COMPOSITIO MATHEMATICA

On the birational p-adic section conjecture

Florian Pop

Compositio Math. **146** (2010), 621–637.

doi:10.1112/S0010437X09004436

FOUNDATION COMPOSITIO MATHEMATICA

The London Mathematical Society

Compositio Math. 146 (2010) 621–637
doi:10.1112/S0010437X09004436

On the birational p-adic section conjecture

Florian Pop

Abstract

In this article we introduce and prove a $\mathbb{Z}/p$ meta-abelian form of the birational p-adic section conjecture for curves. This is a much stronger result than the usual p-adic birational section conjecture for curves, and makes an effective p-adic section conjecture for curves quite plausible.

1. Introduction

Let $X \to k$ be a complete geometrically integral smooth curve over a field k. Recall that Grothendieck's 'section conjecture', which evolved from his *Esquisse d'un Programme* of 1983 (see [Gro98a]) and *Letter to Faltings* of 1984 (see [Gro98b]), predicts that under certain 'anabelian hypotheses' π_1 gives rise to a bijection between the k-rational points of X, which are actually the sections of $X \to k$, and the (conjugacy classes) of sections of $\pi_1(X) \to \pi_1(k)$.

The aim of this article is to formulate and prove a very 'minimalistic' birational variant of this conjecture in the case where k is a finite field extension of $\mathbb{Q}_p$.

To begin with, let k be an arbitrary base field and $K|k$ the function field of a complete geometrically integral smooth curve $X \to k$. Let $\tilde{K}|K$ be some Galois extension, and let $\mathrm{Gal}(\tilde{K}|K)$ denote its Galois group. Further, let $\tilde{k} := \overline{k} \cap \tilde{K}$ be the 'constants' of $\tilde{K}$, and consider the resulting canonical exact sequence

$$1 \to \mathrm{Gal}(\tilde{K}|K\tilde{k}) \longrightarrow \mathrm{Gal}(\tilde{K}|K) \xrightarrow{\tilde{\mathrm{pr}}_K} \mathrm{Gal}(\tilde{k}|k) \to 1.$$

Let $\tilde{X} \to X$ be the normalization of X in the field extension $K \hookrightarrow \tilde{K}$. For $x \in X$ and $\tilde{x} \in \tilde{X}$ above x, let T_x and Z_x, with $T_x \subseteq Z_x$, be the inertia and decomposition groups of $\tilde{x}|x$, respectively, and let $G_x := \mathrm{Aut}(\kappa(\tilde{x})|\kappa(x))$ be the residual automorphism group. By decomposition theory, one has a canonical exact sequence

$$1 \to T_x \to Z_x \to G_x \to 1. \qquad (*)$$

Suppose next that x is k-rational, i.e. $\kappa(x) = k$. Since $\tilde{k} \subset \kappa(\tilde{x})$, the projection $Z_x \xrightarrow{\tilde{\mathrm{pr}}_K} \mathrm{Gal}(\tilde{k}|k)$ gives rise to a canonical surjective homomorphism $G_x \to \mathrm{Gal}(\tilde{k}|k)$, which in general is not injective. Nevertheless, if $\tilde{k} = \kappa(\tilde{x})$, then $G_x \to \mathrm{Gal}(\tilde{k}|k)$ is an isomorphism. Hence, if the exact sequence $(*)$ splits, then $\tilde{\mathrm{pr}}_K$ has sections $\tilde{s}_x : \mathrm{Gal}(\tilde{k}|k) \to Z_x \subset \mathrm{Gal}(\tilde{K}|K)$, called *sections above* x; also, notice that the conjugacy classes of the sections $\tilde{s}_x$ above x build a 'bouquet' which is in canonical bijection with the (non-commutative) continuous cohomology pointed set $\mathrm{H}^1_{\mathrm{cont}}(\mathrm{Gal}(\tilde{k}|k), T_x)$ defined via the split exact sequence $(*)$.

Received 27 July 2008, accepted in final form 9 June 2009, published online 18 March 2010.
2000 Mathematics Subject Classification 11G, 14G (primary), 12E30 (secondary).
Keywords: anabelian geometry, (étale) fundamental groups, p-adically closed fields, local–global principles for Brauer groups, rational points, valuations, Hilbert decomposition theory.
This work was supported by NSF grants DMS-0401056 and DMS-0801144.

Note that if $\mathrm{char}(k)=0$, then T_x is $\mathrm{Gal}(\tilde{k}|k)$-isomorphic to a quotient of $\widehat{\mathbb{Z}}(1)$ and thus abelian; hence $\mathrm{H}^1_{\mathrm{cont}}(\mathrm{Gal}(\tilde{k}|k), T_x)$ is a group. Furthermore, if $\tilde{K}=K^{\mathrm{s}}$ and $\tilde{k}=k^{\mathrm{s}}$ are separable closures of K and k, then $G_x=\mathrm{Gal}(k^{\mathrm{s}}|k)$ and ($*$) is split, and thus sections above x exist; moreover, if $\mathrm{char}(k)=0$, then $T_x\cong\widehat{\mathbb{Z}}(1)$ as G_k-modules, and hence $\mathrm{H}^1_{\mathrm{cont}}(G_k, T_x)\cong\widehat{k^\times}$ via Kummer theory.

If v is an arbitrary valuation of K and $\tilde{v}$ is a prolongation of v to $\tilde{K}$, then we denote by T_v and Z_v, with $T_v\subseteq Z_v$, the inertia and decomposition groups of $\tilde{v}|v$, respectively, and by $G_v=Z_v/T_v$ the residual automorphism group. If $\tilde{s}_v:\mathrm{Gal}(\tilde{k}|k)\to Z_v\subseteq\mathrm{Gal}(\tilde{K}|K)$ is a section of $\tilde{\mathrm{pr}}_K$, then we say that $\tilde{s}_v$ is a *section above* v.

Next, let p be a fixed prime number. We denote by $K'|K$ a maximal $\mathbb{Z}/p$ elementary abelian extension of K and by K'' a maximal $\mathbb{Z}/p$ elementary abelian extension of K'. Then $K''|K$ is a Galois extension, which we shall call the maximal $\mathbb{Z}/p$ *elementary meta-abelian extension* of K. Note that $k':=\overline{k}\cap K'$ and $k'':=\overline{k}\cap K''$ are, respectively, the maximal $\mathbb{Z}/p$ elementary abelian extension and the maximal $\mathbb{Z}/p$ elementary meta-abelian extension of k. We further consider the canonical surjective projections

$$\mathrm{pr}'_K:\mathrm{Gal}(K'|K)\to\mathrm{Gal}(k'|k),\quad \mathrm{pr}''_K:\mathrm{Gal}(K''|K)\to\mathrm{Gal}(k''|k).$$

We will say that a section $s':\mathrm{Gal}(k'|k)\to\mathrm{Gal}(K'|K)$ of pr'_K is *liftable* if there exists a section $s'':\mathrm{Gal}(k''|k)\to\mathrm{Gal}(K''|K)$ of pr''_K which lifts s' to $\mathrm{Gal}(k''|k)$.

Note that if the pth roots of unity μ_p are contained in k and hence in K, then by Kummer theory we have $K'=K[\sqrt[p]{K}\,]$ and $K''=K'[\sqrt[p]{K'}\,]$, and similarly for k.

From now on, suppose in the above context that k is a finite extension of $\mathbb{Q}_p$. Then the promised 'minimalistic' form of the birational p-adic section conjecture is the following.

Theorem A. *In the above notation, suppose that $\mu_p\subset k$. Then the following hold.*

(1) *Every k-rational point $x\in X$ gives rise to a bouquet of conjugacy classes of liftable sections $s'_x:\mathrm{Gal}(k'|k)\to\mathrm{Gal}(K'|K)$ above x, which is in bijection with $\mathrm{H}^1(\mathrm{Gal}(k'|k),\mathbb{Z}/p(1))$.*

(2) *Let $s':\mathrm{Gal}(k'|k)\to\mathrm{Gal}(K'|K)$ be a liftable section. Then there exists a unique k-rational point $x\in X$ such that s' equals one of the sections s'_x defined above.*

Actually, one can reformulate the question addressed by Theorem A in terms of p-adic valuation and obtain the following stronger result. See § 2-H. for definitions, notation and a few facts on p-adically closed fields and p-adic valuations v (for example, the p-adic rank d_v of v), and see [AK66, PR85] for proofs.

Theorem B. *Let k be a p-adically closed field with p-adic valuation v, and suppose that $\mu_p\subset k$. Let $K|k$ be a field extension with transcendence degree* $\mathrm{tr.deg}(K|k)=1$. *Then the following hold.*

(1) *Let w be a p-adic valuation of K with $d_w=d_v$. Then w prolongs v to K and gives rise to a bouquet of conjugacy classes of liftable sections $s'_w:\mathrm{Gal}(k'|k)\to\mathrm{Gal}(K'|K)$ above w.*

(2) *Let $s':\mathrm{Gal}(k'|k)\to\mathrm{Gal}(K'|K)$ be a liftable section. Then there exists a unique p-adic valuation w of K such that $d_w=d_v$, and $s'=s'_w$ for some s'_w as above.*

Remarks.

(1) First, observe that the above assertions do not hold if $\mu_p\not\subset k$. Indeed, if $\mu_p\not\subset k$, then the maximal pro-p quotient $G_k(p)$ of G_k is a pro-p free group on $[k:\mathbb{Q}_p]+1$ generators; see, e.g., [NSW08, Theorem 7.5.11]. From this it follows that all the sections $s':\mathrm{Gal}(k'|k)\to\mathrm{Gal}(K'|K)$ of pr'_K are liftable. Thus, for X with $X(k)$ empty, we have that pr'_K has liftable

sections but that none of these originate from k-rational points of X. (Actually, the same holds for all curves X as above, even when $X(k)$ is non-empty.)

(2) Nevertheless, in the case where μ_p is not contained in the base field, assertions similar to Theorems A and B hold in the following form. Let $l|\mathbb{Q}_p$ be some finite extension and $Y \to l$ a complete geometrically integral smooth curve with function field $L = \kappa(Y)$. Let $k|l$ be a finite Galois extension with $\mu_p \subset k$. Setting $K := Lk$, consider the field extensions $K'|K \hookrightarrow K''|K$ and $k'|k \hookrightarrow k''|k$ as above. Then $k' = K' \cap \bar{l}$ and $k'' = K'' \cap \bar{l}$; moreover, $K'|L$ and $K''|L$, as well as $k'|l$ and $k''|l$, are Galois extensions too, and one gets surjective canonical projections

$$\mathrm{pr}'_L : \mathrm{Gal}(K'|L) \to \mathrm{Gal}(k'|l), \quad \mathrm{pr}''_L : \mathrm{Gal}(K''|L) \to \mathrm{Gal}(k''|l).$$

As above, we will say that a section $s'_L : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ of pr'_L is *liftable* if there exists a section $s''_L : \mathrm{Gal}(k''|l) \to \mathrm{Gal}(K''|L)$ of pr''_L which lifts s'_L. Then one has the following extensions of Theorems A and B.

Theorem A^0. *With the above notation and hypothesis, the following hold.*

(1) *Every l-rational point $y \in Y$ gives rise to a bouquet of conjugacy classes of liftable sections $s'_y : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ above y, which is in bijection with $\mathrm{H}^1(\mathrm{Gal}(k'|l), \mathbb{Z}/p(1))$.*

(2) *Let $s'_L : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ be a liftable section. Then there exists a unique l-rational point $y \in Y$ such that s'_L equals one of the sections s'_y defined above.*

Theorem B^0. *Let l be a p-adically closed field with p-adic valuation v, and let $L|l$ be a field extension with transcendence degree $\mathrm{tr.deg}(L|l) = 1$. Then, in the above notation, the following hold.*

(1) *Let w be a p-adic valuation of L with $d_w = d_v$. Then w prolongs v to L and gives rise to a bouquet of conjugacy classes of liftable sections $s'_w : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ above w.*

(2) *Let $s'_L : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ be a liftable section. Then there exists a unique p-adic valuation w of L such that $d_w = d_v$, and s'_L equals one of the sections s'_w as above.*

Notice that Theorem A^0 obviously implies the full Galois birational p-adic section conjecture, but not vice versa; see Koenigsmann [Koe05] for a proof of the latter (among other things), as well as Remark 7 in this paper.

Indeed, for given $Y \to l$ with function field $L = \kappa(Y)$ as above, let $s : G_l \to G_L$ be a section of the canonical projection $G_L \to G_l$.

(a) Consider finite field extensions $L_i|L$ with $\mathrm{im}(s) \subset G_{L_i}$, and let $Y_i \to l$ be a complete smooth curve with function field $L_i = \kappa(Y_i)$. Notice that $Y_i \to l$ is geometrically integral.

(b) Consider finite Galois extensions $k_i|l$ with $\mu_p \subset k_i$, and set $K_i := L_i k_i$. Let $\phi'_i : G_l \to \mathrm{Gal}(k'_i|l)$ and $\psi'_i : G_{L_i} \to \mathrm{Gal}(K'_i|L_i)$ be the canonical projections.

Then s gives rise functorially (in L_i and k_i) to liftable sections $s'_i : \mathrm{Gal}(k'_i|l) \to \mathrm{Gal}(K'_i|L_i)$ of the canonical projection $\mathrm{pr}'_i : \mathrm{Gal}(K'_i|L_i) \to \mathrm{Gal}(k'_i|l)$ such that for $k_i \subseteq k_j$ and $L_i \subseteq L_j$, and thus for $K_i \subseteq K_j$, one has $s'_i = \mathrm{pr}_{ji} \circ s'_j$ where $\mathrm{pr}_{ji} : \mathrm{Gal}(K'_j|L_j) \to \mathrm{Gal}(K'_i|L_i)$ is the canonical projection. By Theorem A^0, there exists a unique l-rational point $y_i \in Y_i(l)$ such that $s'_i = s'_{y_i}$ in the usual way; and since $s'_i = \mathrm{pr}_{ji} \circ s'_j$, the uniqueness of $y_i \in Y_i(l)$ implies that the canonical morphism $Y_j \to Y_i$ maps $y_j \in Y_j(l)$ to $y_i \in Y_i(l)$ and that $s'_{y_i} = \mathrm{pr}_{ji} \circ s'_{y_j}$. We conclude from this that if $y \in Y(l)$ is the common image of all the points $y_i \in Y_i(l)$ in $Y(l)$, then one has $s = \varprojlim_i s'_i = \varprojlim_i s'_{y_i} = s_y$.

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press

As an application of the results and techniques developed here, one can prove the following fact concerning the p-adic section conjecture for curves. Let $k|\mathbb{Q}_p$ be a finite extension and $X \to k$ a hyperbolic curve. Then there exists a finite *effectively computable* family of finite geometrically $\mathbb{Z}/p$ elementary abelian (ramified) covers $\varphi_i : X_i \to X$, $i \in I$, satisfying:

(i) $\bigcup_i \varphi_i(X_i(k)) = X(k)$, i.e. every k-rational point of X 'survives' in at least one of the covers $X_i \to X$;

(ii) a section $s : G_k \to \pi_1(X)$ can be lifted to a section $s_i : G_k \to \pi_1(X_i)$ for some $i \in I$ if and only if s arises from a k-rational point $x \in X(k)$ in the manner described above.

The details of the proof will be given later.

With regard to the proofs of the above theorems, the main technical point is a generalization of the Tate–Roquette–Lichtenbaum local–global principle for Brauer groups of function fields of curves over p-adically closed fields, as introduced and studied in [Pop88]. As a result of this generalization, one is led to analyze the cohomological behavior of $\mathbb{Z}/p$ elementary abelian extension of Henselizations of the function fields under consideration.

2. Generalities

A. $\mathbb{Z}/p$ derived series and quotients

Let G be a profinite group. We denote by G^i the derived $\mathbb{Z}/p$ series of G; hence, by definition, we have $G^1 := G$ and $G^{i+1} := [G^i, G^i](G^i)^p$ for $i > 0$. We will further set $\overline{G}^{\,i} := G^1/G^{i+1}$ for $i > 0$. Hence, in particular, $\overline{G}' := G^1/G^2$ is the maximal $\mathbb{Z}/p$ elementary quotient of G, and $\overline{G}'' := G^1/G^3$ is the maximal $\mathbb{Z}/p$ elementary meta-abelian quotient of G, i.e. the maximal quotient of G which is an extension of $\overline{G}'$ by some $\mathbb{Z}/p$ elementary abelian extension.

One can check without difficulty that mapping every profinite group G to $\overline{G}^{\,i}$, for $i > 0$, defines a functor from the category of all profinite groups onto the category of all pro-p groups whose derived $\mathbb{Z}/p$ series has length no greater than i. In particular, if $\mathrm{pr} : G \to H$ is a (surjective) morphism of profinite groups, then the following hold:

(1) pr gives rise canonically to a (surjective) morphism $\mathrm{pr}^i : \overline{G}^{\,i} \to \overline{H}^i$;

(2) every section $s : H \to G$ of $\mathrm{pr} : G \to H$ gives rise to a section $s^i : \overline{H}^i \to \overline{G}^{\,i}$ of pr^i.

Finally, in the above context, we say that a section $s' : \overline{H}' \to \overline{G}'$ of pr' is *liftable* if there exists a section $s'' : \overline{H}'' \to \overline{G}''$ of pr'' which reduces to s' or, equivalently, lifts s'.

B. Cohomology and sections

Let G be a profinite group. We endow $\mathbb{Z}/p$ with the trivial G-action and let $\mathrm{H}^n(G, \mathbb{Z}/p)$ be the cohomology groups of G with values in $\mathbb{Z}/p$. Then, in the notation of the previous subsection, for all $i > 0$ we have

$$\mathrm{H}^1(G, \mathbb{Z}/p) = \mathrm{Hom}(G, \mathbb{Z}/p) = \mathrm{Hom}(\overline{G}^{\,i}, \mathbb{Z}/p) = \mathrm{H}^1(\overline{G}^{\,i}, \mathbb{Z}/p),$$

and for every i the cup product gives rise to a canonical pairing

$$\mathrm{Hom}(\overline{G}^{\,i}, \mathbb{Z}/p) \times \mathrm{Hom}(\overline{G}^{\,i}, \mathbb{Z}/p) = \mathrm{H}^1(\overline{G}^{\,i}, \mathbb{Z}/p) \times \mathrm{H}^1(\overline{G}^{\,i}, \mathbb{Z}/p) \xrightarrow{\cup^i} \mathrm{H}^2(\overline{G}^{\,i}, \mathbb{Z}/p).$$

Next, let $\mathrm{pr} : G \to H$ be a quotient of G, and let $\mathrm{pr}' : \overline{G}' \to \overline{H}'$ and $\mathrm{pr}'' : \overline{G}'' \to \overline{H}''$ be the corresponding surjective projections as introduced in the previous subsection.

Lemma 1. *In the above notation, let* $s' : \overline{H}' \to \overline{G}'$ *be a liftable section of* $\mathrm{pr}' : \overline{G}' \to \overline{H}'$ *and let* $\Gamma \subseteq G$ *be the preimage of* $s'(\overline{H}') \subseteq \overline{G}'$ *under the canonical projection* $G \to \overline{G}'$. *Then, for characters* $\chi_H, \psi_H \in \mathrm{Hom}(H, \mathbb{Z}/p)$ *and the induced characters* $\chi_\Gamma, \psi_\Gamma \in \mathrm{Hom}(\Gamma, \mathbb{Z}/p)$, *the following are equivalent:*

(i) $\chi_H \cup \psi_H = 0$ *in* $\mathrm{H}^2(\overline{H}'', \mathbb{Z}/p)$;

(ii) $\chi_H \cup \psi_H = 0$ *in* $\mathrm{H}^2(H, \mathbb{Z}/p)$;

(iii) $\chi_\Gamma \cup \psi_\Gamma = 0$ *in* $\mathrm{H}^2(\Gamma, \mathbb{Z}/p)$.

Proof. The implications (i) ⇒ (ii) and (ii) ⇒ (iii) follow from taking the inflation maps coming from the surjective group homomorphisms $\Gamma \to H \to \overline{H}''$. One proves (iii) ⇒ (i) as follows. Suppose that $\chi_\Gamma \cup \psi_\Gamma = \delta(\varphi)$ is the co-boundary of some map $\varphi : \Gamma \to \mathbb{Z}/p$. We claim that φ factors through the canonical projection $\Gamma \to \overline{H}''$. Indeed, $\chi_\Gamma \cup \psi_\Gamma = \delta(\varphi)$ means that

$$(\chi_\Gamma \cup \psi_\Gamma)(g, h) = g\,\varphi(h) - \varphi(gh) + \varphi(g) = \varphi(h) - \varphi(gh) + \varphi(g) \quad \text{for all } g, h \in \Gamma,$$

where the last equality holds by virtue of the fact that G, and hence Γ, acts trivially on $\mathbb{Z}/p$. Now, if g or h lies in $G^2 \subset \Gamma$, then we have $(\chi_\Gamma \cup \psi_\Gamma)(g, h) = 0$. Equivalently, if g or h lies in $G^2 \subset \Gamma$, then $\varphi(g) - \varphi(gh) + \varphi(h) = 0$ and thus, in particular, the restriction of φ to G^2 is a group homomorphism to $\mathbb{Z}/p$. Hence the restriction of φ to $G^3 = [G^2, G^2](G^2)^p$ is trivial and, finally, φ factors through $\Gamma/G^3 \subset \overline{G}''$. Therefore, $\chi_G \cup \psi_G = 0$ in $\mathrm{H}^2(\Gamma/G^3, \mathbb{Z}/p)$. Now let $s'' : \overline{H}'' \to \overline{G}''$ be a lifting of the section s', and observe that $s''(\overline{H}'') \subseteq \Gamma/G^3$. Then the restriction of $\chi_G \cup \psi_G = 0$ to $s''(\overline{H}'') \subseteq \Gamma/G^3$ is trivial too, i.e. $\chi_H \cup \psi_H = 0$ in $\mathrm{H}^2(s''(\overline{H}''), \mathbb{Z}/p)$. Thus, finally, $\chi_H \cup \psi_H = 0$ in $\mathrm{H}^2(\overline{H}'', \mathbb{Z}/p)$, as claimed. □

C. Basics from Galois cohomology

Let K be an arbitrary field of characteristic other than p, and let G_K be its absolute Galois group. Further, let G_K^i and $\overline{G}_K^i$ be, respectively, the derived $\mathbb{Z}/p$ series and quotients of G_K. We recall the following fundamental facts.

(a) By Kummer theory, one has a canonical isomorphism $K^\times/p = \mathrm{H}^1(G_K, \mu_p)$. In particular, if $\mu_p \subset K$, then the absolute Galois group G_K acts trivially on μ_p; hence, upon choosing some identification $\imath : \mu_p \to \mathbb{Z}/p$ of trivial G_K modules, we get

$$K^\times/p = \mathrm{H}^1(G_K, \mu_p) = \mathrm{Hom}(\mathrm{Gal}(K'|K), \mu_p) \xrightarrow{\imath} \mathrm{Hom}(\mathrm{Gal}(K'|K), \mathbb{Z}/p).$$

(b) Let ${}_p\mathrm{Br}(K)$ denote the p-torsion subgroup of $\mathrm{Br}(K)$. Then ${}_p\mathrm{Br}(K) = \mathrm{H}^2(G_K, \mu_p)$ canonically. Hence, if $\mu_p \subset K$, then $\imath : \mu_p \to \mathbb{Z}/p$ gives rise to an isomorphism

$${}_p\mathrm{Br}(K) = \mathrm{H}^2(G_K, \mu_p) \xrightarrow{\imath} \mathrm{H}^2(G_K, \mathbb{Z}/p).$$

(c) Consider the cup product $K^\times/p \otimes K^\times/p \xrightarrow{\cup} \mathrm{H}^2(G_K, \mu_p \otimes \mu_p)$, $(a, b) \mapsto \chi_a \cup \chi_b$, which is actually surjective by the Merkurjev–Suslin theorem. If $\mu_p \subset K$, then the isomorphism $\imath : \mu_p \to \mathbb{Z}/p$ gives rise to a surjective morphism

$$K^\times/p \otimes K^\times/p \xrightarrow{\cup} \mathrm{H}^2(G_K, \mathbb{Z}/p), \quad (a, b) \mapsto \chi_a \cup \chi_b.$$

Combining these observations with Lemma 1 above, we deduce the following result. Let $K|k$ be a regular field extension, and suppose that $\mathrm{char}(k) \neq p$ and $\mu_p \subset k$. As in the Introduction, we consider a maximal $\mathbb{Z}/p$ elementary abelian extension $K'|K$ of K, the corresponding $k' := K' \cap \overline{k}$

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press

etc. and the resulting canonical surjective projections

$$\mathrm{pr}'_K : \mathrm{Gal}(K'|K) \to \mathrm{Gal}(k'|k), \quad \mathrm{pr}''_K : \mathrm{Gal}(K''|K) \to \mathrm{Gal}(k''|k).$$

Lemma 2. *In the above context, let $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ be a liftable section of pr'_K and let $M \subset K'$ be the fixed field of $\mathrm{im}(s')$ in K'. Then for any elements $a, b \in k^\times$ and the corresponding p-cyclic k-algebras $A_k(a, b)$ and $A_M(a, b)$, we have that $A_k(a, b)$ is trivial in $\mathrm{Br}(k)$ if and only if $A_M(a, b)$ is trivial in $\mathrm{Br}(M)$.*

D. Hilbert decomposition in elementary $\mathbb{Z}/p$ abelian extensions

Let K be a field of characteristic not equal to p that contains μ_p. Let v be a valuation of K and let v' be some prolongation of v to K'. Let $V_{v'}$, $T_{v'}$ and $Z_{v'}$ with $V_{v'} \subseteq T_{v'} \subseteq Z_{v'}$ be, respectively, the ramification, inertia and decomposition groups of $v'|v$ in $\mathrm{Gal}(K'|K)$. We remark that because $\mathrm{Gal}(K'|K)$ is commutative, the groups $V_{v'}$, $T_{v'}$ and $Z_{v'}$ depend only on v; therefore we will simply denote them by V_v, T_v and Z_v. Finally, we denote by $K^Z \subseteq K^T \subseteq K^V$ the corresponding fixed fields in K'.

Lemma 3. *With the above notation, the following statements hold.*

(1) *Let $U^v := 1 + p^2\mathfrak{m}_v$. Then K^Z contains $\sqrt[p]{U^v}$ and we have $K^Z = K[\sqrt[p]{U^v}\ ]$, provided that p is a v-unit. In particular, if w_1 and w_2 are independent valuations of K, then $Z_{w_1} \cap Z_{w_2} = \{1\}$.*

(2) *If $p \neq \mathrm{char}(Kv)$, then $V_v = \{1\}$ and $K'v' = (Kv)'$, and hence $G_v := Z_v/T_v = \mathrm{Gal}(Kv'|Kv)$. If $p = \mathrm{char}(Kv)$, then $V_v = T_v$, and the residue field $K'v'$ contains $(Kv)^{1/p}$ and the maximal $\mathbb{Z}/p$ elementary abelian extension of Kv.*

(3) *Let $L := K_v^{\mathrm{h}}$ be the Henselization of K with respect to v. Then $L' = LK'$ is a maximal $\mathbb{Z}/p$ elementary extension of L. Therefore we have $\mathrm{Gal}(L'|L) \cong Z_v$ canonically.*

Proof. (1) Everything is clear, except maybe the assertion concerning the independent valuations w_1 and w_2. To prove this, consider an arbitrary $x \neq 0$. Since w_1 and w_2 are independent, there exists $y \neq 0$ which is arbitrarily w_1-close to 1 and arbitrarily w_2-close to x. More precisely, there exists $y \neq 0$ such that, first, $w_1(1-y) > 2w_1(p)$ and, second, $w_2(x-y) > 2w_2(p) + w_2(x)$ or, equivalently, $w_2(1-y/x) > 2w_2(p)$. But then, by the first assertion of the lemma, we have $\sqrt[p]{y} \in K^{Z_{w_1}}$ and $\sqrt[p]{y/x} \in K^{Z_{w_2}}$, hence $\sqrt[p]{x} \in K^{Z_{w_2}} K^{Z_{w_1}}$. Since $K^{Z_{w_2}} K^{Z_{w_1}} = (K')^{Z_{w_2} \cap Z_{w_1}}$ and $x \in K^\times$ was arbitrary, we get $K' \subseteq (K')^{Z_{w_2} \cap Z_{w_1}}$. Therefore $Z_{w_2} \cap Z_{w_1} = 1$ as claimed.

(2) If $p \neq \mathrm{char}(Kv)$, then everything is clear by Kummer theory and general valuation theory. If $p = \mathrm{char}(Kv)$ and $p \neq \mathrm{char}(K)$, it follows that $\mathrm{char}(K) = 0$. Recall that by Artin–Schreier theory, the maximal $\mathbb{Z}/p$ elementary abelian extension of Kv is generated by the roots of all the Artin–Schreier polynomials $Y^p - Y - \overline{a}$, with $\overline{a} \in Kv$. We show that every such polynomial has a root in the residue field of some $\mathbb{Z}/p$ cyclic extension $K[\alpha]$ with $\alpha^p = u$ for some $u \in K$. Indeed, by the general non-sense of Kummer theory versus Artin–Schreier theory, one has the following.

Let $X^p - u \in \mathcal{O}_v[X]$ be some Kummer polynomial over K. We note that $\lambda := \zeta_p - 1 \in K$, as $\mu_p \subset K$, and recall that $p = \prod_{0<\mu<p}(1-\zeta_p^\mu)$. Since $1 - \zeta_p^\mu = -\lambda(1 + \cdots \zeta_p^{\mu-1})$ and thus, in particular, $(1 + \cdots \zeta_p^{\mu-1}) \equiv \mu \pmod{\lambda}$, we finally get $p \equiv \lambda^{p-1}(p-1)! \equiv -\lambda^{p-1} \pmod{\lambda^p}$, because $(p-1)! \equiv -1 \pmod{p}$ by Wilson's theorem. Hence, upon setting $X := \lambda X_0 + 1$ and $u := \lambda^p u_0 + 1$, the equation $X^p = u$ is equivalent to the equation $X_0^p - X_0 + \lambda f(X_0) = u_0$, where $f(X_0) \in \mathcal{O}_v[X_0]$ is an explicitly computable polynomial. Therefore, if $\wp = \mathrm{Frob} - \mathrm{id}$ is the Artin–Schreier operator and $\overline{u}_0 \in Kv \backslash \wp(Kv)$, then v is totally inert in $K_u := K[\sqrt[p]{u}\,]$. And, if w is the unique prolongation of v to K_u, then the residue field of w is $K_u w = (Kv)[\beta]$ with $\beta^p - \beta = \overline{u}_0$.

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press

By reversing the process above, we can see that each Artin–Schreier extension of Kv is obtained by reducing a properly chosen Kummer $\mathbb{Z}/p$ extension of K.

(3) First, if v has rank one, then K is dense in $L := K^{\mathrm{h}}_v$. Hence, given $\hat{u} \in \mathcal{O}_L$, there exists $u \in \mathcal{O}_K$ such that $\hat{u} = u(1+\eta)$ in K^{h} with $v^{\mathrm{h}}(\eta) > 2v^{\mathrm{h}}(p)$. But then $1+\eta$ is a pth power in K^{h} by Hensel's lemma, and hence the roots of $X^p - u$ and the roots of $X^p - \hat{u}$ generate the same field extension of K^{h}. To treat the general case, one uses induction on the rank of the valuation v and then 'takes limits'. □

E. Elementary $\mathbb{Z}/p$ abelian extensions of Henselian fields

In this subsection, we will prove a technical result concerning elementary $\mathbb{Z}/p$ abelian extensions of Henselian fields. The context is as follows. Let L be a Henselian field with respect to a valuation w. Suppose that $\mathrm{char}(L) = 0$ and $\mathrm{char}(Lw) = p > 0$, and that $\mu_p \subset L$. Further, let $L' = L[\sqrt[p]{L^\times}]$ be the maximal elementary $\mathbb{Z}/p$ abelian extension of L and $\mathrm{Gal}(L'|L) := \mathrm{Gal}(L'|L)$ its Galois group. Since w is Henselian, w has a unique prolongation to L', which we again denote by w.

Lemma 4. *In the above context, suppose that w is a rank-one valuation. Let $\Lambda|L$ be a subextension of $L'|L$ such that $L'|\Lambda$ is a finite extension. Then the following hold.*

(1) *$L'w \mid \Lambda w$ is finite, and Λw contains $(Lw)^{1/p}$.*

(2) *If Lw is not finite, or if $wL \not\approx \mathbb{Z}$, then for every $u \in L$ there exists $t \in L^\times$ which satisfies $L_t := L[\sqrt[p]{t}\,] \subseteq \Lambda$ and $w(u) \in p \cdot wL_t \subseteq p \cdot w(\Lambda)$. Hence $wL \subseteq p \cdot w\Lambda$.*

(3) *In particular, if $wL \not\subseteq p \cdot w\Lambda$, then $wL \approx \mathbb{Z}$ and Lw is finite.*

Proof. The proof is inspired by [Pop88, Korollar 2.7] and uses in an essential way [Pop88, Lemma 2.6]. Let $\mathcal{O}$ and $\mathfrak{m}$ be, respectively, the valuation ring and valuation ideal of w. Then, by [Pop88, Lemma 2.6], one has exact sequences of the form

$$1 \to \mathcal{O}^\times/p \to L^\times/p \to w(L)/p \to 1 \quad \text{and} \quad 1 \to (1+\mathfrak{m})/p \to \mathcal{O}^\times/p \to (Lw)^\times/p \to 1. \qquad (*)$$

By Kummer theory (note that $\mu_p \subset L$ by hypothesis), one has $\Lambda = L[\sqrt[p]{\Delta}]$ for a subgroup $\Delta \subset L^\times$ such that Δ contains the pth powers of all the elements of $L^\times$ and $L^\times/\Delta$ is canonically Pontrjagin dual (hence non-canonically isomorphic) to $\mathrm{Gal}(L'|\Lambda)$. In particular, $L^\times/\Delta = (L^\times/p)/(\Delta/p)$ is a finite elementary $\mathbb{Z}/p$ abelian group. Hence, from the above exact sequences $(*)$ it follows that upon setting $\Delta_0 := \Delta \cap \mathcal{O}^\times$ and $\Delta_1 := \Delta \cap (1+\mathfrak{m})$ we have that $(1+\mathfrak{m})/\Delta_1$ and $\mathcal{O}^\times/\Delta_0$ are finite groups; moreover, if Δw denotes the image of Δ_0 in $Lw^\times$, then $Lw^\times/\Delta w$ is a finite group.

(1) First, if Lw is finite, then Lw is perfect and thus there is nothing to prove. Now suppose that Lw is infinite. Then since $Lw^\times/\Delta w$ is finite, it follows that Δw is infinite too. Hence, for every $a \in Lw$, there exist $x \neq y$ in Δw such that $a - x, a - y \neq 0$ and $(a-x)\Delta w = (a-y)\Delta w$. Equivalently, there exists $z \in \Delta w$ such that $a - x = z(a-y)$ and hence $a = (x - yz)/(1-z)$. On the other hand, since $x, y, z \in \Delta w$, one has $x^{1/p}, y^{1/p}, x^{1/p} \in (\Delta w)^{1/p} \subset \Lambda w$ and thus $a^{1/p} \in \Lambda w$. Since a was arbitrary, we get $(Lw)^{1/p} \subseteq \Lambda w$ as claimed.

(2) From the discussion above it follows that $(1+\mathfrak{m})/\Delta_1$ is finite. Let $1 + a_j$, $1 \leqslant j \leqslant n$, be representatives for $(1+\mathfrak{m})/\Delta_1$.

Case (i). w is not discrete on L. Then for every $u \in L^\times$ there exists some $u_1 \in L^\times$ such that $0 < w(uu_1^p) < w(p), w(a_j)$ for all $j = 1, \ldots n$. Since $1 + uu_1^p \in 1 + \mathfrak{m}$, there exists j and

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press

some $t \in \Delta_1$ such that

$$1 + uu_1^p = t(1 + a_j).$$

Set $t = 1 + a$. Since $0 < w(uu_1^p) < w(p), w(a_j)$, it immediately follows from the ultra-metric triangle inequality that $w(uu_1^p) = w(a)$. On the other hand, since $t \in \Delta$, one has $t = \theta^p$ for some $\theta \in \Lambda$, i.e. $L_t := L[\sqrt[p]{t}\,] = L[\theta] \subseteq \Lambda$. Hence $1 + a = \theta^p$ and, upon setting $\theta = 1 + b$, one gets $1 + a = (1 + b)^p$. From this we obtain $w(b) > 0$. Since $w(a) = w(uu_1^p) < w(p)$ and $1 + a = (1 + b)^p$, the ultra-metric triangle inequality implies that $w(a) = w(b^p)$ in wL_t. Thus one has

$$w(u) + pw(u_1) = w(uu_1^p) = w(a) = p \cdot w(b),$$

and hence $w(u) = pw(b) - pw(u_1) \in p \cdot wL_t$ as claimed.

Case (ii). w is discrete on L. Suppose that Lw is not finite. Let $\mathfrak{m}$ and $\mathcal{O}$, with $\mathfrak{m} \subset \mathcal{O} \subset L$, be the valuation ideal and valuation ring of w in L, respectively. Since L contains μ_p and $p \geqslant 2$, it follows that we have the inclusions $(1 + \mathfrak{m})^p \subseteq (1 + \mathfrak{m}^p) \subseteq 1 + \mathfrak{m}^2$. After choosing a uniformizing parameter π of $\mathcal{O}$, one gets in the usual way an isomorphism of groups

$$\phi : (1 + \mathfrak{m})/(1 + \mathfrak{m}^2) \to Lw^+, \quad 1 + x\pi \mapsto x \pmod{\mathfrak{m}}.$$

Hence $(1 + \mathfrak{m})/(1 + \mathfrak{m})^p$ is infinite, because it has as its homomorphic image the infinite group $(1 + \mathfrak{m})/(1 + \mathfrak{m}^2) \cong Lw^+$. Next, recall that $(1 + \mathfrak{m})/\Delta_1$ is a finite group. Therefore $\phi(1 + \mathfrak{m})/\phi(\Delta_1) = Lw^+/\phi(\Delta_1)$ is finite too. Hence there exist (infinitely many) elements $t := 1 + a \in \Delta_1$ with $a \in \pi\mathcal{O}^\times$. For any such $t \in \Delta_1$, we have $t = \theta^p$ for some $\theta \in \Lambda$; hence we have, as above, $L_t = L[\theta]$. Setting $\theta := 1 + b$, we have $1 + a = (1 + b)^p$. Equivalently,

$$a = \sum_{i=1}^{p-1} \binom{p}{i} b^i + b^p = pb\epsilon + b^p$$

for some w-unit $\epsilon \in \Lambda$. Since π divides p in $\mathcal{O}$, one has $w(p\,b\,\epsilon) > w(\pi)$, and therefore $w(\pi) = w(a) = w(b^p) = p \cdot w(b)$ in $w\Lambda$. Since $wL = \mathbb{Z}\,w(\pi)$, it follows that $w(u) \subseteq p \cdot wL_t$, as claimed. □

F. Inertial cohomology

In this subsection, we recall a well-known result concerning the cohomology of the maximal inert extension of a Henselian field (which goes back to Witt). The situation is as follows. Let L be a Henselian field with respect to a valuation w, let $L_1|L$ be a finite unramified Galois extension, and let $G := \mathrm{Gal}(L_1|L)$ be the Galois group of $L_1|L$. Let $\mathcal{O}_L \subset \mathcal{O}_{L_1}$ and $\mathfrak{m}_L \subset \mathfrak{m}_{L_1}$ be the corresponding valuation rings and valuation ideals, respectively. As remarked in [Pop88, Lemma 2.2], the group of principal units $1 + \mathfrak{m}_{L_1}$ is G-cohomologically trivial, and there exists an exact sequence of cohomology groups

$$0 \to \mathrm{H}^2(G, L_1w^\times) \to \mathrm{H}^2(G, L_1^\times) \to \mathrm{H}^1(G, (\mathbb{Q} \otimes wL)/wL) \to 0,$$

so that we have an exact sequence of the form

$$0 \to \mathrm{Br}(L_1w|Lw) \to \mathrm{Br}(L_1|L) \to \mathrm{Hom}(G, (\mathbb{Q} \otimes wL)/wL) \to 0. \qquad (\dagger)$$

We also remark that if $M|L$ is some algebraic extension, linearly disjoint from L_1, say, and $M_1 = ML_1$ is the compositum (in some fixed algebraic closure), then the above exact sequence

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press

gives rise to a commutative diagram of the form

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Br}(L_1w|Lw) & \longrightarrow & \mathrm{Br}(L_1|L) & \longrightarrow & \mathrm{Hom}(G, (\mathbb{Q}\otimes wL)/wL) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \\ 0 & \longrightarrow & \mathrm{Br}(M_1w|Mw) & \longrightarrow & \mathrm{Br}(M_1|M) & \longrightarrow & \mathrm{Hom}(G, (\mathbb{Q}\otimes wM)/wM) & \longrightarrow & 0 \end{array}$$

where the left two vertical maps are the canonical restriction maps and the rightmost one is induced by the canonical embedding $wL \hookrightarrow wM$. We will use these observations to prove the following result.

LEMMA 5. *Let L be Henselian with respect to a* rank-one *valuation w and satisfy the conditions that* $\mathrm{char}(L)=0$, $\mu_p \subset L$ *and* $\mathrm{char}(Lw)=p>0$. *Let $L_1|L$ be a p-cyclic unramified sub-extension of $L'|L$, so that $G\cong\mathbb{Z}/p$, and let $\Lambda|L$ be a sub-extension of $L'|L$ such that $L'|\Lambda$ is finite and $\Lambda|L$ and $L_1|L$ are linearly disjoint. Suppose that the restriction map*

$$\mathrm{res}:\mathrm{Br}(L_1|L)\to\mathrm{Br}(\Lambda_1|\Lambda)\subseteq\mathrm{Br}(\Lambda)$$

is non-trivial. Then $wL\approx\mathbb{Z}$ and $Lw|\mathbb{F}_p$ is a finite extension, i.e. L is a discrete-valued field with finite residue field of characteristic p.

Proof. By way of contradiction, suppose that the conclusion of the lemma does not hold.

Since $G=\mathrm{Gal}(L_1|L)$ has order p, it follows that $L_1=L[\sqrt[p]{a}\,]$ for some $a\in L$, and that $\mathrm{Br}(L_1|L)$ consists of cyclic algebras of index p of the form $A_L(a,u)$ with $u\in L^\times$. In particular, $\mathrm{Br}(L_1|L)$ is a torsion group of exponent p. Further, since $L_1w|Lw$ is also cyclic of degree p, it follows that $\mathrm{Br}(L_1w|Lw)$ is generated by cyclic algebras of index p and, moreover, every such algebra from $\mathrm{Br}(L_1w|Lw)$ is also split by some purely inseparable extension of degree p of Lw. Therefore, the restriction map $\mathrm{Br}(L_1w|Lw)\xrightarrow{\mathrm{res}}\mathrm{Br}(Lw^{1/p})$ is trivial. On the other hand, by Lemma 4(1), we have $Lw^{1/p}\subseteq\Lambda w$. Hence the restriction map

$$\mathrm{Br}(L_1w|Lw)\xrightarrow{\mathrm{res}}\mathrm{Br}(\Lambda_1w|\Lambda w)\subseteq\mathrm{Br}(\Lambda w) \qquad (*)$$

is trivial. Therefore, if $A_L(a,u)\in\mathrm{Br}(L_1|L)$ has non-trivial image in $\mathrm{Br}(\Lambda_1|\Lambda)$, then by the exact sequence (†) and the above diagram applied with $M:=\Lambda$, we get that $A_L(a,u)$ does not lie in the image of $\mathrm{Br}(L_1w|Lw)$ in $\mathrm{Br}(L_1|L)$. Equivalently, $A_L(a,u)$ is ramified, i.e. $w(u)$ is non-trivial in wL/p. Since we have assumed that the conclusion of Lemma 5 does not hold, by Lemma 4(2) there exists $L_t:=L[\sqrt[p]{t}\,]\subseteq\Lambda$ with $t\in L^\times$ such that $w(u)\in p\cdot wL_t$. But then, by the fundamental (in)equality, we have

$$p=[L_t:L]\geqslant[L_tw:Lw]\cdot(wL_t:wL)\geqslant[L_tw:Lw]\cdot p\geqslant p.$$

Therefore, the above inequalities are actually equalities, and $[L_tw:Lw]=1$, i.e. $L_tw=Lw$. Also, $L_{t,1}w=L_1w$, where $L_{t,1}:=L_tL_1$ is the compositum of L_t and L_1 inside Λ_1.

Hence, from the above commutative diagram applied to $M:=L_t$, it follows that the image $A_{L_t}(a,u)$ of $A_L(a,u)$ in $\mathrm{Br}(L_{t,1}|L_t)$ actually lies in $\mathrm{Br}(L_{t,1}w|L_tw)=\mathrm{Br}(L_1w|Lw)$. But then the image of $A_{L_t}(a,u)$ in $\mathrm{Br}(\Lambda_1|\Lambda)$ actually lies in the image of $\mathrm{Br}(L_{t,1}w|L_tw)=\mathrm{Br}(L_1w|Lw)$ in $\mathrm{Br}(\Lambda_1w|\Lambda w)$. On the other hand, the image of $\mathrm{Br}(L_1w|Lw)$ in $\mathrm{Br}(\Lambda_1w|\Lambda w)$ is trivial by the discussion around ($*$) above. Therefore $A_\Lambda(a,u)$ is trivial in $\mathrm{Br}(\Lambda_1|\Lambda)$, which is a contradiction. □

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press

G. $\mathrm{Gal}(k_1'|k_1)$ and $\mathrm{Br}(k_1)$

Let $k|\mathbb{Q}_p$ be a finite extension with $\mu_p \subset k$. Let $k_1|k$ be an arbitrary (not necessarily Galois and not necessarily finite) algebraic extension and let $[k_1 : k]$ denote its degree (as a supernatural number). As usual, let $k_1'|k_1$ be a maximal $\mathbb{Z}/p$ elementary extension of k_1 and $\mathrm{Gal}(k_1'|k_1) := \mathrm{Gal}(k_1'|k_1)$ its Galois group.

Lemma 6. *In the above context, the following hold.*

(1) *The restriction map* ${}_p\mathrm{Br}(k) \to \mathrm{Br}(k_1)$ *is injective if and only if* $[k_1 : k]$ *is not divisible by* p.

(2) *Suppose that* $(p, [k_1 : k]) = 1$. *Then* $\mathrm{Gal}(k_1'|k_1) \cong (\mathbb{Z}/p)^{e_{k_1}+2}$, *where* $e_{k_1} := [k_1 : \mathbb{Q}_p]$.

Proof. (1) After identifying $\mathrm{Br}(k)$ with $\mathbb{Q}/\mathbb{Z}$ via the invariant $\mathrm{inv}_k : \mathrm{Br}(k) \to \mathbb{Q}/\mathbb{Z}$, the restriction $\mathrm{Br}(k) \to \mathrm{Br}(k_1)$ becomes multiplication by $[k_1 : k]$. Hence ${}_p\mathrm{Br}(k) \to \mathrm{Br}(k_1)$ is injective if and only if $[k_1 : k]$ is not divisible by p.

(2) If $k_1|k$ is finite, then the assertion follows from local class field theory. Furthermore, the canonical projection $\mathrm{Gal}(k_1'|k_1) \to \mathrm{Gal}(k'|k)$ is surjective, as $[k_1 : k]$ is prime to p. Finally, by taking limits over all the finite sub-extensions $k_i|k$ of $k_1|k$, the assertion follows. □

H. p-adic valuations and formally p-adic fields

We recall a few basic facts about p-adic valuations and (formally) p-adically closed fields; see [AK66, PR85] for more details.

(1) A valuation v of a field k is called (formally) *p-adic* if the residue field kv is a finite field $\mathbb{F}_q$ with $q = p^{f_v}$ and the value group vk has a minimal positive element 1_v such that $v(p) = e_v \cdot 1_v$ for some natural number $e_v > 0$. The number $d_v := e_v f_v$ is called the *p-adic rank* (or degree) of the p-adic valuation v. Note that a field k carrying a p-adic valuation v must necessarily have $\mathrm{char}(k) = 0$, as $v(p) \neq \infty$, and $\mathrm{char}(kv) = p$.

(2) Let v be a p-adic valuation of k with valuation ring $\mathcal{O}_v$. Then $\mathcal{O}_1 := \mathcal{O}[1/p]$ is the valuation ring of the unique maximal proper coarsening v_1 of v, which is called the *canonical coarsening* of v. Note that upon setting $k^0 := kv_1$ and $v_0 = v/v_1$, the corresponding valuation on k^0, we have that v_0 is a p-adic valuation of k^0 with $e_{v_0} = e_v$ and $f_{v_0} = f_v$; hence $d_{v_0} = d_v$ and, moreover, v_0 is a discrete valuation of k^0. In particular, the following properties hold.

(a) v has rank one if and only if v_1 is the trivial valuation, and this is true if and only if $v = v_0$.

(b) Giving a p-adic valuation v of a field k of p-adic rank $d_v = e_v f_v$ is equivalent to giving a place $\mathfrak{p}$ of k with values in a finite extension l of $\mathbb{Q}_p$ such that the residue field $k\mathfrak{p}$ of $\mathfrak{p}$ is dense in l and $l|\mathbb{Q}_p$ has ramification index e_v and residual degree f_v.

(c) If $v_i < v$ is a strict coarsening of v, then $v_i \leqslant v_1$ and the quotient valuation v/v_i on the residue field kv_i is a p-adic valuation with $e_{v/v_i} = e_v$, $f_{v/v_i} = f_v$ and thus $d_{v/v_i} = d_v$. (Actually, $(kv_i)(v_i/v_1) \cong kv_1$ and $(kv_i)(v_i/v) \cong kv$ canonically.)

(3) Let v be a p-adic valuation of k and $l|k$ a finite field extension, and denote by $w|v$ the prolongations of v to l. Then all the w are p-adic valuations. Moreover, the *fundamental equality* holds: $[l : k] = \sum_{w|v} e(w|v) f(w|v)$, where $e(w|v)$ and $f(w|v)$ are, respectively, the ramification index and the residual degree of $w|v$. Further, if w_1 is the canonical coarsening of w and $w_0 = w/w_1$ is the canonical quotient on the residue field lw_1, then by general decomposition theory of valuations one has $e(w|v) = e(w_1|v_1)e(w_0|v_0)$ and $f(w|v) = f(w_0|v_0)$; moreover, $e_w = e_v\, e(w_0|v_0)$ and $f_w = f_v\, f(w|v)$, thus $d_w = d_v e(w_0|v_0) f(w|v)$.

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press

(4) A field k is called (formally) *p-adically closed* if k carries a p-adic valuation v such that for every finite extension $l|k$ one has that if v has a prolongation w to l with $d_w = d_v$, then $l = k$. There is a characterization of the p-adically closed fields as follows. For a field k endowed with a p-adic valuation v and canonical coarsening v_1, the following are equivalent:

(i) k is p-adically closed with respect to v;

(ii) v is Henselian and $v_1 k$ is divisible (possibly trivial);

(iii) v_1 is Henselian and $v_1 k$ is divisible (possibly trivial), and the residue field $k^0 := kv_1$ is relatively algebraically closed in its completion $\widehat{k^0}$ (which is itself a finite extension of $\mathbb{Q}_p$).

We also note that if k is p-adically closed with respect to some p-adic valuation v, then the valuation ring of v is completely determined by k. In particular, for every field k there exists at most one valuation v (up to equivalence of valuations) such that k is p-adically closed with respect to v.

(5) For every field k endowed with a p-adic valuation v, there exist p-adic closures $\tilde{k}$ and $\tilde{v}$ such that $d_{\tilde{v}} = d_v$. Moreover, the space of the isomorphy classes of p-adic closures of k and v has a concrete description as follows. Let v_1 be the canonical coarsening of v and $\widehat{k^0}|\mathbb{Q}_p$ the completion of the residue field of $k^0 = kv_1$. Then there exists a canonical exact sequence of the form $1 \to I_{v_1} \longrightarrow D_v \xrightarrow{\text{pr}} G_{\widehat{k^0}} \to 1$, and the space of isomorphy classes of p-adic closures of k and v is in bijection with the space of sections of pr and thus with $\mathrm{H}^1_{\text{cont}}(G_{\widehat{k^0}}, I_{v_1})$.

(6) If L is p-adically closed with respect to the p-adic valuation w and $l \subseteq L$ is a subfield which is relatively closed in L, then l is p-adically closed with respect to $v := w|_l$ and v and w have equal p-adic ranks; also, L and l are elementarily equivalent. Therefore, the elementary equivalence class of a p-adically closed field k is determined by both the *absolute subfield* $k^{\text{abs}} := k \cap \overline{\mathbb{Q}}$ of k and the completion $\widehat{k^0} = \widehat{k^{\text{abs}}}$. Note that the p-adic valuation of k^{abs} is discrete and that k^{abs} is actually the relative algebraic closure of $\mathbb{Q}$ in $k^0 := kv_1$. Further, $\overline{L} = L\overline{l} = L\overline{\mathbb{Q}}$. Therefore, if $L|l$ is an extension of p-adically closed fields of the same rank, then the canonical projection $G_L \to G_l$ is an isomorphism.

(7) Finally, let $(L, w)|(l, v)$ be an extension of p-adically closed fields with $d_w = d_v$. Let $k|l$ be some Galois extension, and set $K := Lk$. Then, using the notation from the introduction, the following canonical projections are isomorphisms:

$$\text{pr}'_L : \text{Gal}(K'|L) \to \text{Gal}(k'|l), \quad \text{pr}''_L : \text{Gal}(K''|L) \to \text{Gal}(k''|l). \tag{$\dagger$}$$

Remark 7. Let l,v be a finite field extension of $\mathbb{Q}_p$, and let $L = \kappa(Y)$ be the function field of a complete smooth curve $Y \to l$. Let $s : G_l \to G_L$ be a section of $\text{pr}_L : G_L \to G_l$, and let $\tilde{L}$ be the fixed field of $\text{im}(s)$ in $\overline{L}$. Then $\overline{L} = \tilde{L}\overline{l} = \tilde{L}l\overline{\mathbb{Q}} = \tilde{L}\overline{\mathbb{Q}}$, and $G_{\tilde{L}} \to G_l \to G_{l^{\text{abs}}}$ are all isomorphisms. Hence $\tilde{L}$ is p-adically closed by [Pop88, assertion E.11] and elementarily equivalent to l^{abs}, and hence to l, by paragraph (6) above; moreover, if $\tilde{w}$ is the valuation of $\tilde{L}$, then $d_{\tilde{w}} = d_v$ and $v = \tilde{w}|_l$. Thus $w := \tilde{w}|_L$ is a p-adic valuation of L with $d_w = d_v$ and $w|_l = v$. Hence, by statement (2)(b) above, the canonical coarsening w_1 of w defines an l-rational place of $L|l$, and thus an l-rational point $y \in Y(l)$, such that $\text{im}(s)$ is contained in a decomposition group D_y above y. Therefore, recalling that distinct decomposition groups above l-places of $L|l$ have trivial intersection (by a theorem of F. K. Schmidt), it follows that y and D_y are uniquely determined by $\text{im}(s)$. This proves the *birational p-adic section conjecture* for $Y \to l$; see [Koe05] for more details.

I. A local–global principle for the Brauer group

Here we recall the following result, which was proved in [Pop88, Theorem 4.5] and uses in an essential way the results of Tate [Tat59], Roquette [Roq66] and Lichtenbaum [Lic69].

Fact. *Let k be a p-adically closed field, and let $M|k$ be a field extension of transcendence degree* $\mathrm{tr.deg}(M|k) \leqslant 1$. *Further, let $w|v$ denote the prolongations of the p-adic valuation v of k to M, and for each w let M_w^{h} be a Henselization of M with respect to w. Then the following canonical exact sequence of Brauer groups is exact:*

$$0 \to \mathrm{Br}(M) \to \prod_{w|v} \mathrm{Br}(M_w^{\mathrm{h}}).$$

We will use a special form of the above fact which reads as follows. Let w be a prolongation of v to M and let $\mathcal{O}_w$ and $\mathfrak{m}_w$ be its valuation ring and valuation ideal, respectively. Further, let $\mathcal{O}_{w_1} := \mathcal{O}_w[1/p]$ be the coarsening of $\mathcal{O}_w$ obtained by inverting the prime number p, and denote by w_1 the corresponding coarsening of w. Then w_1 is a prolongation to M of the canonical coarsening v_1 of v. Setting $M_0 := Mw_1$ and $w_0 := w/w_1$, it follows from general valuation theory that $M_0|k_0$ is a field extension with $\mathrm{tr.deg}(M_0|k_0) \leqslant 1$ and that w_0 is a prolongation of v_0 to M_0. For every prolongation $w|v$, the following are equivalent:

(i) w_0 is a rank one valuation;

(ii) the minimal prime ideal of $\mathcal{O}_w$ which contains the rational prime number p is the valuation ideal $\mathfrak{m}_w$.

In particular, for every prolongation $w|v$ of v to M there exists a unique coarsening $\tilde{w}$ such that $\tilde{w}$ is a prolongation of v to M and $\tilde{w}$ satisfies the equivalent conditions (i) and (ii) above. Indeed, for any given $w|v$, let $\tilde{\mathfrak{m}}$ be the minimal prime ideal of $\mathcal{O}_w$ which contains the prime number p. Then, by general valuation theory, the localization $\tilde{\mathcal{O}} := (\mathcal{O}_w)_{\tilde{\mathfrak{m}}}$ is a valuation ring with valuation ideal $\tilde{\mathfrak{m}}$, and its valuation $\tilde{w}$ is the unique coarsening of w satisfying the equivalent conditions (i) and (ii) above.

Fact 8. *Let k be a p-adically closed field, and let $M|k$ be a field extension of transcendence degree* $\mathrm{tr.deg}(M|k) \leqslant 1$. *Let $\mathcal{W}$ be the set of all the prolongations $w|v$ of v to M that satisfy the equivalent conditions (i) and (ii) above. Then the following canonical exact sequence of Brauer groups is exact:*

$$0 \to \mathrm{Br}(M) \to \prod_{w \in \mathcal{W}} \mathrm{Br}(M_w^{\mathrm{h}}).$$

Proof. For a non-trivial division algebra A over M, let $w|v$ be a prolongation such that, writing M_w^{h} for the Henselization of M with respect to w, one has $A_{M_w^{\mathrm{h}}} \neq 0$ in $\mathrm{Br}(M_w^{\mathrm{h}})$. Now let $\tilde{w}$ be the unique coarsening of w such that $\tilde{w} \in \mathcal{W}$. Then, since $\tilde{w}$ is a coarsening of w, it follows that M_w^{h} contains a Henselization $M_{\tilde{w}}^{\mathrm{h}}$ of M with respect to $\tilde{w}$. On the other hand, since $M_{\tilde{w}}^{\mathrm{h}} \subseteq M_w^{\mathrm{h}}$ and $A_{M_w^{\mathrm{h}}} \neq 0$ in $\mathrm{Br}(M_w^{\mathrm{h}})$, we have that $A_{M_{\tilde{w}}^{\mathrm{h}}} \neq 0$ in $\mathrm{Br}(M_{\tilde{w}}^{\mathrm{h}})$. □

3. Proof of Theorem B

To prove assertion (1), let $\tilde{K}, \tilde{w}$ be a p-adic closure of K, w, and let $\tilde{k}, \tilde{v}$ be the relative algebraic closure of k in $\tilde{K}$ endowed with the restriction of $\tilde{w}$ to $\tilde{k}$. Then $d_{\tilde{v}} = d_{\tilde{w}} = d_w$. Since $d_v = d_w$ by hypothesis, we get $d_{\tilde{v}} = d_v$ and hence $\tilde{k} = k$. We conclude by applying relation (†) from § 2-H., paragraph (7), with $l := k$ and $L := \tilde{K}$, and taking into account the fact that the isomorphism $\mathrm{Gal}(\tilde{K}''|\tilde{K}) \to \mathrm{Gal}(k''|k)$ factors through $\mathrm{Gal}(K''|K) \to \mathrm{Gal}(k''|k)$ and thus gives rise to a liftable section of $\mathrm{Gal}(K'|K) \to \mathrm{Gal}(k'|k)$.

To prove assertion (2), let $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ be a liftable section and let $M \subset K'$ be the fixed field of $\mathrm{im}(s')$. Consider $a, b \in k$ such that $k_1 := k[\sqrt[p]{a}]$ is the unique unramified extension of degree p of k and the p-cyclic algebra $A_k(a, b)$ is non-trivial in $\mathrm{Br}(k)$ or, equivalently, $\chi_a \cup \chi_b \neq 0$ in $\mathrm{H}^2(G_k, \mathbb{Z}/p)$. Then, by Lemma 2, $A_M(a, b)$ is non-trivial in $\mathrm{Br}(M)$. Hence, from Fact 8, it follows that there exists some prolongation $w \in \mathcal{W}$ of v to M such that, writing $\Lambda := M^{\mathrm{h}}_w$ for the Henselization of M with respect to w, one has $A_\Lambda(a, b) \neq 0$ in $\mathrm{Br}(\Lambda)$. With an abuse of notation, we will write w for the Henselian prolongation of w to Λ and so on.

For w as above, let $L := K^{\mathrm{h}}_w \subseteq \Lambda$ denote the (unique) Henselization of K with respect to (the restriction of) w which is contained in Λ. Then the compositum $LM \subseteq \Lambda$ is Henselian with respect to w, hence we must have $LM = \Lambda$. Note that $L' = K'L$ by Lemma 3(3), and $K'|M$ is finite because $\mathrm{im}(s')$ is finite and $M = (K')^{\mathrm{im}(s')}$. We conclude that $L' = LK'$ is finite over $\Lambda = LM$; also, $A_\Lambda(a, b) \neq 0$ in $\mathrm{Br}(\Lambda)$ implies $A_L(a, b) \neq 0$ in $\mathrm{Br}(L)$, as $L \subset \Lambda$.

Lemma 9. *The valuation w is a p-adic valuation of L.*

Proof. As in the discussion above, let w_1 and v_1 be, respectively, the canonical coarsenings of w and v, i.e. the valuations with valuation rings $\mathcal{O}_w[1/p]$ and $\mathcal{O}_v[1/p]$, respectively. We denote the corresponding residue fields by $k_0 := kv_1$, $L_0 := Lw_1$ and $\Lambda_0 := \Lambda w_1$; recall also that $v_0 := v/v_1$ on k_0 and $w_0 := w/w_1$ on L_0 and Λ_0 are rank-one valuations (since $w \in \mathcal{W}$). Note that the following hold.

(a) w_1 prolongs v_1 to L and Λ, and w_0 prolongs v_0 to L_0 and Λ_0, as w prolongs v to L.

(b) w_1 and v_1, as well as w_0 and v_0, are Henselian because w and v are.

(c) $L'w_1|Lw_1$ is the maximal $\mathbb{Z}/p$ elementary abelian extension of $L_0 = Lw_1$ by Lemma 3(2), hence $L'w_1$ equals the maximal $\mathbb{Z}/p$ elementary abelian extension $L'w_1 = L'_0$ of L_0.

(d) Further, since $L'|\Lambda$ is finite by the discussion above, it follows that $L'w_1|\Lambda w_1$ is finite by the fundamental inequality. Since $L'w_1 = L'_0$ and $\Lambda w_1 = \Lambda_0$, we get that $L'_0|\Lambda_0$ is finite.

Recall the v-unramified extension $k_1 := k[\sqrt[p]{a}]$ with $\mathrm{Gal}(k_1|k) =: G$ defined above. We set $\Lambda_1 := \Lambda k_1$ and remark that $\Lambda_1|\Lambda$ is a w-unramified cyclic extension with Galois group canonically isomorphic to G. Moreover, since $k_1|k$ is v-unramified, $k_1|k$ is also v_1-unramified, as v_1 is a coarsening of v. Correspondingly, $L_1|L$ is w_1-unramified. Let $k_{01} := k_1 v_1$ and $\Lambda_{01} := \Lambda_1 w_1$ be the corresponding residue fields. Observe that $k_{01}|k_0$ is a v_0-unramified cyclic extension with Galois group canonically isomorphic to G; correspondingly, $\Lambda_{01}|\Lambda_0$ is a w_0-unramified cyclic extension with Galois group canonically isomorphic to G.

We next consider the resulting commutative diagram, shown below, of Brauer/cohomology groups deduced from the extension of valued fields $(\Lambda, w_1)|(k, v_1)$ and the corresponding residue fields, as discussed in §§ 1 and 2-F.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Br}(k_{01}|k_0) & \longrightarrow & \mathrm{Br}(k_1|k) & \longrightarrow & \mathrm{Hom}(G, (\mathbb{Q} \otimes v_1 k)/v_1 k) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \\
0 & \longrightarrow & \mathrm{Br}(\Lambda_{01}|\Lambda_0) & \longrightarrow & \mathrm{Br}(\Lambda_1|\Lambda) & \longrightarrow & \mathrm{Hom}(G, (\mathbb{Q} \otimes w_1 \Lambda)/w_1 \Lambda) & \longrightarrow & 0
\end{array}$$

We recall that $v_1 k$ is divisible, hence $\mathbb{Q} \otimes v_1 k = v_1 k$ and therefore $(\mathbb{Q} \otimes v_1 k)/v_1 k = (0)$. Thus we deduce that $\mathrm{Br}(k_{01}|k_0) \to \mathrm{Br}(\Lambda_{01}|\Lambda_0) \subseteq \mathrm{Br}(\Lambda_0)$ is non-trivial.

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press

Now let us set $L_1 := Lk_1$ and write $L_{01} := L_1 w_1$. Then, reasoning as above, we get that $L_1|L$ is w-unramified and hence w_1-unramified. Furthermore, $L_{01}|L_0$ is a w_0-unramified extension with Galois group canonically isomorphic to G, and it is obvious that $\mathrm{Br}(k_{01}|k_0) \to \mathrm{Br}(\Lambda_0)$ factors through $\mathrm{Br}(L_{01}|L_0)$. Therefore $\mathrm{Br}(L_{01}|L_0) \to \mathrm{Br}(\Lambda_0)$ is non-trivial.

By Lemma 5 applied to L_0 endowed with the Henselian rank-one valuation w_0, the w_0-unramified extension $L_{01}|L_0$ and the extension $\Lambda_0|L_0$ such that $L'_0|\Lambda_0$ is finite, we get that w_0 is discrete and has finite residue field (of characteristic p, as w_0 prolongs v_0). Equivalently, w is a (Henselian) p-adic valuation of L, as claimed. □

Lemma 10. *The p-adic valuation w from Lemma 9 has p-adic rank equal to the p-adic rank of v and satisfies* $\mathrm{im}(s') \subseteq Z_w$.

Proof. The proof is a refinement of the arguments in the proof of the previous lemma. As remarked there, the canonical restriction map

$$\mathrm{res} : \mathrm{Br}(k_{01}|k_0) \to \mathrm{Br}(L_{01}|L_0) \to \mathrm{Br}(\Lambda_0)$$

is non-trivial. Since completion does not change the inertial cohomology, without loss of generality we can replace $k_0 \subseteq L_0 \subseteq \Lambda_0$ by the corresponding sequence of completions $\hat{k}_0 \subseteq \hat{L}_0 \subseteq \hat{\Lambda}_0$, all of which are finite extensions of $\mathbb{Q}_p$, and thus deduce that

$$\mathrm{res} : \mathrm{Br}(\hat{k}_{01}|\hat{k}_0) \to \mathrm{Br}(\hat{L}_{01}|\hat{L}_0) \to \mathrm{Br}(\hat{\Lambda}_0)$$

is non-trivial. But then, from Lemma 6, it follows that $[\hat{\Lambda}_0 : \hat{k}_0]$ is prime to p and therefore $[\Lambda_0 : k_0] = [\hat{\Lambda}_0 : \hat{k}_0]$ is prime to p. Hence, from $[\Lambda_0 : k_0] = [\Lambda_0 : L_0] \cdot [L_0 : k_0]$ it follows that both $[L_0 : k_0]$ and $[\Lambda_0 : L_0]$ are prime to p. On the other hand, $\Lambda_0|L_0$ is a sub-extension of the $\mathbb{Z}/p$ elementary abelian extension $L'_0|L_0$. Thus, finally, $\Lambda_0 = L_0$.

Now recall that $M = (K')^{\mathrm{im}(s')}$ is the fixed field of $\mathrm{im}(s') = s'(\mathrm{Gal}(k'|k))$ in K'; furthermore, $L' = LK'$ and $\Lambda = ML$ inside L', by the discussion at the beginning of the proof. From this we deduce the following sequence of inequalities:

$$[k' : k] = |\mathrm{Gal}(k'|k)| = [K' : M] \geqslant [LK' : LM] = [L' : \Lambda]. \qquad (*)$$

Moreover, because k is p-adically closed, and hence $\mathrm{pr}_k : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(k'_0|k_0)$ is an isomorphism, one has $[k' : k] = [k'_0 : k_0]$, and by the fundamental inequality we have $[L' : \Lambda] \geqslant [L'w_1 : \Lambda w_1]$. On the other hand, we have $L'w_1 = L'_0$ and $\Lambda w_1 := \Lambda_0$, and $\Lambda_0 = L_0$ by the remarks above. Thus the above sequences of inequalities can be extended as follows:

$$[k'_0 : k_0] = [k' : k] = [K' : M] \geqslant [LK' : LM] = [L' : \Lambda] \geqslant [L'w_1 : \Lambda w_1] = [L'_0 : L_0]. \qquad (**)$$

Next, observe that by Lemma 6(2) we have $[k'_0 : k_0] = p^{e_{k_0}}$, where $e_{k_0} := [\hat{k}_0 : \mathbb{Q}_p]$, and $[L'_0 : L_0] = p^{e_{L_0}}$, with $e_{L_0} := [\hat{L}_0 : \mathbb{Q}_p]$. Hence the inequality $(**)$ above implies $e_{k_0} \geqslant e_{L_0}$. On the other hand, $k_0 \subseteq L_0$ implies $e_{k_0} \leqslant e_{L_0}$. Hence $e_{k_0} = e_{L_0}$ and $\hat{k}_0 = \hat{L}_0$. Equivalently, w is a p-adic valuation having p-adic rank equal to

$$d_w = [\hat{L}_0 : \mathbb{Q}_p] = [\hat{k}_0 : \mathbb{Q}_p] = d_v$$

and hence equal to the p-adic rank of v. Moreover, because of this, all the inequalities in the formulas $(*)$ and $(**)$ above are actually equalities. Therefore $[K' : M] = [LK' : LM]$, and the restriction map $\mathrm{Gal}(L'|L) = \mathrm{Gal}(L'|L) \to Z_w \subset \mathrm{Gal}(K'|K)$, which maps $\mathrm{Gal}(L'|L)$ isomorphically onto Z_w by the fact that $L' = K'L$, defines an isomorphism

$$\mathrm{Gal}(L'|\Lambda) \to \mathrm{Gal}(K'|M) = s'(\mathrm{Gal}(k'|k)).$$

Equivalently, $\mathrm{im}(s') \subseteq Z_w$, as claimed. □

Coming back to the proof of Theorem B, we have the following. Let $M \subseteq K'$ be the fixed field of $\mathrm{im}(s')$ in K'; then there exists a p-adic valuation w of M such that w prolongs v to M and has p-adic rank d_w equal to the p-adic rank d_v of v; moreover, $\mathrm{im}(s')$ is contained in the decomposition group Z_w of w in $\mathrm{Gal}(K'|K)$.

Remark 11. The precise structure of Z_w can be deduced as follows. First, let w_1 be the canonical coarsening of w and let T_{w_1} and Z_{w_1} with $T_{w_1} \subset Z_{w_1}$ be, respectively, the inertia and decomposition groups above w_1 in $\mathrm{Gal}(K'|K)$. Then $Z_w = Z_{w_1}$, and $\mathrm{pr}'_K : \mathrm{Gal}(K'|K) \to \mathrm{Gal}(k'|k)$ gives rise to an exact sequence

$$1 \to T_{w_1} \to Z_{w_1} \xrightarrow{\mathrm{pr}'_K} \mathrm{Gal}(k'|k) \to 1$$

such that $s'(\mathrm{Gal}(k'|k)) \subseteq Z_{w_1} = Z_w$ is a complement of T_{w_1}. If T_{w_1} is non-trivial, then $T_{w_1} \cong \mu_p$ as a $\mathrm{Gal}(k'|k)$-module, and thus $T_{w_1} \cong \mathbb{Z}/p$ non-canonically as a $\mathrm{Gal}(k'|k)$-module.

Lemma 12. *The p-adic valuation w from Lemma 10, which satisfies $\mathrm{im}(s') \subseteq Z_w$, is unique.*

Proof. Consider p-adic valuations w^1 and w^2 such that $\mathrm{im}(s') \subset Z_{w^i}$ for $i = 1, 2$. We claim that $w^1 = w^2$. Indeed, let w be the maximal common coarsening of w^1 and w^2. By way of contradiction, suppose that $w < w^1, w^2$. Then the valuations w^1/w and w^2/w are independent p-adic valuations on Kw, both of which prolong the p-adic valuation of the p-adically closed field kw. Further, from Lemma 3(2), it follows that $K'w$ is the maximal $\mathbb{Z}/p$ elementary abelian extension of Kw; moreover, since $\mathrm{im}(s') \subset Z_{w^i}$ for $i = 1, 2$, general decomposition theory for valuations gives that $s'_w(\mathrm{Gal}(k'|k)) \subset Z_{w^i/w}$ for $i = 1, 2$. On the other hand, by the construction of w, we have that w^1/w and w^2/w are independent valuations of Kw. However, since w^1/w and w^2/w are independent, it follows from Lemma 3(2) that $Z_{w^1/w} \cap Z_{w^2/w}$ is trivial. This is a contradiction, because $\mathrm{im}(s'_w) \subset Z_{w^i/w}$ for $i = 1, 2$. □

The proof of Theorem B is thus complete.

4. Proof of Theorem A

The following stronger assertion holds (from which Theorem A follows immediately).

Theorem 13. *Let $k|\mathbb{Q}_p$ be a finite extension containing the pth roots of unity, and let $k_0 \subseteq k$ be a subfield which is relatively algebraically closed in k. Let X_0 be a complete smooth curve over k_0, and let $K_0 = k_0(X)$ be the function field of X_0.*

1. *Every k-rational point $x \in X_0$ gives rise to a bouquet of conjugacy classes of liftable sections $s'_x : \overline{G}'_{k_0} \to \overline{G}'_{K_0}$ above x.*
2. *Let $s' : \overline{G}'_{k_0} \to \overline{G}'_{K_0}$ be a liftable section. Then there exists a unique k-rational point $x \in X_0$ such that s' equals one of the sections s'_x mentioned above.*

Proof. (1) Let v be the valuation of k. Notice that, by § 2-H.(b), there exists a bijection from the p-adic valuations w of $\kappa(X_0)$ with $d_w = d_v$ to the k-rational points x of X_0 which sends each w to the center x of the canonical coarsening w_1 on $X = X_0 \times_{k_0} k$. We conclude by applying Theorem B(1).

(2) Since $k_0 \subseteq k$ is relatively algebraically closed, k_0 is p-adically closed. Let v be the valuation of k and of all subfields of k. Since k_0 is p-adically closed, we can apply Theorem B and get that for every section $s' : \overline{G}'_{k_0} \to \overline{G}'_{K_0}$, there exists a unique p-adic valuation w of K_0 which prolongs v

to K_0 and has p-adic rank equal to the p-adic rank of v, such that s' is a section above w. Let w_1 be the canonical coarsening of v. Then we have the following two cases.

Case 1. The valuation w_1 is trivial.

Then w is a discrete valuation of K that prolongs v to K and has the same residue field and same value group as v. Equivalently, the completions $\hat{k}_0$ and $\hat{K}_0$ are equal, and hence equal to k. Therefore w is uniquely determined by the embedding $\imath_w : (K_0, w) \hookrightarrow (k, v)$. In geometric terms, $\imath_w$ defines a k-rational point x of X_0 and so on.

Case 2. The valuation w_1 is not trivial.

In this case w_1 is a k_0-rational place of K_0, hence it defines a k_0-rational point x_0 of X_0, and hence a k-rational point x of X_0, and so forth. □

5. Proof of Theorem B^0

First, the proof of assertion (1) is identical to the proof of Theorem B(1), so we omit it. As for assertion (2), let $s'_L : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ be a liftable section of the canonical projection $\mathrm{pr}'_L : \mathrm{Gal}(K'|L) \to \mathrm{Gal}(k'|l)$. Then the restriction of s'_L to $\mathrm{Gal}(k'|k) \subseteq \mathrm{Gal}(k'|l)$ gives rise to a liftable section $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ of $\mathrm{pr}'_K : \mathrm{Gal}(K'|K) \to \mathrm{Gal}(k'|k)$. Hence, by Theorem B, there exists a unique p-adic valuation w^1 of K which prolongs the p-adic valuation v_k of k to K and has $d_{w^1} = d_{v_k}$ and $s' = s_{w^1}$ in the usual way. Let $w = w^1|_L$ be the restriction of w^1 to L. Then w prolongs the valuation v of l to L. We claim that w^1 is the unique prolongation of w to K. Indeed, let $w^2 := w^1 \circ \sigma_0$ with $\sigma_0 \in \mathrm{Gal}(k|l)$ be a further prolongation of w to K. If $(w^i)'$ is a prolongation of w^i to K' for $i = 1, 2$ and $\sigma \in \mathrm{im}(s'_L)$ is a preimage of σ_0, then $(w^2)' := (w^1)' \circ \sigma$ is a prolongation of w^2 to K'. Therefore, if $Z_{w^1} \subset \mathrm{Gal}(K'|K)$ is the decomposition group above w^1, then $Z_{w^2} := \sigma Z_{w^1} \sigma^{-1}$ is the decomposition group above w^2. On the other hand, $\mathrm{im}(s') \subseteq Z_{w^1}$ by Theorem B (or, more precisely, by Lemma 10 in the proof of Theorem B). Since $\sigma \in \mathrm{im}(s'_L)$ and $\mathrm{Gal}(k'|k)$ is a normal subgroup of $\mathrm{Gal}(k'|l)$, we have that $\mathrm{im}(s')$ is normal in $\mathrm{im}(s'_L)$, and it follows that $\sigma(\mathrm{im}(s'))\sigma^{-1} = \mathrm{im}(s')$. Hence $\mathrm{im}(s') \subseteq Z_{w^1} \cap Z_{w^2}$. But then, by Theorem B (or, more precisely, by Lemma 12 in the proof of Theorem B), we must have $w^1 = w^2$. Equivalently, $\mathrm{im}(s'_L)$ is contained in $Z_w \subset \mathrm{Gal}(K'|L)$. So we finally conclude that $d_w = d_v$ as claimed.

6. Proof of Theorem A^0

The following stronger assertion holds (from which Theorem A^0 follows immediately).

Theorem 14. *Let $l|\mathbb{Q}_p$ be a finite extension. Let $l_0 \subset l$ be a relatively algebraically closed subfield and $k_0|l_0$ a finite Galois extension with $\mu_p \subset k_0$. Let Y_0 be a complete smooth geometrically integral curve over l_0. Let $L_0 = \kappa(Y_0)$ be the function field of Y_0, and let $K_0 = L_0 k_0$.*

(1) *Every l-rational point $y \in Y_0$ gives rise to a bouquet of conjugacy classes of liftable sections $s'_y : \mathrm{Gal}(k'_0|l_0) \to \mathrm{Gal}(K'_0|L_0)$ above y.*

(2) *Let $s' : \mathrm{Gal}(k'_0|l_0) \to \mathrm{Gal}(K'_0|L_0)$ be a liftable section. Then there exists a unique l-rational point $y \in Y_0(l)$ such that s' equals one of the sections s'_y mentioned above.*

Proof. The proof is identical to the proof of Theorem A above, the only difference being that one uses Theorem B^0 instead of Theorem B. □

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press

Acknowledgements

I would like to thank, among others, J.-L. Colliot-Thélène, D. Harbater, J. Ellenberg, M. Kim, H. Nakamura, M. Saidi, J. Stix, T. Szamuely and A. Tamagawa for stimulating discussions concerning the section conjecture.

References

AK66 J. Ax and S. Kochen, *Diophantine problems over local fields: III. Decidable fields*, Ann. of Math. (2) **83** (1966), 437–456.

Fal98 G. Faltings, *Curves and their fundamental groups (following Grothendieck, Tamagawa and Mochizuki)*, Astérisque **252** (1998), 131–150, Exposé 840.

Gro98a A. Grothendieck, *Letter to Faltings (June 1983)*, in *Geometric Galois actions 1*, London Mathematical Society Lecture Note Series, vol. 242 (Cambridge University Press, Cambridge, 1998), 5–48. See SL98 below.

Gro98b A. Grothendieck, *Esquisse d'un programme (1984)*, in *Geometric Galois actions 1*, London Mathematical Society Lecture Note Series, vol. 242 (Cambridge University Press, Cambridge, 1998), 49–58. See SL98 below.

Koe05 J. Koenigsmann, *On the 'section conjecture' in anabelian geometry*, J. Reine Angew. Math. **588** (2005), 221–235.

Lic69 S. Lichtenbaum, *Duality theorems for curves over p-adic fields*, Invent. Math. **7** (1969), 120–136.

NSW08 J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, Grundlehren der mathematischen Wissenschaften, vol. 323, second edition (Springer, Berlin, 2008).

Pop88 F. Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. Reine Angew. Math. **392** (1988), 145–175.

PR85 A. Prestel and P. Roquette, *Formally p-adic fields*, Lecture Notes in Mathematics, vol. 1050 (Springer, Berlin, 1985).

Roq66 P. Roquette, *Splitting of algebras by function fields of one variable*, Nagoya Math. J. **27** (1966), 625–642.

SL98 L. Schneps and P. Lochak (eds), *Geometric Galois actions 1*, London Mathematical Society Lecture Note Series, vol. 242 (Cambridge University Press, Cambridge, 1998).

Ser65 J.-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics, vol. 5 (Springer, Berlin, 1965).

Sza04 T. Szamuely, *Groupes de Galois de corps de type fini*, Astérisque **294** (2004), 403–431.

Tat59 J. Tate, *Cohomology of abelian varieties over p-adic fields*, Notes by Serge Lang, Princeton University (May 1959).

Florian Pop pop@math.upenn.edu
Department of Mathematics, University of Pennsylvania, 209 South 33rd Street,
Philadelphia, PA 19104, USA

https://doi.org/10.1112/S0010437X09004436 Published online by Cambridge University Press