phi(\alpha)\Phi(\beta x)=\Phi(\alpha)\Phi(\beta)\Phi(x)$$

whence

$$\Phi(\alpha\beta)=\Phi(\alpha)\Phi(\beta).$$

Since by definition $\Phi(1)=1$, this shows that $\Phi:k^\times\to k'^\times$ is a group morphism.

4.2. We have to show that the map $\Phi : F \to F'$ defined in Subsection 4.1 is a field morphism. By definition, we already have $\Phi(0) = 0$, $\Phi(1) = 1$ and for $\alpha \in k$, $x \in F^\times \setminus k^\times$,

$$\Phi(\alpha x) = \Phi(\alpha)\Phi(x),\ \overline{\Phi(x)} = \phi(\overline{x}),\ \overline{\Phi(1+x)} = \phi(\overline{1+x}) = \overline{1+\Phi(x)}.$$

Lemma 31. *For every $x, y \in F$ we have*

$$\Phi(x+y) = \Phi(x) + \Phi(y).$$

Proof. We may assume $x, y \neq 0$.

Case 1: 1, $\Phi(x)$, $\Phi(y)$ are linearly independent over k'. Then

$$\mathfrak{l}_{k'}(\overline{1+\Phi(x)}, \overline{\Phi(y)}) \neq \mathfrak{l}_{k'}(\overline{\Phi(x)}, \overline{1+\Phi(y)}).$$

Since ϕ preserves collinearity and

$$\overline{1+x+y} \in \mathfrak{l}_k(\overline{1+x}, \overline{y}) \cap \mathfrak{l}_k(\overline{x}, \overline{1+y})$$

we see that

$$\phi(\overline{1+x+y}) = \mathfrak{l}_{k'}(\overline{1+\Phi(x)}, \overline{\Phi(y)}) \cap \mathfrak{l}_{k'}(\overline{\Phi(x)}, \overline{1+\Phi(y)})$$

while, on the other hand, a direct computation shows that

$$\overline{1+\Phi(x)+\Phi(y)} = \mathfrak{l}_{k'}(\overline{1+\Phi(x)}, \overline{\Phi(y)}) \cap \mathfrak{l}_{k'}(\overline{\Phi(x)}, \overline{1+\Phi(y)}).$$

This forces

$$\overline{1+\Phi(x+y)} = \phi(\overline{1+x+y}) = \overline{1+\Phi(x)+\Phi(y)}$$

whence $\Phi(x+y) = \Phi(x) + \Phi(y)$.

Case 2: 1, $\overline{x}$, $\overline{y}$ are all distinct in $F^\times/k^\times$ (hence 1, $\overline{\Phi(x)}$, $\overline{\Phi(y)}$ are all distinct in $F'^\times/k'^\times$; recall ϕ is injective) but 1, $\Phi(x)$, $\Phi(y)$ are linearly dependent over k'. Then, by assumption, there exists $z \in F^\times$ such that 1, $\Phi(x)$, $\Phi(z)$ (equivalently 1, $\Phi(y)$, $\Phi(z)$) are linearly independent over k'. Then, by the above, we have

(a) since 1, $\Phi(x)$, $\Phi(z)$ are linearly independent over k', we have
$$\Phi(x+z) = \Phi(x) + \Phi(z);$$
(b) since 1, $\Phi(x+y)$, $\Phi(z)$ are linearly independent over k', we have
$$\Phi(x+y+z) = \Phi(x+y) + \Phi(z);$$
(c) since 1, $\Phi(x+z) = \Phi(x) + \Phi(z)$, $\Phi(y)$ are linearly independent over k', we have
$$\Phi(x+y+z) = \Phi(x+z) + \Phi(y) = \Phi(x) + \Phi(z) + \Phi(y).$$

Combining (b), (iii), we obtain, again, $\Phi(\alpha x + \beta y) = \Phi(\alpha)\Phi(x) + \Phi(\beta)\Phi(y)$.

Case 3: $\alpha := x \in k^\times$, $x := y \in F^\times \setminus k^\times$. In 4.1.3 we established

$$\Phi(\alpha + x) = \Phi(\alpha)\Phi(1 + \alpha^{-1}x) \text{ and } \Phi(\alpha^{-1}x) = \Phi(\alpha)^{-1}\Phi(x),$$

so that it is enough to show that $\Phi(1+x) = 1 + \Phi(x)$. By assumption, there exists $y \in F$ such that 1, $\Phi(x)$, $\Phi(y)$ are linearly independent over k'. In particular, by Case 1, $\Phi(x+y) = \Phi(x) + \Phi(y)$. Then, the elements 1, $\Phi(1+x)$, $\Phi(y)$ are also linearly independent over k'. Hence, by Case 1, $\Phi(1+x+y) = \Phi(1+x) + \Phi(y)$. As a result,

$$\overline{\Phi(1+x+y)} = \overline{1+\Phi(x+y)} = \overline{1+\Phi(x)+\Phi(y)}$$

and

$$\overline{\Phi(1+x+y)} = \overline{\Phi(1+x)+\Phi(y)},$$

which forces $\Phi(1+x) = 1+\Phi(x)$.

Case 4: $\alpha := x$, $\beta := y \in k^\times$. Let $x \in F^\times \setminus k^\times$. Then, on the one hand

$$\Phi(1+\alpha x+\beta x) \overset{(1)}{=} \Phi(1+\alpha x)+\Phi(\beta x) \overset{(2)}{=} 1+\Phi(\alpha x)+\Phi(\beta x) = 1+(\Phi(\alpha)+\Phi(\beta))\Phi(x),$$

where (1) is by Case 2 and (2) is by Case 3. While, on the other hand, if $\alpha+\beta\neq 0$, Case 3 also yields

$$\Phi(1+\alpha x+\beta x) = 1+\Phi((\alpha+\beta)x) = 1+\Phi(\alpha+\beta)\Phi(x).$$

This shows $\Phi(\alpha+\beta) = \Phi(\alpha)+\Phi(\beta)$ unless $\beta = -\alpha$. For this last case, we have, by Case 3,

$$\Phi(1+\alpha x) = 1+\Phi(\alpha)\Phi(x),\ \Phi(1-\alpha x) = 1+\Phi(-\alpha)\Phi(x)$$

and, by Case 2,

$$\Phi(2) = \Phi((1+\alpha x)+(1-\alpha x)) = \Phi(1+\alpha x)+\Phi(1-\alpha x).$$

This implies

$$2+(\Phi(\alpha)+\Phi(-\alpha))x = \Phi(2)\in k'$$

hence $\Phi(\alpha)+\Phi(-\alpha) = 0$. □

Corollary 32. *For every $x, y \in F^\times$ we have*

$$\Phi(xy) = \Phi(x)\Phi(y).$$

Proof. By Lemma 31, we have

$$\Phi(x(1+y)) = \Phi(x)+\Phi(xy) \text{ and } \Phi(1+y) = 1+\Phi(y).$$

Also, since $\phi : F^\times/k^\times \to F'^\times/k'^\times$ is a group morphism, we have

$$\overline{\Phi(xy)} = \overline{\phi(xy)} = \phi(\overline{x})\phi(\overline{y}) = \overline{\Phi(x)\Phi(y)}$$

and

$$\overline{\Phi(x)+\Phi(xy)} = \overline{\Phi(x(1+y))} = \overline{\phi(\overline{x}\overline{(1+y)})} = \phi(\overline{x})\phi(\overline{1+y}) =$$
$$= \overline{\Phi(x)(1+\Phi(y))} = \overline{\Phi(x)+\Phi(x)\Phi(y)}.$$

This forces $\Phi(xy) = \Phi(x)\Phi(y)$ as claimed. □

4.3. End of the proof. At this stage, we have shown that there exists a field morphism $\Phi : F \to F'$ such that

- $\Phi(k) \subset k'$;
- the induced group morphism $\overline{\Phi} : F^\times/k^\times \to F'^\times/k'^\times$ coincides with

$$\phi : F^\times/k^\times \to F'^\times/k'^\times.$$

It remains to prove the unicity and Part (b): $\Phi : F \to F'$ is an isomorphism if $\phi : F^\times/k^\times \to F'^\times/k'^\times$ is.

4.3.1. *Unicity.* Let $\Psi : F \to F'$ be another field morphism such that $\Psi(k) \subset k'$ and $\overline{\Psi} = \phi$. Then, for every $x \in F^\times$ there exists a unique $\lambda_x \in k'^\times$ such that $\Phi(x) = \lambda_x \Psi(x)$. But necessarily we have $\lambda_1 = 1$ and, if $x \in F^\times \setminus k^\times$, so that $\Phi(x), \Psi(x) \in F'^\times \setminus k'^\times$, and

$$1 + \lambda_x \Psi(x) = 1 + \Phi(x) = \Phi(1 + x) = \lambda_{1+x} \Psi(1 + x) = \lambda_{1+x}(1 + \Psi(x)).$$

This shows $\lambda_x = \lambda_{1+x} = 1$. If $\alpha \in k^\times$ and $x \in F^\times \setminus k^\times$, we have

$$\lambda_\alpha \Psi(\alpha) \lambda_x \Psi(x) = \Phi(\alpha)\Phi(x) = \Phi(\alpha x) = \lambda_{\alpha x} \Psi(\alpha x).$$

Since $\lambda_{\alpha x} = \lambda_x = 1$ by the above, this forces $\lambda_\alpha = 1$ as well.

This concludes the proof of Lemma 29 (a).

4.3.2. *Part (b).* Lemma 29 (b) follows formally from the existence and uniqueness assertion in Lemma 29 (a). Indeed, since $\phi^{-1} : F'^\times/k'^\times \to F^\times/k^\times$ is also a group isomorphism which preserves lines, there exists a unique field morphism $\Psi : F' \to F$ such that the induced group morphism $\overline{\Psi} : F'^\times/k'^\times \to F^\times/k^\times$ coincides with $\phi^{-1} : F'^\times/k'^\times \to F^\times/k^\times$. Applying again this argument with the identity morphisms of $F^\times/k^\times$, $F'^\times/k'^\times$, one gets $\Phi \circ \Psi = Id_{F'}$, $\Psi \circ \Phi = Id_F$.

References

[1] E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.

[2] H. Bass and J. Tate. The Milnor ring of a global field. *Algebraic K-theory, II: "Classical" algebraic K-theory and connections with arithmetic (Proc. Conf., Seattle, Wash., Battelle Memorial Inst., 1972)*, pages 349–446. Lecture Notes in Math., Vol. 342, 1973.

[3] Fedor Bogomolov and Yuri Tschinkel. Milnor K_2 and field homomorphisms. In *Surveys in differential geometry. Vol. XIII. Geometry, analysis, and algebraic geometry: forty years of the Journal of Differential Geometry*, volume 13 of *Surv. Differ. Geom.*, pages 223–244. Int. Press, Somerville, MA, 2009.

[4] Fedor Bogomolov and Yuri Tschinkel. Introduction to birational anabelian geometry. In *Current developments in algebraic geometry*, volume 59 of *Math. Sci. Res. Inst. Publ.*, pages 17–63. Cambridge Univ. Press, Cambridge, 2012.

[5] François Charles and Bjorn Poonen. Bertini irreducibility theorems over finite fields. *J. Amer. Math. Soc.*, 29:81–94, 2016.

[6] Alexander Grothendieck. E.G.A. IV. Etude locale des schémas et des morphismes de schémas, troisième partie. *Publ. Math. I.H.E.S.*, 28:5–255, 1966.

[7] Jean-Pierre Jouanolou. *Théorèmes de Bertini et applications*, volume 42 of *Progress in Mathematics*. Birkhäuser, 1983.

[8] Bruno Kahn. A sheaf-theoretic reformulation of the tate conjecture. 1998. `arXiv:math/9801017`.

[9] Serge Lang. On quasi algebraic closure. *Ann. of Math. (2)*, 55:373–390, 1952.

[10] Serge Lang. *Introduction to algebraic geometry*. Interscience Publishers, Inc., New York-London, 1958.

[11] Hideyuki Matsumura. *Commutative algebra*. W. A. Benjamin, Inc., New York, 1970.

[12] A. S. Merkurjev and A. A. Suslin. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR Ser. Mat.*, 46(5):1011–1046, 1135–1136, 1982.

[13] Florian Pop. On the birational anabelian program initiated by Bogomolov I. *Invent. Math.*, 187(3):511–533, 2012.

[14] Florian Pop. Recovering function fields from their decomposition graphs. In *Number theory, analysis and geometry*, pages 519–594. Springer, New York, 2012.

[15] John Tate. Symbols in arithmetic. *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, pages 201–211, 1971.

[16] Adam Topaz. Reconstructing function fields from rational quotients of mod-ℓ Galois groups. *Math. Ann.*, 366(1-2):337–385, 2016.

[17] Adam Topaz. A Torelli theorem for higher-dimensional function fields. 2017. `arXiv:1705.01084`.

[18] Vladimir Voevodsky. Motivic cohomology with $\mathbf{Z}/2$-coefficients. *Publ. Math. Inst. Hautes Études Sci.*, (98):59–104, 2003.

[19] Vladimir Voevodsky. Reduced power operations in motivic cohomology. *Publ. Math. Inst. Hautes Études Sci.*, (98):1–57, 2003.

Anna Cadoret
IMJ-PRG – Sorbonne Université, Paris, FRANCE
anna.cadoret@imj-prg.fr

Alena Pirutka
CIMS, New York University, New York, U.S.A.
National Research University Higher School of Economics, RUSSIAN FEDERATION
pirutka@cims.nyu.edu