ON THE BIRATIONAL p-ADIC SECTION CONJECTURE

FLORIAN POP

Abstract. In this manuscript we introduce/prove a very "minimalistic" form of the p-adic birational section Conjecture, which is much stronger than and implies the usual p-adic birational section Conjecture.

1. Introduction

We begin by recalling Grothendieck's Section Conjectures as evolved from Grothendieck's *Esquisse d'un Programme* [G1] and his *Letter to Faltings* [G2]: Let k be an arbitrary base field, and $X \to k$ be a geometrically integral smooth curve. Then there exists a canonical exact sequence of (étale) fundamental groups

$$(*) \qquad 1 \to \pi_1(\overline{X}) \longrightarrow \pi_1(X) \xrightarrow{pr_X} G_k \to 1\,,$$

where $G_k = \mathrm{Aut}_k\big(\overline{k}\big)$ is the absolute Galois group of k, and $\overline{X} := X \times_k \overline{k}$ is the base change of X to a fixed separable closure $\overline{k}$ of k. Let $\tilde{X} \to X$ be the universal cover of X. Note that since X is smooth, $\tilde{X}$ is an integral k-scheme, and the corresponding extension of the function fields $\kappa(\tilde{X})|\kappa(X)$ is a Galois extension with $\mathrm{Gal}\big(\kappa(\tilde{X})|\kappa(X)\big) = \pi_1(X)$. Next let $Y \to k$ be the normal completion of $X \to k$, and $\tilde{Y} \to Y$ the normalization of Y in the field extension $\kappa(\tilde{X})|\kappa(X)$. For $x \in Y$ a k-rational point, let $\tilde{x} \in \tilde{Y}$ be a point above x, and $T_x \subset Z_x$ be the inertia, respectively decomposition, groups of $\tilde{x}|x$ in $\pi_1(X) = \mathrm{Gal}\big(\kappa(\tilde{X})|\kappa(X)\big)$. Then by general decomposition theory one has the following:

- $pr_X(Z_x) = G_k$, and $T_x = Z_x \cap \pi_1(\overline{X})$.
- The canonical exact sequence $1 \to T_x \longrightarrow Z_x \xrightarrow{pr_X} G_k \to 1$ is split.

Therefore, the following hold:

1) If $x \in X(k)$, then $T_x = \{1\}$, hence pr_X maps Z_x isomorphically onto G_k. Thus $\tilde{x}|x$ gives rise canonically to a group theoretical section $s_x : G_k \to Z_x \subset \pi_1(X)$ of the canonical projection $pr_X : \pi_1(X) \to G_k$. In other words, the k-rational point $x \in X$ gives rise canonically to the conjugacy class of the group theoretical section s_x of the canonical projection pr_X.

2) If $x \in Y(k)\backslash X(k)$ is a k-rational point "at infinity" of X, then the inertia group T_x is not necessarily trivial, and the split exact sequence $1 \to T_x \longrightarrow Z_x \xrightarrow{pr_X} G_k \to 1$ gives rise to a "bouquet" of conjugacy classes of sections $\tilde{s}_x : G_k \to \pi_1(X)$ of pr_X. Concretely, the space

Date: August 11, 2007.

1991 *Mathematics Subject Classification.* Primary 12E, 12F, 12G, 12J; Secondary 12E30, 12F10, 12G99.

Key words and phrases. anabelian geometry, pro-ℓ groups, Galois theory, function fields, valuations, Zariski prime divisors, Hilbert decomposition theory.

Supported by NSF grant DMS-0401056. I would like to thank David Harbater, Minhyong Kim, Jochen Koeningsmann, Mohamed Saidi, Jakob Stix, Tamás Szamuely, and many others for the interesting discussion concerning the (birational) section Conjecture.

of all these conjugacy classes of sections is the non-commutative continuous $\mathrm{H}^1_{\mathrm{cont}}(G_k, T_x)$ defined via the split exact sequence $1 \to T_x \longrightarrow Z_x \xrightarrow{pr_X} G_k \to 1$.

Note that in the case $\mathrm{char}(k) = 0$, one has $T_x \cong \widehat{\mathbb{Z}}(1)$ as G_k-modules. In particular, the space of sections $\mathrm{H}^1_{\mathrm{cont}}(G_k, T_x)$ is well understood, as via Kummer theory one has $\mathrm{H}^1_{\mathrm{cont}}(G_k, T_x) \cong \widehat{k}$, where the last group is the adic completion of the multiplicative group $k^\times$ of the field k.

Grothendieck's section Conjecture asserts roughly that under certain "anabelian hypotheses" all the sections of pr_X arise in the way described above. Precisely, recall that a finitely generated field is a field which is finitely generated over its prime field. A curve $X \to k$ is called hyperbolic, if it has a smooth geometrically integral completion $Y \to k$ (hence X itself is smooth and geometrically integral), and X has negative Euler characteristic. Equivalently, if $r = |\overline{Y} \backslash \overline{X}|$, and g is the geometric genus of X, then $2g - 2 + r > 0$.

Section Conjecture. *Let k be a finitely generated field, $X \to k$ a non-isotrivial hyperbolic curve. Then all the sections of $pr_X : \pi_1(X) \to G_k$ arise in the way explained above.*

Related to the above Section conjecture (for curves), but weaker than it, is the birational section Conjecture, which is derived from the section Conjecture for curves by starting with some complete geometrically integral smooth curve and taking limits over a system of Zariski open neighborhoods of its generic point. In a birational setting it sounds as follows: For the beginning, let k be an arbitrary base field, and $K|k$ a function field of a geometrically integral complete smooth curve $X \to k$. Then there exists a canonical bijection between the k-places v of $K|k$ and the closed points x of X, by interpreting each such closed point as a Weil prime divisor of X. If v and x and correspond to each other, then the corresponding residue fields are equal: $\kappa(x) = \kappa(v)$. Hence x is a k-rational point if and only if v is k-rational place of $K|k$. Let $\tilde{K}|K$ be some Galois extension, and let $\tilde{G}_K := \mathrm{Gal}(\tilde{K}|K)$ denote the Galois group of $\tilde{K}|K$. Further let $\tilde{k} := \overline{k} \cap \tilde{K}$ be the "constants" of $\tilde{K}$, and set $\tilde{G}_k := \mathrm{Gal}(\tilde{k}|k)$. Hence one has a canonical exact sequence

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

For a k-rational point x of X and its k-rational place v of K, let $\tilde{v}$ be a prolongation to $\tilde{K}$, and $T_{\tilde{v}} \subseteq Z_{\tilde{v}}$ be the inertia, respectively decomposition, groups of $\tilde{v}|v$, and $G_{\tilde{v}} := \mathrm{Aut}_{Kv}\big(\tilde{K}\tilde{v}\big)$ the residual automorphism group. By general Hilbert decomposition theory one has a canonical exact sequence

$$(*) \qquad 1 \to T_{\tilde{v}} \to Z_{\tilde{v}} \to G_{\tilde{v}} \to 1\,.$$

We remark that in general $\tilde{k} \subset \tilde{K}\tilde{v}$ can be a strict inclusion, hence in particular, the canonical projection $\tilde{G}_v \to \tilde{G}_k$ is not an isomorphism, even if v is a k-rational place of $K|k$. Further, the above exact sequence $(*)$ is not necessarily split. The conclusion is that in general a k-rational point x of X does not necessarily give rise to a section of $\tilde{p}_K : \mathrm{Gal}(\tilde{K}|K) \to \mathrm{Gal}(\tilde{k}|k)$.

Nevertheless, if $\tilde{k} = \overline{k}$ is an algebraic closure of k, then $\tilde{K}\tilde{v} = \overline{k}$, and if v is a k-rational place of $K|k$, then one has: $G_{\tilde{v}} = G_k$, and the exact sequence $(*)$ is split. Hence in this case, every k-rational point x gives rise via its k-rational place v to a bouquet of conjugacy classes of section $s_x : G_k \to \mathrm{Gal}(\tilde{K}|K)$ of the projection $\tilde{p}_K : \mathrm{Gal}(\tilde{K}|K) \to G_k$. Precisely, the space of such conjugacy classes is the non-commutative continuous cohomology group $\mathrm{H}^1_{\mathrm{cont}}(G_k, T_{\tilde{v}})$

defined via the split exact sequence $(*)$ above. And note that if $\mathrm{char}(k)=0$, then as in the case of curves, one has $T_x \cong \widehat{\mathbb{Z}}(1)$ as G_k-modules, and therefore $\mathrm{H}^1_{\mathrm{cont}}(G_k, T_x) \cong \widehat{k}$.

After this preparation, we can announce the following:

Birational section Conjecture. *Let k be the pure inseparable closure of a finitely generated infinite field, and $\kappa(X)$ the function field of smooth complete curve $X \to k$. Then every section of the canonical projection $G_{\kappa(X)} \to G_k$ arises from some k-rational point x of X in the way described above.*

There are (several) variants of the the above conjectures, from which we mention the *p-adic (birational) section Conjecture*: This is the question whether the assertions of the above section Conjecture, respectively birational section Conjecture, are true over a base field k which is a finite extension $k|\mathbb{Q}_p$ of $\mathbb{Q}_p$. We call the resulting conjectures the *p-adic section Conjecture,* respectively the *p-adic birational section Conjecture.*

Before coming to the content of this manuscript, let me mention that the section Conjecture is essentially open, as well as it is unknown what is the precise relation between the section Conjecture and the Mordell Conjecture, now Faltings' Theorem [Fa1]. There are nevertheless some interesting results concerning the section Conjecture, from which we mention the following: Nakamura's description of "cuspidal points" in a global setting [Na]; Tamagawa's "section Conjecture" for hyperbolic curves over finite fields [Ta], see also [Fa2]; Mochizuki's description of cuspidal points in the p-adic setting [Mo]; the results by Kim [Ki] concerning the section Conjecture in the motivic setting. And finally the proof of the p-adic birational section Conjecture, see Koenigsmann [Ko] using among other things Pop [P1]. (Actually, although not explicitly stated in [P1] as such, a proof of the p-adic birational section Conjecture can be immediately deduced from [P1], Introduction, assertions E.11 and E.12, by using well known facts about p-adically closed fields.)

The aim of this note is to prove a very "minimalistic" form of the p-adic birational section Conjecture, which in other words is a very strong —and I would say unexpected— form of the p-adic birational section Conjecture, and reads as follows: Let $k|\mathbb{Q}_p$ be a finite extension with $\mu_p \subset k$. Let $X \to k$ be a complete smooth geometrically integral curve, and $K := \kappa(X)$ its function field. We denote by $K' = K[\sqrt[p]{K}\,]$ a maximal $\mathbb{Z}/p$ elementary abelian extension of K, and by$K'' = K'[\sqrt[p]{K'}\,]$ a maximal $\mathbb{Z}/p$ elementary abelian extension of K'. Then $K''|K$ is a Galois extension, which we call the maximal $\mathbb{Z}/p$ elementary meta-abelian extension of K. Then $k' := \overline{k} \cap K'$, and $k'' := \overline{k} \cap K''$ are the maximal $\mathbb{Z}/p$ elementary abelian extension, respectively the maximal $\mathbb{Z}/p$ elementary meta-abelian extension of k. We denote by $\overline{G}'_K := \mathrm{Gal}(K'|K)$ and $\overline{G}''_K := \mathrm{Gal}(K''|K)$, and by $\overline{G}'_k := \mathrm{Gal}(k'|k)$ and $\overline{G}''_k := \mathrm{Gal}(k'|k)$, the corresponding Galois groups. Further we consider the canonical surjective projections:

$$pr'_K : \overline{G}'_K \to \overline{G}'_k, \quad pr''_K : \overline{G}''_K \to \overline{G}''_k.$$

We will say that a section $s' : \overline{G}'_k \to \overline{G}'_K$ of $pr'_K : \overline{G}'_K \to \overline{G}'_k$ is liftable, if there exists a section $s'' : \overline{G}''_k \to \overline{G}''_K$ of $pr''_K : \overline{G}''_K \to \overline{G}''_k$ which lifts s'.

The "minimalistic" form of the p-adic birational section Conjecture is the following:

Theorem A. *In the above notations, suppose that k contains the p^{th} roots of unity. Then the following hold:*

1) *Every k-rational point x of X gives rise to a bouquet of liftable sections* $s'_x : \overline{G}'_k \to \overline{G}'_K$.

2) *Let* $s' : \overline{G}'_k \to \overline{G}'_K$ *be a liftable section. Then there exists a unique k-rational point x of X such that s' equals one of the sections s'_x as defined above.*

Before embarking on the proof, we should remark that by "taking limits", Theorem A implies the p-adic birational section conjecture, *but not vice-versa!*

We will actually prove the following stronger result, from which Theorem A above can be easily deduced. (See Section 2, F), for more information on p-adically closed fields):

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

1) *Let w be a p-adic valuation of K which prolongs v and has the same p-adic rank as v, and let $Z''_w \subset \overline{G}''_K$ be the decomposition group of some prolongation of w to K''. Then $pr''_K(Z''_w) = \overline{G}''_k$, and $pr''_K : Z''_w \to \overline{G}''_k$ is split. Hence w gives rise to a bouquet of liftable sections $s'_w : \overline{G}'_k \to \overline{G}'_K$ of pr'_K.*

2) *Conversely, let $s' : \overline{G}'_k \to \overline{G}'_K$ be a liftable section. Then there exists a p-adic valuation w of K which prolongs v to K and has the same p-adic rank as v such that $s' = s'_w$ as indicated above.*

Concerning the proof of Theorem B —thus also of Theorem A above: The main technical point is a generalization of the Tate–Roquette–Lichtenbaum Local-Global Principle for Brauer groups of function fields $K|k$ of curves over p-adically closed fields, as introduced and studied in Pop [P1]. As a result of that, one is lead to analyze the cohomological behavior of $\mathbb{Z}/p$-elementary abelian extension of Henselizations of K.

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 we have by definition $G^0 := G$, and $G^i := [G^{i-1}, G^{i-1}](G^{i-1})^p$ for $i > 0$. We will further set $\overline{G}^i := G/G^i$ for $i > 0$. Hence in particular we have: $\overline{G}' := G/G^1$ is the maximal $\mathbb{Z}/p$-elementary quotient of G, and $\overline{G}'' := G/G^2$ 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 checks without any difficulty that mapping every profinite group G to $\overline{G}^i$, $i > 0$, defines a functor from the category of all profinite groups onto the category of all profinite groups whose derived $\mathbb{Z}/p$ series has length $\leq i$. In particular, if $pr : G \to H$ is a (surjective) morphism of profinite groups, then the following hold:

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

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

Finally, in the context above, 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, which 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 notations of the previous sub-section, for all $i>0$ we have

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

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

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

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

Lemma 2.1. *In the above notations, let $s':\overline{H}'\to\overline{G}'$ be a* liftable *section of $pr':\overline{G}'\to\overline{H}'$, 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 $\chi_H,\psi_H\in\mathrm{Hom}\big(H,\mathbb{Z}/p\big)$ and the induced ones $\chi_\Gamma,\psi_\Gamma\in\mathrm{Hom}\big(\Gamma,\mathbb{Z}/p\big)$, 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 equivalence i) $\Leftrightarrow$ ii) follows from the well known fact that

$$\ker\big(\,\mathrm{H}^2(\overline{H}',\mathbb{Z}/p)\xrightarrow{\mathrm{inf}}\mathrm{H}^2(\overline{H}'',\mathbb{Z}/p)\,\big)=\ker\big(\,\mathrm{H}^2(\overline{H}',\mathbb{Z}/p)\xrightarrow{\mathrm{inf}}\mathrm{H}^2(H,\mathbb{Z}/p)\,\big)$$

a fact which itself can be immediately deduced from the "five term exact sequence" coming from spectral theory. Implication ii) $\Rightarrow$ iii) follows by the fact that $\chi_\Gamma\cup\psi_\Gamma$ is the image of $\chi_H\cup\psi_H$ under the inflation map $\mathrm{H}^2(H,\mathbb{Z}/p)\xrightarrow{\mathrm{inf}}\mathrm{H}^2(\Gamma,\mathbb{Z}/p)$. Finally, the implication iii) $\Rightarrow$ i) is as follows: Suppose that $\chi_\Gamma\cup\psi_\Gamma=\delta(\varphi)$ is the boundary of some map $\varphi:\Gamma\to\mathbb{Z}/p$. We claim that $\chi_H\cup\psi_H=0$ in $\mathrm{H}^2(\overline{H}'',\mathbb{Z}/p)$. Indeed, $\chi_\Gamma\cup\psi_\Gamma=\delta(\varphi)$ means that for all $g,h\in\Gamma$ one has:

$$\chi_\Gamma\cup\psi_\Gamma(g,h)=g\,\varphi(h)-\varphi(gh)+\varphi(h)=\varphi(h)-\varphi(gh)+\varphi(h),$$

the last equality taking place by the fact that G, hence Γ, act trivially on $\mathbb{Z}/p$. Now if g or h lie in $G^1\subset\Gamma$, then we have $\chi_\Gamma\cup\psi_\Gamma(g,h)=0$. Equivalently, if g or h lie in $G^1\subset\Gamma$, then $\varphi(h)-\varphi(gh)+\varphi(h)=0$. In particular, the restriction of φ to G^1 is a group homomorphism to $\mathbb{Z}/p$. In particular, the restriction of φ to $G^2=[G^1,G^1](G^1)^p$ is trivial, and finally φ factors through $\overline{G}''$. Therefore, $\chi_G\cup\psi_G=0$ in $\mathrm{H}^2(\overline{G}'',\mathbb{Z}/p)$. Now let $s'':\overline{H}''\to\overline{G}''$ be a lifting of the section s'. Then the restriction of $\chi_G\cup\psi_G=0$ to $s''(\overline{H}'')$ is trivial too, i.e., $\chi_H\cup\psi_H=0$ in $\mathrm{H}^2\big(s''(\overline{H}''),\mathbb{Z}/p\big)$. Thus finally, $\chi_H\cup\psi_H=0$ in $\mathrm{H}^2\big(\overline{H}'',\mathbb{Z}/p\big)$, as claimed. $\square$

C) *Basics from Galois cohomology*

Let K be an arbitrary field of characteristic $\neq p$, and G_K be its absolute Galois group. Further let G_K^i and $\overline{G}_K^i$ be the derived $\mathbb{Z}/p$ series, respectively quotients of G_K. We recall the following basic/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 choosing some identification $\imath : \mu_p \to \mathbb{Z}/p$ of trivial G_K modules, we get:

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

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

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

Combining these observations with the Lemma 2.1 above we get the following: Let $K|k$ be a regular field extension, $pr_K : G_K \to G_k$ the canonical (surjective) projection, and let $pr^i_K : \overline{G}^i_K \to \overline{G}^i_k$, $i > 0$, be defined as above. Suppose that $\mathrm{char}(k) \neq p$, and $\mu_p \subset k$. Then $K' = K[\sqrt[p]{K^\times}]$ is a maximal $\mathbb{Z}/p$-elementary extension of K, hence $\overline{G}'_K = \mathrm{Gal}(K'|K)$. Further, $k' = K' \cap \overline{k}$ is a maximal $\mathbb{Z}/p$-elementary extension of k, and $\overline{G}'_k = \mathrm{Gal}(k'|k)$, etc.

Lemma 2.2. *In the above context, let $s' : \overline{G}'_k \to \overline{G}'_K$ be a liftable section of $pr'_K : \overline{G}'_K \to \overline{G}'_k$, and let $M \subset K'$ be the fixed field of $s'(\overline{G}'_k)$ in K'. Then for any elements $a, b \in k^\times$, and the corresponding p-cyclic k-algebras $A_k(a, b)$, respectively $A_M(a, b)$, one has: $A_k(a, b)$ 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 $\neq p$ containing μ_p. Let v be a valuation of K, and v' some prolongation of v to K', and $V_{v'} \subseteq T_{v'} \subseteq Z_{v'}$ be the ramification, the inertia, and the decomposition, groups of $v'|v$ in $\overline{G}'_K$, respectively. We remark that because $\overline{G}'_K$ 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 2.3. *In the above notations, the following hold:*

1) Let $U^v := 1 + p^2\mathfrak{m}_v$. Then K^Z contains $\sqrt[p]{U^v}$, and $K^Z = K[\sqrt[p]{U^v}\,]$, provided 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 $K'v' = (Kv)'$. Hence $G_v := Z_v/T_v = \overline{G}'_{Kv}$. And if $p = \mathrm{char}(Kv)$, then $V_v = T_v$, and the residue field $K'v'$ contains $(Kv)^{\frac{1}{p}}$.

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

Proof. Everything is clear, but maybe the assertion concerning the independent valuations w^1 and w^2 from assertion 1): Consider $x \neq 0$ arbitrary. Since w^1 and w^2 are independent, there exist $y \neq 0$ which are arbitrarily close to 1 with respect to w^1 and arbitrarily close to x with respect to w^2. 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 we finally have $\sqrt[p]{x} \in K^{Z_{w^2}} K^{Z_{w^1}}$. □

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 $\overline{G}'_L := \mathrm{Gal}(L'|L)$ be its Galois group. Since w is Henselian, w has a unique prolongation to L', which we again denote by w'.

Lemma 2.4. *In the above context, suppose that v is rank one valuation. Let $\Lambda|L$ be a sub-extension of $L'|L$ such that $L'|\Lambda$ is a finite extension. Then the following hold:*

1) *The residue field Λw contains $(Lw)^{\frac{1}{p}}$.*
2) *If $wL \not\subset p \cdot w\Lambda$, then w is discrete on L, and Lw is finite.*

Proof. The proof is inspired by [P1], Korollar 2.7, and uses in an essential way Lemma 2.6 of loc.cit. Let $\mathcal{O}$ and $\mathfrak{m}$ be the valuation ring, respectively the valuation ideal of w. Then by loc.cit., one has exact sequences of the form:

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

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 p^{th} powers of all the elements of $L^\times$, and $K^\times/\Delta$ is canonically Pontrjagin dual (thus non-canonically isomorphic) to $\mathrm{Gal}(L'|\Lambda)$. In particular, $L^\times/\Delta$ is a finite elementary $\mathbb{Z}/p$ abelian group. Hence by assertions $(*)$, it follows that denoting $\Delta_1 := \Delta \cap (1+\mathfrak{m})$ and by Δw the image of Δ in $Lw^\times$, we have: $(1+\mathfrak{m})/\Delta_1$ and $Lw^\times/\Delta w$ are finite groups.

To 1): By Lemma 2.3, 2), it follows that $L'w$ contains $(Lw)^{\frac{1}{p}}$. Further, the Frobenius morphism maps Δw isomorphically onto $(\Delta w)^{\frac{1}{p}} \subseteq (Lw)^{\frac{1}{p}}$. Hence it defines an isomorphism of $Lw^\times/\Delta w$ onto $(Lw^\times)^{\frac{1}{p}}/(\Delta w)^{\frac{1}{p}}$. Thus finally $(Lw^\times)^{\frac{1}{p}}/(\Delta w)^{\frac{1}{p}}$ is finite. Since $(\Delta w)^{\frac{1}{p}} \subset \Lambda w$, it follows that $(Lw^\times)^{\frac{1}{p}}/(\Lambda w)^\times$ is finite. Now we conclude as in the proof of assertion 1 of loc.cit.: First, if Lw is finite, then Lw is perfect, thus there is nothing to prove. Now suppose that Lw is infinite. Since $(Lw^\times)^{\frac{1}{p}}/(\Lambda w)^\times$ is finite, for every $a \in (Lw^\times)^{\frac{1}{p}}$ there exist $x, y, z \in \Lambda w$, $x \neq y$, such that $a - x = (a-y)z$. Hence $z \neq 1$, and $a = (x - yz)/(1-z)$ lies in Λw.

To 2): By the discussion above, it follows that $(1+\mathfrak{m})/\Delta_1$ is finite, and let $1+a_j$, $1 \leq j \leq n$, be representatives for $(1+\mathfrak{m})/\Delta_1$.

Case 1) w is not discrete on L.

Then for every $\gamma \in wL/p$ there exists some $a \in L^\times$ such that wa is a representative for $\gamma \in wL/p$, and further one has: $0 < wa < wp, wa_j$ for all $j = 1, \dots n$. Let us set

$$1 + a = (1+b)\prod_j (1+a_j)^{r_j}$$

with $1 + b \in \Delta$. Then by the choice of a it immediately follows by the ultra-metric triangle inequality that $wa = wb$. On the other hand, $\sqrt[p]{1+b} \in \sqrt[p]{\Delta} \subset \Lambda$. Hence $1 + b = (1+c)^p$ for some $c \in \Lambda$ satisfying $wc > 0$. Since $wb = wa < wp$, one immediately gets that $wb = wc^p$ in $w\Lambda$. Thus $wa = p \cdot wc$ in $v\Lambda$. Hence finally $wL \subseteq p \cdot w\Lambda$.

Case 2) w is discrete on L.

Suppose that Lw is not finite. Let $\mathfrak{m} \subset \mathcal{O} \subset L$ be the valuation ideal, respectively valuation ring, of w in L. Since L contains μ_p, and $p \geq 2$, 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

$$\phi : (1+\mathfrak{m})/(1+\mathfrak{m}^2) \to \kappa_{\mathcal{O}}^{+}, \quad 1+x\pi \mapsto x \,(\operatorname{mod} \mathfrak{m}).$$

Hence it follows that $(1+\mathfrak{m})/(1+\mathfrak{m})^p$ is infinite, as it has as homomorphic image the infinite group $(1+\mathfrak{m})/(1+\mathfrak{m}^2) \cong \kappa_{\mathcal{O}}^{+}$. Next recall that $(1+\mathfrak{m})/\Delta_1$ is a finite group. Therefore $\phi(1+\mathfrak{m})/\phi(\Delta_1) = \kappa_{\mathcal{O}}^{+}/\phi(\Delta_1)$ is finite too. Hence there exist infinitely many elements $1+x\pi \in \Delta_1$ with $x \in \mathcal{O}^{\times}$. For any such $1+x\pi \in \Delta_1$ we have $(1+x\pi)^{\frac{1}{p}} \in \Lambda$, hence there exists some $\pi_x \in \Lambda$ such that $1+x\pi = (1+\pi_x)^p$ in Λ. Thus we have $w\pi = pw\pi_x$ in $w\Lambda$. Since $wL = \mathbb{Z}\, w\pi$, it finally follows that $wL \subset p \cdot w\Lambda$. $\square$

E) *Inertial cohomology*

In this subsection we recall a well known result concerning the cohomology of the maximal inert extension of a Henselian field (which it seems goes back to Witt). The situation is as follows: Let L be a Henselian field with respect to a valuation w, and $L_1|L$ 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, respectively valuation ideals. As remarked in [P1], Lemma 2.2, the group of principal units $1+\mathfrak{m}_{L_1}$ is G-cohomologically trivial, and for every integer n one has a split exact sequence of Tate cohomology groups:

$$0 \to \widehat{\mathrm{H}}^i(G, \kappa_{L_1}^{\times}) \to \widehat{\mathrm{H}}^i(G, L_1^{\times}) \to \widehat{\mathrm{H}}^{i-1}(G, (\mathbb{Q}\otimes wL)/wL) \to 0.$$

We will use this result in the special situation $i = 2$. Hence we have a split exact sequence of the form:

$$0 \to \mathrm{Br}(\kappa_{L_1}|\kappa_L) \to \mathrm{Br}(L_1|L) \to \mathrm{Hom}\big(G, (\mathbb{Q}\otimes wL)/wL\big) \to 0.$$

We also remark that if $\Lambda|L$ is some algebraic extension, say linearly disjoint with L_1, and $\Lambda_1 = \Lambda L_1$ is the compositum (in some fixed algebraic closure), then the above exact sequence gives rise to a commutative diagram of the form

$$\begin{array}{ccccccc} 0 \to & \mathrm{Br}(\kappa_{L_1}|\kappa_L) & \to & \mathrm{Br}(L_1|L) & \to & \mathrm{Hom}\big(G, (\mathbb{Q}\otimes wL)/wL\big) & \to 0 \\ & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & \\ 0 \to & \mathrm{Br}(\kappa_{\Lambda_1}|\kappa_\Lambda) & \to & \mathrm{Br}(\Lambda_1|\Lambda) & \to & \mathrm{Hom}\big(G, (\mathbb{Q}\otimes w\Lambda)/w\Lambda\big) & \to 0 \end{array}$$

where the first two vertical maps are the canonical restriction maps, and the last one is induced by the canonical embedding $wL \hookrightarrow w\Lambda$.

The very specific situation we will be considering is the one in the context of the previous subsection, namely: $\mathrm{char}(L) = 0$ and $\mathrm{char}(\kappa_L) = p > 0$, and has w is a rank one valuation. Further we take for $L_1|L$ a p-cyclic unramified extension, hence $G \cong \mathbb{Z}/p$. And take $\Lambda|L$ to be an elementary $\mathbb{Z}/p$ abelian extension such that $K'|\Lambda$ is finite, and such that $\Lambda|L$ and $L_1|L$ are linearly disjoint.

Lemma 2.5. *In the above context, suppose that the restriction map*

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

is non-trivial. Then w is discrete on L and Lw is a finite extension of $\mathbb{F}_p$.

Proof. Since $G = \mathrm{Gal}(L_1|L)$ has order p, it follows that $\mathrm{Br}(L_1|L)$ and $\mathrm{Br}(\kappa_{L_1}|\kappa_L)$ are torsion groups of exponent p. In particular, the restriction map

$$\mathrm{Br}(\kappa_{L_1}|\kappa_L) \xrightarrow{\mathrm{res}} \mathrm{Br}(\kappa_L^{\frac{1}{p}})$$

is trivial. On the other hand, by Lemma 2.4, 1), above, we have $\kappa_L^{\frac{1}{p}} \subset \kappa_\Lambda$. Hence the restriction map

$$\mathrm{Br}(\kappa_{L_1}|\kappa_L) \xrightarrow{\mathrm{res}} \mathrm{Br}(\kappa_\Lambda)$$

is trivial. Therefore, from the commutativity of the diagram above, it follows that the restriction map

$$\mathrm{res} : \mathrm{Hom}\big(G, (\mathbb{Q} \otimes wL)/wL\big) \to \mathrm{Hom}\big(G, (\mathbb{Q} \otimes w\Lambda)/w\Lambda\big)$$

is non-trivial. Equivalently, since $G \cong \mathbb{Z}/p$, the image of $wL \hookrightarrow w\Lambda$ is not contained in $p \cdot w\Lambda$. But then by by Lemma 2.4, 2), above, it follows that wL is discrete and Lw is finite, as claimed. $\square$

F) *On* $\overline{G}'_{k_1}$ *and* $\mathrm{Br}(k_1)$

Let k be a finite extension of $\mathbb{Q}_p$ with $\mu_p \subset k$. Let $l|k$ an arbitrary algebraic extension of k, and let $[l : k]$ denote its degree (as a super-natural number). As usual, let $l'|l$ be a maximal $\mathbb{Z}/p$-elementary extension of l, and $G'_l := \mathrm{Gal}(l'|l)$ its Galois group.

Lemma 2.6. *In the above contex the following hold:*

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

2) *Suppose that* $[l : k]$ *is not divisible by* p. *Then* $G'_l := \mathrm{Gal}(l'|l) \cong (\mathbb{Z}/p)^{e_l+2}$, *where* $e_l := [l : \mathbb{Q}_p]$.

Proof. To 1): By the the properties of p-adic fields we have: After identifying $\mathrm{Br}(k)$ with $\mathbb{Q}/\mathbb{Z}$ via the invariant isomorphism $\mathrm{inv}_k : \mathrm{Br}(k) \to \mathbb{Q}/\mathbb{Z}$, the restriction map $\mathrm{Br}(k) \to \mathrm{Br}(l)$ becomes the multiplication by $[l : k]$. Hence ${}_p\mathrm{Br}(k) \to \mathrm{Br}(l)$ is injective if and only if $[l : k]$ is not divisible by p.

To 2): If $l|k$ is finite, then the assertion follows by local class field theory. Further, the canonical projection $\overline{G}'_l \to \overline{G}'_k$ is surjective, as $[l : k]$ is prime to p. Finally, by taking limits over all the finite sub-extensions $l_i|k$ of $l|k$, the assertion follows. $\square$

G) *A local-global principle for the Brauer group*

The final tool in the proof of the main result is the Local-Global Principle originating in work of Tate [T], Roquette [Ro], and finally Lichtenbaum [Li], for the Brauer group of curves over p-adic fields, see especially [Li]. We begin by recalling the basic facts about p-adic valuations and p-adically closed fields, see [P–R] more details.

A valuation v of a field k is called **(formally) p-adic**, if the residue field kv is a finite field $\mathbb{F}_{p^{f_v}}$, 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 invariant $d_v := e_v f_v$ is called the **p-adic 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 $v(p) \neq 0$. Further, if $l|k$ is a finite field extension, and v is a p-adic valuation on k, then all the prolongations w of v to l are p-adic valuations, and $e_w \geq e_v$, $f_w \geq f_v$, hence $d_w \geq d_v$. Finally, if v is a p-adic valuation of k, then $\mathcal{O}_1 := \mathcal{O}[1/p]$ is the valuation ring of the unique maximal proper coarsening of v; and v_1 is called the canonical coarsening of v. Note that setting $k_0 := kv_1$, and $v_0 = v/v_1$ the corresponding valuation on k_0 we have: 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, v has rank one if and only if v_1 is the trivial valuation if and only if $v = v_0$.

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: If v has a prolongation w to l with $d_w = d_v$, then $l = k$. One has the following characterization of the p-adically closed fields: For a field k endowed with a p-adic valuation v, in the above notations the following are equivalent:

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

ii) v is Henselian, and $vK\,/\,(\mathbb{Z}\cdot 1_v)$ is divisible.

iii) v_1 is Henselian, and $v_1 k$ is divisible (maybe trivial), and the residue field $k_0 := kv_1$ is relatively algebraically closed in its completion $\hat{k}_0$ (which is itself a finite extension of $\mathbb{Q}_p$).

The following hold: If k is p-adically closed with respect to the p-adic valuation v, and $l \subseteq k$ is a subfield which is relatively closed in k, then l is p-adically closed with respect to $w := v|_l$, and v and w have equal p-adic ranks. The elementary equivalence class of the p-adically closed field k is completely determined by the *absolute subfield* $k^{\mathrm{abs}} := k \cap \overline{\mathbb{Q}}$ of k. Note that the p-adic valuation of k^{abs} is discrete, and k^{abs} is actually the relative algebraic closure of $\mathbb{Q}$ in $k_0 := kv_1$. Finally, the p-adic valuation of k_0 is exactly the quotient $v_0 := v/v_1$ of v by its canonical coarsening v_1. And k has v_1-inert algebraic extension only, hence in particular, the canonical projection

$$\pi_{v_1} : G_k \to G_{k_0}$$

is an isomorphism. Thus viewing $k|k_0$ as a field extension via some elmbedding $k_0 \hookrightarrow k$, it follows that the projections

$$(\dagger) \qquad pr^i_k : \overline{G}^i_k \to \overline{G}^i_{k_0}$$

are isomorphisms for all $i > 0$.

After this short excursion into p-adically closed fields, we recall the following result, which was proved in [P1], Theorem 4.5, and uses in an essential way the mentioned results by Tate, Roquette, Lichtenbaum:

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

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

We will use a more special form of the above Fact which reads as follows: Let w be a prolongation of v to M, and $\mathcal{O}_w, \mathfrak{m}_w$ be its valuation ring, respectively valuation ideal. 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 L of the canonical coarsening v_1 of v. Further, setting $M_0 := Mw_1$ and $w_0 := w/w_1$, it follows by general valuation theory that $M_0|k_0$ is a field extension with $\mathrm{tr.deg}(M_0|k_0) \leq 1$, and 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), 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), ii), above.

Fact 2.7. *Let k be a p-adically closed field, and let $M|k$ be a field extension of transcendence degree* $\mathrm{tr.deg}(M|k) \leq 1$. *Let $\mathcal{W}$ be the set of all the prolongations $w|v$ of v to M satisfying the equivalent conditions* i), ii)*, above. Then the canonical exact sequence of Brauer groups below 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 denoting by M_w^{h} 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 $\mathrm{Br}(M_w^{\mathrm{h}})$, it follows that $A_{M_{\tilde{w}}^{\mathrm{h}}} \neq 0$ in $\mathrm{Br}(M_{\tilde{w}}^{\mathrm{h}})$. $\square$

3. Proof of Theorem B

In the context of Theorem B, let $s' : \overline{G}'_k \to \overline{G}'_K$ be a liftable section of $pr'_K : \overline{G}'_K \to \overline{G}'_k$. Let $M \subset K'$ be the fixed field of $s'(\overline{G}'_k)$. Consider $a, b \in k$ such that $k_1 := k[\sqrt[p]{a}]$ is the unique unramified extension of degree p of k, and such that 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 2.2, it follows that $A_M(a,b)$ is non-trivial in $\mathrm{Br}(M)$. Hence by Fact 2.7, it follows that there exists some prolongation $w \in \mathcal{W}$ of v to M such that denoting by $\Lambda := M_w^{\mathrm{h}}$ the Henselization of M with respect to w, one has: $A_\Lambda(a,b) \neq 0$ in $\mathrm{Br}(\Lambda)$. By abuse of language, we will denote by w the Henselian prolongation of w to Λ, etc.

For a valuation w as above, let $L := K_w^{\mathrm{h}} \subseteq \Lambda$ 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 $LM = \Lambda$. And since $A_\Lambda(a,b) \neq 0$ in $\mathrm{Br}(\Lambda)$, one also has $A_L(a,b) \neq 0$ in $\mathrm{Br}(L)$, as $L \subset \Lambda$.

Lemma 3.1. *The valuation w is a p-adic valuation of L.*

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

a) w_1 prolongs of 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, and w_0 and v_0 are Henselian, as w and v were so.

c) $L'w_1|Lw_1$ is the maximal $\mathbb{Z}/p$ elementary abelian extension of $L_0 = Lw_1$, by Lemma 2.3, 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, it follows that $L'w_1|\Lambda w_1$ is finite, by the fundamental inequality. Since $L'w_1 = L'_0$, we get: $L'_0|\Lambda_0$ is finite.

Recall the unique 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 an w-unramified cyclic extension with Galois group $\cong G$ canonically. 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. We denote the corresponding residue fields by $k_{01} := k_1 v_1$, and $\Lambda_{01} := \Lambda_1 w_1$. And remark that $k_{01}|k_0$ is a v_0-unramified cyclic extension with Galois group $\cong G$ canonically. Correspondingly, $\Lambda_{01}|\Lambda_0$ is a w_0-unramified cyclic extensions with Galois group $\cong G$ canonically.

We next consider the resulting commutative diagram 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 Section 1, E):

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

Hence we deduce that $\mathrm{Br}(k_{01}|k_0) \to \mathrm{Br}(\Lambda_0)$ is non-trivial.

Now let us set $L_1 := Lk_1$ and denote $L_{01} := L_1 w_1$. Then reasoning as above we get: $L_1|L$ is w-unramified, hence w_1-unramified. And further, $L_{01}|L_0$ is a w_0-unramified extension with Galois group $\cong G$ canonically. 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 we have: $\mathrm{Br}(L_{01}|L_0) \to \mathrm{Br}(\Lambda_0)$ is non-trivial.

Hence by Lemma 2.5 applied to L_0 endowed with the Henselian rank one valuation w_0, and 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: 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 3.2. *The p-adic valuation w from previous Lemma has p-adic rank equal to the p-adic rank of v and satisfies: $s'(\overline{G}'_k) \subseteq Z_w$.*

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 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 by Lemma 2.6, 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 $M = (K')^{s'(\overline{G}'_k)}$ is the fixed field of $s'(\overline{G}'_k)$ in K'; further, $L' = LK'$, and $\Lambda = ML$ inside L', by the discussion at above at the beginning of the proof. From this we deduce the following sequence of inequalities:

$$(*) \qquad [k' : k] = |G'_k| = [K' : M] \geq [LK' : LM] = [L' : \Lambda]\,.$$

Further, since k is p-adically closed, hence $pr_k : G'_k \to G_{k_0}$ is an isomorphism, it follows that $[k' : k] = [k'_0 : k_0]$. Further, by the fundamental inequality we have $[L' : \Lambda] \geq [L'w_1 : \Lambda w_1]$. 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:

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

On the other hand, by Lemma 2.6, 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 $e_{k_0} \geq e_{L_0}$. On the other hand, $k_0 \subseteq L_0$, implies $e_{k_0} \leq e_{L_0}$. Hence finally $e_{k_0} = e_{L_0}$, and $\hat{k}_0 = \hat{L}_0$. Equivalently, w is a p-adic valuation having p-adic rank equal to

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

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

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

Equivalently, $s'(\overline{G}'_k) \subseteq Z_w$, as claimed.

□

Coming back to the proof of Theorem B, we have the following: Let $M \subseteq K'$ be the fixed field of $s'(G'_k)$ in K'. Then there exist p-adic valuations w of K such that w prolong v to K and have p-adic rank d_w equal to the p-adic rank d_v of v; and moreover, $s'(G'_k)$ is contained in the decomposition group Z_w of w in $\overline{G}'_K$.

Remark 3.3. The precise structure of Z_w can be deduced as follows: First, let w_1 is the canonical coarsening of w, and $T_{w_1} \subset Z_{w_1}$ be the inertia/decomposition groups above w_1 in G'_K. Then $Z_w = Z_{w_1}$, and the projection $pr'_K : \overline{G}'_K \to \overline{G}'_k$ gives rise to a split exact sequence:

$$1 \to T_{w_1} \to Z_{w_1} \xrightarrow{pr'_K} G'_k \to 1,$$

and $s'(G'_k) \subset Z_{w_1} = Z_w$ is a complement of T_{w_1}. Further, if T_{w_1} is non-trivial, then $T_{w_1} \cong \mu_p$ canonically as a G'_k-module, thus $T_{w_1} \cong \mathbb{Z}/p$ non-canonically as a G'_k-module.

Since we will not further need the above assertion about the structure of Z_w, we will not go into the details of the proof.

In order to conclude the proof of Theorem B, we have to show that for the given section $s' : G'_k \to G'_K$ of the canonical projection $pr' : G'_K \to G'_k$, there exists only one p-adic valuation w such that $s'(G'_k) \subseteq Z_w$. In order to do so, consider p-adic valuations w^1 and w^2 such that $s'(G'_k) \subset Z_{w^i}$, $i = 1, 2$. We claim that $w^1 = w^2$. Indeed, let w be the maximal common coarsening of w^1, w^2. By 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 prolonging the p-adic valuation of the p-adically closed field kw. Further, by Lemma 2.3, 2, it follows that $K'w$ is the maximal $\mathbb{Z}/p$ elementary abelian extension of Kw; and moreover, since $s'(G'_k) \subset Z_{w^i}$, $i = 1, 2$, it follows by general decomposition theory for valuations that $s'_w(G'_k) \subset Z_{w^i/w}$, $i = 1, 2$. On the other hand, by the construction of w, it follows that w^1/w and w^2/w are independent valuations of Kw. On the other hand, since w^1/w and w^2/w are independent, it follows by Lemma 2.3, 2, that $Z_{w^1/w} \cap Z_{w^2/w}$ is trivial. Contradiction, as $s'_w(G'_k) \subset Z_{w^i/w}$, $i = 1, 2$.

The proof of Theorem B is complete.

4. Proof of Theorem A

Theorem A is an immediate consequence of the following:

Theorem 4.1. *Let $k|\mathbb{Q}_p$ be a finite extension containing the p^{th} roots of unity, and let $k_0 \subseteq k$ a subfield which is relatively algebraically closed in k. Let X_0 be a complete smooth curve over k_0, and $K_0 = k_0(X)$ the function field of X_0.*

1) *Every k-rational point x of X_0 gives rise to a bouquet of liftable sections $s'_x : \overline{G}'_{k_0} \to \overline{G}'_{K_0}$.*

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 of X_0 such that s' equals one of the sections s'_x mentioned above.*

Proof. Assertion 1) is clear by the discussion in Introduction. To 2): Since $k_0 \subseteq k$ is relatively algebraically closed, it follows that 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: 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. Let w' be the canonical coarsening of v. We have the possibilities:

Case 1. The valuation w' is trivial.

Then w is a discrete valuation of K prolonging v to K, and having the same residue field and the same value group as v. Equivalently, the completions $\hat{k}_0$ and $\hat{K}_0$ are equal, 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 $x_w \in X_0(k)$, etc.

Case 1. The valuation w' is not trivial.

Then w' is a k_0-rational place of K_0, and hence it defines a k_0-rational point x_0 of X_0; hence by functoriality, we get k-rational point $x \in X_0(k)$ which completely determines w', hence w, etc.

Theorem 4.1 is proved.

□

References

[Fa1] Faltings, G., *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern,* Inventiones Math. **73** (1983), 349–366

[Fa2] Faltings, G., *Curves and their fundamental groups* (following Grothendick, Tamagawa and Mochizuki), Astérisque, Vol **252** (1998), Exposé 840.

[GGA] Geometric Galois Actions I, LMS LNS Vol **242**, eds L. Schneps – P. Lochak, Cambridge Univ. Press 1998.

[G1] Grothendieck, A., *Letter to Faltings,* June 1983. See [GGA].

[G2] Grothendieck, A., *Esquisse d'un programme,* 1984. See [GGA].

[Ki] Kim, M., *The motivic fundamental group of* $\mathbb{P}\backslash\{0,1,\infty\}$ *and the theorem of Siegel,* Inventiones Math. **161** (2005), 629–656.

[Ki] Kim, M., *The unipotent Albanese map and Selmer varieties for curves.* See `www.archiv.math.NT.0510441`.

[Ko] Koenigsmann, J., *On the 'section conjecture' in anabelian geometry,* J. reine angew. Math. **588** (2005), 221–235.

[Li] Lichtenbaum, S., *Duality theorems for curves over p-adic fields,* Inventiones Math. **7** (1969), 120–136.

[Mo] Mochizuli, Sh., *Galois sections in absolute anabelian geometry,* Nagoya Mth. J. **179** (2005), 17–45.

[Na] Nakamura, H., *Galois rigidity of the étale fundamental groups of punctured projective lines,* J. reine angew. Math. **411** (1990), 205–216.

[Ne] Neukirch, J., *Kennzeichnung der p-adischen und endlichen algebraischen Zahlkörper,* Inventiones Math. **6** (1969), 269–314.

[P1] Pop, F., *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. reine angew. Math. **392** (1988), 145–175.

[P2] Pop, F., *Pro-ℓ abelian-by-central Galois theory of Zariski prime divisors,* Manuscript, Philadelphia 2006. See: `www.math.upenn.edu/~pop/Research/Papers.html`.

[P–R] Prestel, A. and Roquette, P., Formally p-adic fields, LNM 1050, Springer Verlag 1985.

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

[Sz] Szamuely, T., *Groupes de Galois de corps de type fini,* (d'après Pop), Astérisque, Vol. **294** (2004), 403–431.

[Se] Serre, J.-P., Cohomologie Galoisienne, LNM 5, Springer 1965.

[Ta] Tamagawa, A., *The Grothendieck conjecture for affine curves,* Compositio Math. **109** (1997), 135–194.

[T] Tate, J., *Cohomology of abelian varieties over p-adic fields,* Notes by Serge Lang, Princeton University, May 1959.

Department of Mathematics
University of Pennsylvania
DRL, 209 S 33rd Street
Philadelphia, PA 19104. USA
E-mail address: `pop@math.upenn.edu`
URL: `http://math.penn.edu/~pop`