# THE PROJECTIVITY OF THE FUNDAMENTAL GROUP OF AN AFFINE LINE

by

Moshe Jarden, Tel Aviv University

Dedicated to Professor Masatoshi Ikeda
on the occasion of his 70th birthday

The Turkish Journal of Mathematics, to appear
5 February, 1998

## Introduction

Let $C$ be an algebraically closed field and let $F$ be a function field of one variable over $C$ of genus $g$. Consider a finite nonempty set $S$ of prime divisors of $F/C$. Denote the maximal Galois extension of $F$ which is ramified at most at $S$ by $F_S$. Let $r = |S|$. The Galois group $\mathcal{G}(F_S/F)$ is also the completion of the fundamental group of the affine curve which is obtained by deleting the $r$ points that correspond to the elements of $S$ from the unique smooth projective model of $F/C$.

If $\mathrm{char}(C) = 0$, then a consequence of the Riemann existence theorem asserts that $\mathcal{G}(F_S/F)$ is generated by $2g + r$ elements $\sigma_1, \ldots, \sigma_r, \tau_1, \tau_1', \ldots, \tau_g, \tau_g'$ with the unique relation $\sigma_1 \cdots \sigma_r [\tau_1, \tau_1'] \cdots [\tau_g, \tau_g'] = 1$. This implies that $\mathcal{G}(F_S/F)$ is the free profinite group on the generators $\sigma_2, \ldots, \sigma_r, \tau_1, \tau_1', \ldots, \tau_g, \tau_g'$. In particular $\mathcal{G}(F_S/F)$ is projective.

The elements $\sigma_1, \ldots, \sigma_r$ above can be selected to generate inertia groups over the elements of $S$. Let $G(F)$ be the absolute Galois group of $F$. Since $G(F) = \varprojlim \mathcal{G}(F_S/F)$, where $S$ ranges over all finite sets of prime divisors of $F/C$, and since restriction maps inertia groups onto inertia groups, $G(F)$ is the free profinite group $\hat{F}_m$ of rank $m = \mathrm{card}(C)$ [Rib, p. 70, Thm. 8.1 for $C = \mathbb{C}$ or Ja1, §1.8]. In particular, $G(F)$ is a projective group.

It turns out that the conclusion $G(F) \cong \hat{F}_m$, with $m = \mathrm{card}(C)$, is true also for arbitrary characteristic. There are three methods to prove this result. The first one which is due to Harbater [Har] uses formal patching. The second one of Pop [Pop] applies analytic geometry. The third one, which Haran and Völklein introduce in [HaV] uses the elementary method of "field patching". However, [HaV] treats only the case where $C$ is countable. The general case along this line is treated in [Ja2].

Whereas the projectivity of $G(F)$ in the case $\mathrm{char}(C) = 0$ is a consequence of the complex analytic methods which are inherited in the proof of Riemann existence theorem, it is the starting point in each of the three proofs that the preceding paragraph mentions.

In §1 we present a proof of the projectivity of $G(F)$ which strives to be as elementary as possible. In particular, it replaces heavier use of Galois cohomology by more basic results in that theory.

The projectivity of $G(F)$ is also the starting point for the proof of the projectivity of $\mathcal{G}(F_S/F)$ ($S$ is, as above, a finite nonempty set of prime divisors of $F/C$), which we prove in §2. Serre [Ser, Prop. 1] proves the projectivity of $\mathcal{G}(F_S/F)$ by etale cohomology. Matzat and Malle [MaM, Chap. V, Thm. 5.3] use Grothendieck lifting to characteristic 0 and then rely on the result obtained by complex analytic methods.

Section 2 of this work suggests an elementary proof for the projectivity of $\mathcal{G}(F_S/F)$. In order to get a weak solution for a finite embedding problem for $\mathcal{G}(F_S/F)$ we first solve it for $G(F)$. Then we modify the solution to decompose through $\mathcal{G}(F_S/F)$. This method goes back to Reichardt-Scholz, Schafarevich, and Sonn.

Unfortunately, we do not know how to prove that $\mathcal{G}(F_S/F)$ is free by elementary methods if $\mathrm{char}(C) = 0$. We do prove however in §3, as [MaM, §V5.1] does, that $\mathcal{G}(F_S/F)$ is not free if $\mathrm{char}(C) \neq 0$. Again, unlike in [MaM], we use only algebraic methods in the proof.

Acknowledgement: The writing of this work benefited from discussions with Sigrid Böge, Dan Haran, Wulf-Dieter Geyer, Heinrich Matzat, and Aharon Razon.

## 1. **The projectivity of $G(C(x))$**

Let $C$ be an algebraically closed field and let $x$ be a transcendental element over $C$. Denote the absolute Galois group of $C(x)$ by $G(C(x))$. Recall that a profinite group $G$ is **projective** if for each epimorphism $\varphi\colon G \to A$ and each epimorphism $\alpha\colon B \to A$ of profinite groups, there exists a homomorphism $\gamma\colon G \to B$ such that $\alpha \circ \gamma = \varphi$ [FrJ, Chap. 20]. Alternatively, the cohomological dimesnion of $G$ is at most 1. It is well know that $G(C(x))$ is a projective group. This fact is sometimes referred to as "a theorem of Tsen". However, a careful analysis shows that Tsen's contribution is only one ingredient of the proof. We put here all the ingredients of the proof together and try to simplify each step as much as possible.

Theorem 1.1: *Let $F$ be a function field of one variable over an algebraically closed field $C$. Then $G(F)$ is a projective group.*

*Proof:* The proof divides into eight parts.

Part A: *Let $f_i(X_0,\ldots,X_d)$, $i=1,\ldots,d$, be forms with coefficients in $C$. Then there exist $x_0,\ldots,x_d \in C$ not all 0, such that $f_i(\mathbf{x}) = 0$, $i=1,\ldots,d$.* [La2, p. 43].

From now on $K$ will denote an algebraic extension of $C(x)$ which will be eventually more specified.

Part B: *$K$ is a $C_1$-field.* That is, each form of degree $d$ over $K$ with $d+1$ variables has a nontrivial zero. This is Tsen's theorem from 1933 [Lor, p. 151]. The proof of this part relies on Part A.

Part C: *Let $L$ be a finite Galois extension of $K$. Then $\mathrm{Norm}_{L/K} L^\times = K^\times$.*

Indeed, let $w_1,\ldots,w_d$ be a basis of $L/K$ and let $G = \mathcal{G}(L/K)$. Then

$$f(X_1,\ldots,X_d) = \prod_{\sigma\in G} (X_1 w_1^\sigma + \cdots + X_d w_d^\sigma)$$

is a form of degree $d$ with coefficients in $K$. If $x_1,\ldots,x_d \in K$ and $f(x_1,\ldots,x_d) = 0$, then there exists $\sigma \in G$ such that $x_1 w_1^\sigma + \cdots + x_d w_d^\sigma = 0$. Since $w_1^\sigma,\ldots,w_d^\sigma$ also form a basis over $K$, we have $x_1 = \cdots = x_d = 0$.

Let now $a \in K^\times$. By Part B, there exist $y_0, y_1, \ldots, y_d \in K$, not all 0, such that $f(y_1, \ldots, y_d) = y_0^d a$. By the preceding paragraph, $y_0 \neq 0$. Hence, with $x_i = y_i/y_0$, $i = 1, \ldots, d$, and $b = x_1 w_1 + \cdots + x_d w_d$ we have $\mathrm{Norm}_{L/K} b = a$.

Part D: *Let $L$ be a cyclic extension of $K$. Then every short exact sequence*

$$\begin{tikzcd} 1 \arrow[r] & L^\times \arrow[r] & E \arrow[r, "h"] & \mathcal{G}(L/K) \arrow[r] & 1 \end{tikzcd}$$

*for which the action of $\mathcal{G}(L/K)$ on $L^\times$ is the Galois action splits.*

Let $n = [L : K]$ and let $\sigma$ be a generator of $\mathcal{G}(L/K)$. We have to find $\varepsilon \in E$ such that $h(\varepsilon) = \sigma$ and $\varepsilon^n = 1$.

We begin with any $\varepsilon \in E$ such that $h(\varepsilon) = \sigma$. By assumption, for each $y \in L^\times$, we have $y^\varepsilon = \varepsilon^{-1} y \varepsilon = y^\sigma$. Also, $\varepsilon^n \in L^\times$. Hence, $(\varepsilon^n)^\sigma = (\varepsilon^n)^\varepsilon = \varepsilon^n$, and therefore $\varepsilon^n \in K^\times$.

By Part C, there exists $x \in L^\times$ such that $\mathrm{Norm}_{L/K} x = \varepsilon^n$. For arbitrary elements $x, \varepsilon$ of a group $G$, one proves by induction on $n$ that

$$(x\varepsilon)^n = \varepsilon^n x^{\varepsilon^n} x^{\varepsilon^{n-1}} \cdots x^\varepsilon.$$

In our case, for $x^{-1}$ instead of $x$, this formula gives

$$(x^{-1}\varepsilon)^n = \varepsilon^n x^{-\varepsilon^n} x^{-\varepsilon^{n-1}} \cdots x^{-\varepsilon} = \varepsilon^n x^{-\sigma^n} x^{-\sigma^{n-1}} \cdots x^{-\sigma} = \varepsilon^n \mathrm{Norm}_{L/K} x^{-1} = 1.$$

So, $x^{-1}\varepsilon$ is the desired element of $E$.

Part E*: *Let $E$ be a $p$-Sylow subfield of $C(x)_s$ (i.e., $E$ is the fixed field in $C(x)_s$ of a $p$-Sylow subgroup of $G(C(x))$.). Then $H^2(G(E), E_s^\times) = 1$.* Indeed, by [Rib, p. 114], $H^2(G(E), E_s^\times) = \varinjlim H^2(\mathcal{G}(N/E), N^\times)$, where $N$ ranges over all finite Galois extensions of $E$ and the maps involved in the direct limit are inflations. We prove by induction

* The standard argument at this point uses a special case of cohomological triviality: Let $G$ be a finite group and let $A$ be a $G$-module. If $\hat{H}^0(G, A) = A^G/NA = 0$ (where $Na = \Sigma_{\sigma \in G} \sigma a$) and $H^1(G, A) = 0$, then $H^2(G, A) = 0$ [CaF, p. 113, Thm. 9]. In our case, $G = \mathcal{G}(N/K)$, $A = N^\times$ and $A^G/NA = K^\times/\mathrm{Norm}_{N/K} N^\times = 1$, by Part C. Also, $H^1(G, N^\times) = 1$, by Hilbert's theorem 90. So, indeed, $H^2(G, A) = 1$. We are indebted to Sigrid Böge for her help to replace cohomological triviality by the more elementary argument of Part E.

on the degree, that for each finite Galois extension $N/K$ with $E \subseteq K \subseteq N \subseteq C(x)_s$ we have $H^2(\mathcal{G}(N/K), N^\times) = 1$.

Indeed, $N/K$ is a $p$-extension. Hence, if it is not trivial, it has a cyclic subextension $L/K$ of degree $p$. By Part D, $H^2(\mathcal{G}(L/K), L^\times) = 1$. By induction, $H^2(\mathcal{G}(N/L), N^\times) = 1$. Finally use the exactness of the inflation restriction sequence

$$\begin{tikzcd} H^2(\mathcal{G}(L/K), L^\times) \arrow[r, "\mathrm{inf}"] & H^2(\mathcal{G}(N/K), N^\times) \arrow[r, "\mathrm{res}"] & H^2(\mathcal{G}(N/L), N^\times) \end{tikzcd}$$

[CaF, p. 125] to conclude that $H^2(\mathcal{G}(N/K), N^\times) = 1$.

PART F: *Let $E$ be a $p$-Sylow subfield of $C(x)_s$. Then, $G(E)$ is projective; hence $p$-free.* The statement holds for $p = \mathrm{char}(E)$ by [Rib, 256]. So, assume that $p \neq \mathrm{char}(E)$.

By [Rib, p. 211 and p. 218], we have to prove that $H^2(G(E), \mathbb{Z}/p\mathbb{Z}) = 0$. To this end consider the short exact sequence

(1) $$\begin{tikzcd} 1 \arrow[r] & \mu_p \arrow[r] & E_s^\times \arrow[r, "p"] & E_s^\times \arrow[r] & 1, \end{tikzcd}$$

where $\mu_p$ is the group of roots of unity of order $p$ and the map from $E_s^\times$ to $E_s^\times$ is raising to the $p$th power. Since $\mu_p \subseteq C$, the action of $G(E)$ on $\mu_p$ is trivial and therefore $\mu_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a $G(E)$-module. Consider the following segment of the long exact sequence that the exact sequence (1) gives [Rib, p. 115]:

(2) $$\begin{tikzcd} H^1(G(E), E_s^\times) \arrow[r] & H^2(G(E), \mathbb{Z}/p\mathbb{Z}) \arrow[r] & H^2(G(E), E_s^\times). \end{tikzcd}$$

The left term of (2) is trivial, by Hilbert's Theorem 90. The right term of (2) is trivial, by Part F. Hence, the middle term of (2) is trivial.

PART G: *$G(C(x))$ is projective.*

This follows from Part F and [FrJ, Prop. 20.47]. Note that the proof of the latter theorem is carried out without cohomology.

PART H: *Conclusion of the proof.* By [FrJ, Cor. 20.14], each closed subgroup of a projective group is projective. Conclude from Part G that $G(F)$ is projective. ∎

PROBLEM 1.2: *Eliminate cohomology from the proof.*

## 2. The projectivity of the fundamental group of a smooth affine curve

Let $\Gamma$ be a smooth curve of genus $g$ over an algebraically closed field $C$ and let $F$ be the function field of $\Gamma$. Then $\Gamma$ corresponds to the set of all prime divisors of $F$ minus a finite subset $S$ of, say, $r$ elements. Let $F_S$ be the maximal separable algebraic extension of $F$ which is unramified outside $S$. The Galois group $G_S = \mathcal{G}(F_S/F)$ is then the **fundamental group** $\Pi_1(\Gamma)$ of $\Gamma$ (actually the completion thereof). If $C = \mathbb{C}$, then by the Riemann existence theorem $G_S$ is presented by $r + 2g$ generators

$$\sigma_1, \ldots, \sigma_r, \tau_1, \tau_1', \ldots, \tau_g, \tau_g' \tag{1}$$

and a single relation

$$\sigma_1 \cdots \sigma_r [\tau_1, \tau_1'] \cdots [\tau_g, \tau_g'] = 1. \tag{2}$$

Douady [Dou] extends this theorem to an arbitrary algebraically closed field $C$ of characteristic 0 (see also [Ja1, §1.8]). If however, $\mathrm{char}(C) > 0$, then the structure of $G_S$ is unknown.

If $r \geq 1$, then each map of $\sigma_2, \ldots, \sigma_r, \tau_1, \tau_1', \ldots, \tau_g, \tau_g'$ into a profinite group $\bar{G}$ extends to a homomorphism of $G$ into $\bar{G}$. Hence, $G_S$ is free on $r - 1 + 2g$ generators. In particular, $G_S$ is projective.

The only known proof of Riemann existence theorem uses methods from complex analysis and functional analysis. The aim of this section is to prove that $G_S$ is projective, without any restriction on the characteristic, by algebraic means*. This will in particular reprove the projectivity of $G_S$ in characteristic 0.

In Part G of the proof of Theorem 1.1 we have used that a profinite group $G$ is projective if and only if for each prime $p$ each $p$-Sylow subgroup $G_p$ of $G$ is projective [FrJ, Prop. 20.37 and Prop. 20.47]. We therefore say that $G$ is ***p*-projective** if $G_p$ is projective.

Lemma 2.1: *Let $p$ be a prime number.*

* The proof is based on tips of Heinrich Matzat.

(a) *Let $G$ be a profinite group. Suppose that for every open subgroup $H$ of $G$, each finite central non-split $p$-embedding problem*

$$\begin{tikzcd} & & & H \arrow[d, "\varphi"] & \\ 0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & B \arrow[r, "\alpha"] & A \arrow[r] & 1 \end{tikzcd}$$

*is solvable. Then $G$ is $p$-projective.*

(b) *Let $N/F$ be a Galois extension. Suppose that for each finite subextension $K$ of $N/F$, for each finite Galois subextension $L/K$ of $N/K$, and every non-split central exact sequence of $p$-groups*

(3)
$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & B \arrow[r, "\alpha"] & \mathcal{G}(L/K) \arrow[r] & 1, \end{tikzcd}$$

*there exists a Galois extension $\hat{L}$ of $K$ which contains $L$ and which is contained in $N$ and there exists an isomorphism $\gamma$: $\mathcal{G}(\hat{L}/K) \to B$ such that $\alpha \circ \gamma = \mathrm{res}_L$ (we say that $\hat{L}$* **solves** *the embedding problem (3).) Then $\mathcal{G}(N/F)$ is $p$-projective.*

*Proof:* Statement (b) is a reinterpretation of (a) for Galois groups. So we prove (a).

Let $G_p$ be a $p$-Sylow subgroup of $G$. It order to prove that $G_p$ is projective, it suffices to prove that each finite central $p$-embedding problem

(4)
$$\begin{tikzcd} & & & G_p \arrow[d, "\varphi_p"] & \\ 0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & B \arrow[r, "\alpha"] & A \arrow[r] & 1 \end{tikzcd}$$

is **weakly solvable**, i.e., there exists a homomorphism $\gamma$: $G_p \to B$ such that $\alpha \circ \gamma = \varphi_p$ [Rib, p. 211, Prop. 3.1 and p. 218, Proposition 4.1]. If $\alpha$ has a section $\alpha'$: $A \to B$, then $\gamma = \alpha' \circ \varphi_p$ is a weak solution of (4). Suppose therefore that (4) does not split.

Choose an open normal subgroup $N$ of $G$ such that $G_p \cap N \leq \mathrm{Ker}(\varphi_p)$. Let $H = G_pN$. Then $H$ is an open subgroup of $G$ which contains $G_p$ and $\varphi_p$ extends to a homomorphism $\varphi$: $H \to A$. By assumption, there exists a homomorphism $\gamma$: $H \to B$ such that $\alpha \circ \gamma = \varphi$. The restriction of $\gamma$ to $G_p$ weakly solves embedding problem (4).

∎

Let $\alpha_i$: $G_i \to G$, $i = 1, 2$, be homomorphisms of profinite groups. Then $G_1 \times_G G_2 = \{(x_1, x_2) \in G_1 \times G_2 \mid \alpha_1(x_1) = \alpha_2(x_2)\}$ is the **fibre product** of $G_1$ and $G_2$ over $G$. It is characterized by the following property: For each pair $\beta_i$: $H \to G_i$, $i = 1, 2$, of homomorphisms such that $\alpha_1 \circ \beta_1 = \alpha_2 \circ \beta_2$ there exists a unique homomorphism $\beta$: $H \to G_1 \times_G G_2$ such that $\pi_i \circ \beta = \beta_i$, where $\pi_i$ is the projection on the $i$th coordinate, $i = 1, 2$ [FrJ, §20.2].

Recall that an epimorphism $\alpha$: $B \to A$ of profinite groups is **Frattini** if it maps no proper closed subgroup of $B$ onto $A$ [FrJ, §20.6]. For example, a short exact sequence $0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \tilde{G} \xrightarrow{\alpha} A \longrightarrow 1$ does not split if and only if $\alpha$ is Frattini.

Lemma 2.2 (After [Son, Lemma 2.6]): *Consider exact sequences of finite groups,*

$$1 \longrightarrow H_i \longrightarrow G_i \xrightarrow{\alpha_i} G \longrightarrow 1, \qquad i = 1, 2,$$

*such that $|H_1| = |H_2|$ and $\alpha_1$ is Frattini. Then there exists an isomorphism $\varphi$: $G_2 \to G_1$ such that $\alpha_1 \circ \varphi = \alpha_2$ if and only if the projection map $\pi_2$: $G_1 \times_G G_2 \to G_2$ has a section.*

*Proof:* Suppose first that $\varphi$: $G_2 \to G_1$ is an isomorphism such that $\alpha_1 \circ \varphi = \alpha_2$. Then there is a homomorphism $\pi_2'$: $G_2 \to G_1 \times_G G_2$ such that $\pi_2 \circ \pi_2' = \mathrm{id}$.

Conversely, suppose that $\pi_2'$ as above exists. Let $\pi_1$: $G_1 \times_G G_2 \to G_1$ be the projection on the first factor. Then $\varphi = \pi_1 \circ \pi_2'$ is a homomorphism from $G_2$ to $G_1$ such that $\alpha_1 \circ \varphi = \alpha_2$. In particular, $\alpha_1(\varphi(G_2)) = G$. Since $\alpha_1$ is Frattini, $\varphi(G_2) = G_1$. Since $|G_1| = |G_2|$, this implies that $\varphi$ is an isomorphism. ∎

Lemma 2.3 ([Sha, p. 109 or Son, Prop. 2.5]): *Let $p$ be a prime number and let $L/K$ be a finite Galois extension with $p \neq \mathrm{char}(K)$. Suppose that $K$ contains a $p$th primitive root $\zeta$ of 1. Suppose also that (3) is a non-split* central embedding problem. Let $L(x^{1/p})$ with $x \in L^\times$ be a solution field of (3). Then,*

(a) *for each $\sigma \in G(K)$ there is $u \in L^\times$ such that $\sigma x = xu^p$, and*

(b) *the set of solution fields coincides with the set of fields $L((ax)^{1/p})$, $a \in K^\times$.*

*Proof of (a):* Consider first $\sigma \in G(K)$. Then $L((\sigma x)^{1/p}) = L(x^{1/p})$ and therefore, by Kummer theory, there exist $u \in L^\times$ and $0 \leq i < p$ such that $\sigma x = x^i u^p$. Hence,

* If (3) splits, $x \in K^\times \smallsetminus (L^\times)^p$, and $a \in x^{-1}(K^\times)^p$, then $L(x^{1/p})$ is a solution field of (3) but $L((ax)^{1/p}) = L$ is not.

$\sigma x^{1/p} = \zeta^j x^{i/p} u$ for some integer $j$. Let $\tau$ be the generator of $\mathcal{G}(L(x^{1/p})/L)$ such that $\tau x^{1/p} = \zeta x^{1/p}$. Then $\tau\sigma x^{1/p} = \tau(\zeta^j x^{i/p} u) = \zeta^j \zeta^i x^{i/p} u$ and $\sigma\tau x^{1/p} = \sigma(\zeta x^{1/p}) = \zeta\zeta^j x^{i/p} u$. Since $\mathcal{G}(L(x^{1/p})/K)$ acts trivially on $\mathcal{G}(L(x^{1/p})/L)$, we have $\sigma\tau = \tau\sigma$. It follows that $i = 1$ and therefore $\sigma x = xu^p$.

*Proof of (b):* Consider now $a \in K^\times$ and let $y = ax$. If $L(y^{1/p}) = L$, then $xa \in L^p$ and therefore $L(x^{1/p}) = L(a^{1/p})$. Hence (3) splits, in contrast to our assumption. It follows that $L(y^{1/p})/L$ is a cyclic extension of degree $p$. For each $\sigma \in G(K)$ we have, by (a), $\sigma y = axu^p = yu^p$. So, $L(y^{1/p})$ is a Galois extension of $K$. If $L(y^{1/p}) = L(x^{1/p})$, then $L(y^{1/p})$ is certainly a solution field of (3).

So, suppose that $L(y^{1/p}) \neq L(x^{1/p})$. Then $a^{1/p} \notin L(y^{1/p})$. Let $N = L(x^{1/p}, y^{1/p})$. Then $\mathcal{G}(N/K) = \mathcal{G}(L(x^{1/p})/K) \times_{\mathcal{G}(L/K)} \mathcal{G}(L(y^{1/p})/K)$ and the restriction maps to $L(x^{1/p})$ and $L(y^{1/p})$ are the projections on the groups $\mathcal{G}(L(x^{1/p})/K)$ and $\mathcal{G}(L(y^{1/p})/K)$, respectively. Moreover, $N = L(y^{1/p}, a^{1/p})$ and therefore the map res: $\mathcal{G}(N/K) \to \mathcal{G}(L(y^{1/p})/K)$ has a section. Since (3) does not split, res: $\mathcal{G}(L(x^{1/p})/K) \to \mathcal{G}(L/K)$ is Frattini. By Lemma 2.2

(5) there exists an isomorphism $\varphi$: $\mathcal{G}(L(y^{1/p})/K) \to \mathcal{G}(L(x^{1/p})/K)$ which commutes with the restriction to $L$.

It follows that $L(y^{1/p})$ is a solution field of (3).

Conversely, suppose that $\hat{L}$ is another solution of (3). Then, (5) holds, for $\hat{L}$ instead of $L(y^{1/p})$. Let $N = \hat{L}(x^{1/p})$. By Lemma 2.2, res: $\mathcal{G}(N/K) \to \mathcal{G}(\hat{L}/K)$ has a section. Since (3) is a central extension, this means in field theoretic terms that $K$ has a cyclic extension $K(b^{1/p})$ of degree $p$ with $b \in K^\times$ such that $\hat{L} \cap K(b^{1/p}) = K$ and $\hat{L}(b^{1/p}) = N$.

As $\hat{L}(x^{1/p}) = \hat{L}(b^{1/p})$, Kummer theory gives $z \in \hat{L}$ and an integer $k$ such that $x = z^p b^k$. So, with $a = b^{-k}$, we have $z^p = ax \in L$. If $z \in L$, then $L(x^{1/p}) = L(b^{1/p})$ and therefore (3) splits, in contrast to our assumption. Conclude that $\hat{L} = L(z) = L((ax)^{1/p})$, as claimed. ∎

Let $v$ be a discrete valuation of a field $L$ and let $p$ be a prime number which is not the characteristic of the residue field of $L$ at $v$ (e.g., $L$ is a function field over $C$,

$p \neq \mathrm{char}(C)$, and $v$ is trivial on $C$). Consider $x \in L \smallsetminus L^p$. Extend $v$ to $L(x^{1/p})$. Then $pv(x^{1/p}) = v(x)$. Hence, if $p \nmid v(x)$, then $v$ ramifies in $L(x^{1/p})$. If $v(x) = pk$ and $t$ is an element in $L$ such that $v(t) = 1$, then with $y = t^{-kp}x$, we have $L(x^{1/p}) = L(y^{1/p})$ and $v(y) = 0$. The reduction of $X^p - y$ at $v$ decomposes into $p$ distinct linear factors (in the algebraic closure of the residue field). Hence, $v$ is unramified in $L(x^{1/p})$.

If $K$ is a function field over $C$, we denote the set of divisors (resp., prime divisors) of $K$ over $C$ by $\mathrm{Div}(K)$ (resp., $\mathrm{PrimDiv}(K)$).

The proof of the next lemma is a modification of the proof of [Son, Prop. 3.2].

Lemma 2.4: *Let $K$ be a function field of one variable over an algebraically closed field $C$. Let $S$ be a finite nonempty set of prime divisors of $K/C$. Let $p \neq \mathrm{char}(K)$ be a prime number and let $L/K$ be a finite Galois subextension of $K_S/K$. Suppose that the central non-split $p$-embedding problem (3) has a solution. Then (3) has a solution field $\hat{L}$ which is contained in $K_S$.*

*Proof:* Let $L(x^{1/p})$ be a solution field of (3). By Lemma 2.3, it suffices to find $a \in K^\times$ such that $L((ax)^{1/p}) \subseteq K_S$.

To this end, let $\mathrm{div}(x) = \sum v_{\mathfrak{P}}(x)\mathfrak{P}$ be a presentation of the principal divisor of $x$ as a sum of distinct $\mathfrak{P} \in \mathrm{PrimDiv}(L)$ with coefficients $v_{\mathfrak{P}}(x)$ (where $v_{\mathfrak{P}}$ is the normalized valuation of $L$ associated with $\mathfrak{P}$). By Lemma 2.3(a), for each $\sigma \in \mathcal{G}(L/K)$ there is $u \in L^\times$ such that $\sigma x = xu^p$. Hence,

$$v_{\mathfrak{P}}(x) \equiv v_{\mathfrak{P}}(\sigma^{-1}x) \equiv v_{\sigma\mathfrak{P}}(x) \mod p.$$

The set of prime divisors in $L$ of each prime divisor $\mathfrak{p}$ of $K$ is a conjugacy class (under the action of $\mathcal{G}(L/K)$). Thus, $\mathrm{div}(x) \equiv \sum_{\mathfrak{p}} n_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P} \mod p\mathrm{Div}(L)$, where $\mathfrak{p}$ ranges over the prime divisors of $K/C$ and $n_{\mathfrak{p}} = v_{\mathfrak{P}}(x)$ is independent of $\mathfrak{P}|\mathfrak{p}$.

If $\mathfrak{p} \notin S$, then $\mathfrak{p}$ is unramified in $L$ and therefore $\mathfrak{p} = \sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}$. It follows that

$$\mathrm{div}(x) = \sum_{\mathfrak{p}\notin S} n_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P} + \sum_{\mathfrak{p}\in S} n_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P} \equiv \mathfrak{a} + \mathfrak{B} \mod p\mathrm{Div}(L),$$

where $\mathfrak{a} \in \mathrm{Div}(K)$ and $\mathfrak{B}$ is a divisor of $L$ which involves only primes over $S$.

Let $\Delta$ be the smooth projective curve over $C$ with function field $K$ and let $J$ be its Jacobian variety. Denote the group of divisors of $K$ of degree 0 by $\mathrm{Div}_0(K)$. There is an epimorphism of $\mathrm{Div}_0(K)$ onto $J(C)$ whose kernel is the group of principal divisors of $K$ [La3, §II.2]. Now choose $\mathfrak{p}_0 \in S$. Since $C$ is algebraically closed, $\deg(\mathfrak{p}_0) = 1$ and therefore $\mathfrak{a} - \deg(\mathfrak{a})\mathfrak{p}_0 \in \mathrm{Div}_0(K)$. Also, $J(C)$ is $p$-divisible [Mum, p. 42]. Hence, there exists $a \in K^\times$ such that $(a) + \mathfrak{a} - \deg(\mathfrak{a})\mathfrak{p}_0 \equiv 0 \mod p\mathrm{Div}(K)$. It follows that $\mathrm{div}(ax) \equiv \deg(\mathfrak{a})\mathfrak{p}_0 + \mathfrak{B} \mod p\mathrm{Div}(L)$. This implies that $v_{\mathfrak{P}}(ax) \equiv 0 \mod p$ for each $\mathfrak{P}$ which does not lie over $S$. Such $\mathfrak{P}$ is unramified in $L((ax)^{1/p})$. Conclude that $L((ax)^{1/p}) \subseteq K_S$. ∎

In order to prove Lemma 2.4 also for $p = \mathrm{char}(C)$ we have to replace Kummer theory in the above arguments by Artin-Schreier theory. We consider the additive operator $\wp$ defined on a field $K$ of characteristic $p > 0$ by $\wp(x) = x^p - x$. For each $x \in K$ we choose $x' \in K_s$ such that $\wp(x') = x$. Then $x', x'+1, \ldots, x'+p-1$ are the $p$ distinct solutions of the equation $\wp(X) = x$. If $x \notin \wp(K)$, then the latter equation is irreducible and $K(x')/K$ is a cyclic extension of degree $p$ and $\mathcal{G}(K(x')/K)$ is generated by an element $\tau$ such that $\tau(x') = x' + 1$. Conversely, if $L/K$ is a cyclic extension of degree $p$, then $L = K(x')$ with $x = \wp(x') \in K$ [La1, p. 215]. Note that the map $x \mapsto x'$ is completely analogous to the map $x \mapsto x^{1/p}$ that we use for $\mathrm{char}(K) \neq p$.

For each subgroup $A$ of the additive group of $K$ we have $[K(\wp^{-1}(A)) : K] = [A + \wp(K) : \wp(K)]$ [La1, p. 221]. This gives the following rules for $x, y, z \in K$:

(6a) $K(x') = K$ if and only if $x \in \wp(K)$.

(6b) $K(x') = K(y')$ if and only if there exist $k, l \in \mathbb{Z}$ not both divisible by $p$ such that $kx + ly \equiv 0 \mod \wp(K)$.

(6c) $x' \in K(y', z')$ if and only if there exist $k, l \in \mathbb{Z}$ such that $x \equiv ky + lz \mod \wp(K)$.

Lemma 2.5: *Consider a non-split central embedding problem*

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow B \xrightarrow{\alpha} \mathcal{G}(L/K) \longrightarrow 1 \tag{7}$$

*where $L/K$ is a finite Galois extension of characteristic $p$. Suppose that $L(x')$ is a solution field of (7) for some $x \in L$. Then $\hat{L}$ is a solution field of (7) if and only if $\hat{L} = L((x+a)')$ for some $a \in K$.*

*Proof:* Consider first $\sigma \in \mathcal{G}(L(x')/K)$. Since $\wp(\sigma x') = \sigma\wp(x') = \sigma x$, we have $L((\sigma x)') = L(\sigma x') = L(x')$. Hence, by (6) there exist $b \in L$ and an integer $1 \le l < p$ such that $\sigma x' = lx' + b$. Let $\tau$ be the element of $\mathcal{G}(L(x')/L)$ such that $\tau x' = x' + 1$. Then $\sigma\tau x' = \sigma x' + 1 = lx' + b + 1$ and $\tau\sigma x' = \tau(lx' + b) = lx' + l + b$. Since $\mathcal{G}(L(x')/K)$ acts trivially on $\mathcal{G}(L(x')/L)$, $\sigma\tau = \tau\sigma$. It follows that $l = 1$ and therefore $\sigma x' = x' + b$.

Let now $y = x + a$ with $a \in K$. If $L(y') = L$, then $x + a \in \wp(L)$ and therefore $L(x') = L(a')$. Hence, (7) splits, in contrast to our assumption. It follows that $L(y')/L$ is a cyclic extension of degree $p$.

Let $\sigma \in G(K)$. By the preceding paragraph, $\sigma x = x + \wp(b)$ and therefore $\sigma y \equiv y \mod \wp(L)$. Hence, by (6), $L(y')$ is a Galois extension of $K$. If $L(y') = L(x')$, then $L(y')$ is certainly a solution field of (7).

So, suppose that $L(y') \ne L(x')$. Then $a' \notin L(y')$. Let $N = L(x', y')$. Then $\mathcal{G}(N/K) = \mathcal{G}(L(x')/K) \times_{\mathcal{G}(L/K)} \mathcal{G}(L(y')/K)$ and the restriction maps to $L(x')$ and $L(y')$ are the projections on the groups $\mathcal{G}(L(x')/K)$ and $\mathcal{G}(L(y')/K)$, respectively. Moreover, $N = L(y', a')$ and therefore the map res: $\mathcal{G}(N/K) \to \mathcal{G}(L(y')/K)$ has a section. Since (7) does not split, res: $\mathcal{G}(L(x')/K) \to \mathcal{G}(L/K)$ is Frattini. By Lemma 2.2

(8) there exists an isomorphism $\varphi$: $\mathcal{G}(L(y')/K) \to \mathcal{G}(L(x')/K)$ which commutes with the restriction to $L$.

It follows that $L(y')$ is a solution field of (7).

Conversely, suppose that $\hat{L}$ is another solution field of (7). In particular, $\hat{L}$ is a cyclic extension of degree $p$ of $L$. Hence $\hat{L} = L(y_0')$ with $y_0 = \wp(y_0') \in L$. Also, (8) holds for $\hat{L}$ instead of $L(y')$. Hence, with $N = L(x', y_0')$, res: $\mathcal{G}(N/K) \to \mathcal{G}(\hat{L}/K)$ has a solution (Lemma 2.2). This implies that $N = L(y_0', a_0')$ with $a_0 = \wp(a_0') \in K$. Since $x' \in L(y_0', a_0')$ and $L(y_0') \ne L(x')$, there exist $k, l \in \mathbb{Z}$ with $p \nmid k$ and $b \in L$ such that $ky_0 + la_0 = x + \wp(b)$. So, with $y = ky_0 - \wp(b)$ and $a = -la_0$, we have $y = x + a$ and $\hat{L} = L(y')$, as required. ∎

Let $v$ be a discrete valuation of a field $L$ of characteristic $p$ and let $x \in L$. If $v(x) \ge 0$, then $x'$ is a root of the polynomial $f(X) = X^p - X - x$ with coefficients in the valuation ring of $v$. The reduction of $f$ at $v$ has $p$ distinct roots. Conclude that $v$ is unramified in $L(x')$.

The proof of Lemma 2.6 is a variant of part of the proof of [MaM, Thm. 5.2].

LEMMA 2.6: *Let $K$ be a function field of one variable over an algebraically closed field $C$ of characteristic $p > 0$. Let $S$ be a finite nonempty set of prime divisors of $K/C$. Let $L$ be a finite Galois subextension of $K_S/K$. Suppose that the central non-split $p$-embedding problem (7) has a solution. Then (7) has a solution field $\hat{L}$ which is contained in $K_S$.*

*Proof:* By assumption there exists $x \in L$ such that $L(x')$ solves (7). Denote the set of all $\mathfrak{p} \in \mathrm{PrimDiv}(K) \smallsetminus S$ which have an extension $\mathfrak{P}$ to $L$ such that $v_{\mathfrak{P}}(x) < 0$ by $T$. Then $T$ is a finite set. Extend each $\mathfrak{p} \in \mathrm{PrimDiv}(K) \smallsetminus S$ to a $\mathfrak{P} = \mathfrak{P}_{\mathfrak{p}} \in \mathrm{PrimDiv}(L)$. Since $C$ is algebraically closed, it is the residue field of both $L$ at $\mathfrak{P}$ and of $K$ at $\mathfrak{p}$. Since in addition $\mathfrak{P}/\mathfrak{p}$ is unramified, $K$ is $\mathfrak{P}$-dense in $L$. We may therefore choose $a_{\mathfrak{p}} \in K$ such that

$$v_{\mathfrak{P}}(x - a_{\mathfrak{p}}) \geq 0. \tag{9}$$

Since $S$ is nonempty, the strong approximation theorem [FrJ, Prop. 2.11] gives $a \in K$ such that

$$\begin{aligned} &v_{\mathfrak{p}}(a - a_{\mathfrak{p}}) \geq 0 \text{ if } \mathfrak{p} \in T \smallsetminus S \\ &v_{\mathfrak{p}}(a) \geq 0 \text{ if } \mathfrak{p} \in \mathrm{PrimDiv}(K) \smallsetminus (T \cup S). \end{aligned} \tag{10}$$

Let $y = x - a$. By Lemma 2.5, $L(y')$ is a Galois extension of $K$ which solves (7).

In order to prove that $L(y') \subseteq K_S$ consider $\mathfrak{p} \in \mathrm{PrimDiv}(K) \smallsetminus S$. Let $\mathfrak{P} = \mathfrak{P}_{\mathfrak{p}}$. By (9) and (10), $v_{\mathfrak{P}}(y) \geq 0$. Hence, $\mathfrak{P}$ is unramified in $L(y')$. Since $L(y')$ is Galois over $K$, $\mathfrak{p}$ is unramified in $L(y')$, as desired. ∎

Combine Theorem 1.1, Lemmas 2.4 and 2.6 with Lemma 2.1(b):

THEOREM 2.7: *Let $F$ be a function field of one variable over an algebraically closed field $C$. Let $S$ be a finite nonempty subset of* $\mathrm{PrimDiv}(F)$. *Then $\mathcal{G}(F_S/F)$ is projective.*

*Proof:* We have to prove that $\mathcal{G}(F_S/F)$ is $p$-projective for each prime number $p$. By Lemma 2.1(b) for $F_S$ instead of $N$, it suffices to prove that each embedding problem (3) has a solution field $\hat{L}$ in $F_S$. Since $G(F)$ is projective (Theorem 1.1), there exists a

Galois extgension $\hat{L}$ of $K$ which contains $L$ and there exists embedding $\gamma\colon \mathcal{G}(\hat{L}/K) \to B$ such that $\alpha \circ \gamma = \mathrm{res}_L$. If $p \neq \mathrm{char}(F)$, Lemma 2.4 proves that it is possible to modify $\hat{L}$ to a solution of (3) which is contained in $F_S$. Lemma 2.6 does the same for $p = \mathrm{char}(F)$. Conclude that $\mathcal{G}(F_S/F)$ is projective. ∎

## 3. The non-freeness of the fundamental group of a smooth affine curve

Let $F$ be a function field of one variable over an algebraically closed field $C$. Let $S$ be a finite nonempty set of prime divisors of $F/C$. In the beginning of §2, we have mentioned that if $\mathrm{char}(C) = 0$, then $\mathcal{G}(F_S/F)$ is a free profinite group on $2\,\mathrm{genus}(F) + |S| - 1$ generators. Theorem 2.7 states that for arbitrary characteristic, $\mathcal{G}(F_S/F)$ is projective. By [Har, Pop, or HaV], the absolute Galois group $G(F)$ of $F$ is free. So, one may be tempted to think that $\mathcal{G}(F_S/F)$ is also free. Our main result in this section proves that this is not the case in positive characteristic.

To this end we denote the maximal $p$-extension (resp., elementary abelian $p$-extension) of $F$ which is unramified outside $S$ by $F_S^{(p)}$ (resp., $F_S^{(p,\mathrm{elem})}$).

Theorem 3.1: *Let $F$ and $S$ be as in Theorem 2.7. Suppose that* $\mathrm{char}(C) \neq 0$. *Then $\mathcal{G}(F_S/F)$ is not a free profinite group.*

*Proof:* Let $g = \mathrm{genus}(F)$. For each prime number $p$, $\mathcal{G}(F_S^{(p)}/F)$ is the maximal pro-$p$-quotient of $\mathcal{G}(F_S/F)$. Since $\mathcal{G}(F_S/F)$ is projective, so is $\mathcal{G}(F_S^{(p)}/F)$ [Rib, p. 255]. If $\mathcal{G}(F_S/F)$ were free, then $\mathrm{rank}(\mathcal{G}(F_S^{(p)}/F))$ would be equal to $\mathrm{rank}(\mathcal{G}(F_S/F))$. In particular, $\mathrm{rank}(\mathcal{G}(F_S^{(p)}/F))$ would be independent of $p$. However, by Proposition 3.2 below, $\mathrm{rank}(\mathcal{G}(F_S^{(p)})/F)) = 2g + |S| - 1$ if $p \neq \mathrm{char}(C)$, while, by Proposition 3.3 below, $\mathrm{rank}(\mathcal{G}(F_S^{(p)}/F)) = \infty$ if $p = \mathrm{char}(C)$. Conclude that $\mathcal{G}(F_S/F)$ is not free. ∎

Proposition 3.2: *Let $F$ be a function field of one variable over an algebraically closed field $C$. Then, for each finite set $S$ of prime divisors of $F/C$ and for each prime number $p \neq \mathrm{char}(C)$, $\mathcal{G}(F_S^{(p)}/F)$ is a finitely generated group. More precisely,*

$$\mathrm{rank}(\mathcal{G}(F_S^{(p)}/F)) = \begin{cases} 2\,\mathrm{genus}(F) & \textit{if } S = \emptyset \\ 2\,\mathrm{genus}(F) + |S| - 1 & \textit{if } S \neq \emptyset. \end{cases} \tag{1}$$

*Proof:* By [FrJ, Lemma 20.36], $\mathrm{rank}(\mathcal{G}(F_S^{(p)}/F)) = \dim_{\mathbb{F}_p} \mathcal{G}(F_S^{(p,\mathrm{elem})}/F)$. Denote the group of all divisors of $F/C$ by $\mathrm{Div}(F)$, let $\mathrm{Div}_0(F)$ be the subgroup of all divisors of degree 0, let $P(F)$ be the subgroup of all principal divisors of $F$ and let $g = \mathrm{genus}(F)$.

Case A: $S = \emptyset$. In order to prove (1) in this case, it suffices to prove that

$$\dim_{\mathbb{F}_p} \mathcal{G}(F_\emptyset^{(p,\mathrm{elem})}/F) = 2g. \tag{2}$$

Indeed*, Kummer theory sets a correspondence between the subgroups of $F^\times/(F^\times)^p$ and the $p$-elementary abelian extensions of $F$. If $U$ is a subgroup of $F^\times$, then $F(u^{1/p} \mid u \in U)$ is the extension that corresponds to $U(F^\times)^p/(F^\times)^p$. An extension $F(u^{1/p})/F$ is unramified at a prime $\mathfrak{p}$ of $F/C$ if and only if $p|v_\mathfrak{p}(u)$ (Here $v_\mathfrak{p}$ is the normalized discrete valuation attached to $\mathfrak{p}$.) It follows that $F(u^{1/p})/F$ is unramified (i.e., $F(u^{1/p}) \subseteq F_\emptyset^{(p,\mathrm{elem})}$) if and only if $p|\mathrm{div}(u)$. So, $U = \{u \in F^\times \mid p|\mathrm{div}(u)\}$ contains $(F^\times)^p$ and satisfies $U/(F^\times)^p \cong \mathcal{G}(F_\emptyset^{(p,\mathrm{elem})}/F)$.

Let $\alpha\colon U \to \mathrm{Div}_0(F)$ be the homomorphism that attaches to $u \in U$ the unique $\mathfrak{a}_u \in \mathrm{Div}_0(F)$ such that $\mathrm{div}(u) = p\mathfrak{a}_u$. Since $\alpha\big((F^\times)^p\big) = P(F)$, $\alpha$ induces an isomorphism $U/(F^\times)^p \cong (\mathrm{Div}_0(F)/P(F))_p$. Let $J$ be the Jacobian variety of $F/C$. Then $J(C)_p \cong (\mathrm{Div}_0(F)/P(F))_p$. So, $\mathcal{G}(F_\emptyset^{(p,\mathrm{elem})}/F) \cong J(C)_p \cong (\mathbb{Z}/p\mathbb{Z})^{2g}$ [Mum, p. 39], which proves (2).

Case B: $S = \{\mathfrak{p}\}$. If $u \in F^\times$ and $F(u^{1/p})/F$ is at most ramified at $\mathfrak{p}$, then $\mathrm{div}(u) = v_\mathfrak{p}(u)\mathfrak{p} + p\mathfrak{a}'$ for some $\mathfrak{a}' \in \mathrm{Div}(F)$. Since $\deg(\mathrm{div}(u)) = 0$, we have $p|v_\mathfrak{p}(u)$. Hence, $F(u^{1/p})/F$ is unramified. By (2), $\dim_{\mathbb{F}_p} \mathcal{G}(F_{\{\mathfrak{p}\}}^{(p,\mathrm{elem})}/F) = \dim_{\mathbb{F}_p} \mathcal{G}(F_\emptyset^{(p,\mathrm{elem})}/F) = 2g$.

Case C: *$S$ contains at least two elements.* By induction assume that (1) holds for proper subsets of $S$. Choose $\mathfrak{p} \in S$. Since $p \nmid \mathrm{char}(C)$, $\mathfrak{p}$ is tamely ramified in $F_S^{(p,\mathrm{elem})}$. Hence, the inertia subgroup $I_p$ of $\mathcal{G}(F_S^{(p,\mathrm{elem})}/F)$ over $\mathfrak{p}$ is cyclic [CaF, pp. 29–30, Thm. 1]. But the only cyclic subgroups of the group $(\mathbb{Z}/p\mathbb{Z})^m$ have order 1 or $p$.

Let therefore $S_0 = S \smallsetminus \{\mathfrak{p}\}$. The fixed field of $I_\mathfrak{p}$ in $F_S^{(p,\mathrm{elem})}$ is $F_{S_0}^{(p,\mathrm{elem})}$. By induction,

$$[F_{S_0}^{(p,\mathrm{elem})} : F] = p^{2g+|S_0|-1}. \tag{3}$$

Hence

$$[F_S^{(p,\mathrm{elem})} : F] = [F_S^{(p,\mathrm{elem})} : F_{S_0}^{(p,\mathrm{elem})}][F_{S_0}^{(p,\mathrm{elem})} : F] \le p \cdot p^{2g+|S_0|-1} = p^{2g+|S|-1}. \tag{4}$$

Finally, choose a prime divisor $\mathfrak{o}$ of $F/C$ not in $S$. Also, choose $\mathfrak{p}' \in S_0$. Let $\nu\colon \mathrm{Div}_0(F) \to J(C)$ be the canonical map [La3, p. 35, Thm. 9]. Let $\mathbf{p} = \nu(\mathfrak{p} - \mathfrak{o})$ and

* This part of the proof is borrowed from [FrG, Satz 12].

$\mathbf{p}' = \nu(\mathfrak{p}' - \mathfrak{o})$. Since $J(C)$ is $p$-divisible [Mum, p. 42], there exists $\mathbf{q} \in J(C)$ such that $\mathbf{p} + (p-1)\mathbf{p}' = p\mathbf{q}$. It follows that there exist $u \in F^\times$ and a prime divisor $\mathfrak{q}$ of $F/C$ such that $\mathrm{div}(u) = \mathfrak{p} + (p-1)\mathfrak{p}' - p\mathfrak{q}$ [La3, §II.2]. By Case A, $F(u^{1/p})/F$ is ramified exactly at $\mathfrak{p}$ and $\mathfrak{p}'$. Hence, $F(u^{1/p})$ is an extension of degree $p$ of $F$ which is linearly disjoint from $F_{S_0}^{(p,\mathrm{elem})}$. So, by (3),

$$[F_S^{(p,\mathrm{elem})} : F] \geq [F_{S_0}^{(p,\mathrm{elem})}(u^{1/p}) : F] = p^{2g+|S|-1}. \tag{5}$$

Combine (4) and (5) to conclude that $[F_S^{(p,\mathrm{elem})} : F] = p^{2g+|S|-1}$. ∎

The proof of the following result elaborates on the end of the proof of [MaM, Chap. V, Thm. 5.2].

Proposition 3.3: *Let $F$ be a function field of one variable over an algebraically closed field $C$ of characteristic $p > 0$. Let $S$ be a nonempty finite set of prime divisors of $F/C$. Then* $\mathrm{rank}(\mathcal{G}(F_S^{(p)}/F)) = \infty$.

*Proof:* Again, as in the beginning of the proof of Proposition 3.2, it suffices to prove that $F_S^{(p,\mathrm{elem})}/F$ is an infinite extension.

Indeed, since $S$ is nonempty, there exists $x \in F \smallsetminus C$ such that $v_\mathfrak{p}(x) \geq 0$ for each $\mathfrak{p} \notin S$. Each cyclic extension $F(u)/F$ of degree $p$ with $\wp(u) \in C[x]$ is ramified at most over $S$ (see the remark that precedes Lemma 2.6). Let $S_0$ be the restriction of $S$ to $C(x)$. If we prove that $C(x)$ has infinitely many $p$-elementary extensions which are ramified at most over $S_0$, then since $F/C(x)$ is a finite extension, $F$ will have infinitely many $p$-elementary extensions which are ramified at most at $S$. So, we may assume that $F = C(x)$.

So, by Artin-Schreier theory (see §2), it suffices to prove that the set $\{x^i \mid i \in \mathbb{N},\ p \nmid i\}$ is linearly independent over $\mathbb{F}_p$ modulo $\wp(F)$. Suppose therefore that $I$ is a finite set of positive integers which are not divisible by $p$ and that there exist relatively prime polynomials $f, g \in C[x]$ such that $\sum_{i\in I} \alpha_i x^i = \frac{f(x)^p}{g(x)^p} - \frac{f(x)}{g(x)}$ with $\alpha_i \in \mathbb{F}_p$, not all equal to 0. Then each irreducible factor of $g(x)$ is a pole of the right hand side but not of the left hand side. So, we may assume that $g(x) = 1$ and that $f(x) = \sum_{j=1}^n c_j x^j$, with $c_j \in C$ and $c_n \neq 0$. It follows that

$$\sum_{i \in I} \alpha_i x^i = \sum_{j=1}^{n} c_j^p x^{jp} - \sum_{j=1}^{n} c_j x^j.$$

Comparison of the coefficients of $x^{np}$ on both sides shows that $c_n = 0$. This contradiction proves our claim. ∎

## References

[CaF] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Academic Press, London, 1967.

[Dou] A. Douady, *Détermination d'un groupe de Galois,* C. R. Acad. Sc. Paris **258** (1964), 5305–5308.

[FrG] G. Frey and W.-D. Geyer, *Über die Fundamentalgruppe von Körpern mit Divisorentheorie,* Journal für die reine und angewandte Mathematik **254** (1972), 110–122.

[FrJ] M.D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

[Gre] M. J. Greenberg, *Lectures on forms in many variables,* Benjamin, New York, 1969.

[HaV] D. Haran and H. Völklein, *Galois groups over complete valued fields,* Israel Journal of Mathematics, **93** (1996), 9–27.

[Har] D. Harbater, *Fundamental groups and embedding problems in characteristic p,* Contemporary Mathematics **186** (1995), 353-369.

[Ja1] M. Jarden, *On free profinite groups of uncountable rank,* Contemporary Mathematics **186** (1995), 371–383.

[Ja2] M. Jarden, *Regular split embedding problems over complete valued fields,* Notes, Essen 1996.

[La1] S. Lang, *Algebra,* Addison-Wesley, Reading, 1970.

[La2] S. Lang, *Introduction to algebraic geometry,* Interscience Publishers, New York, 1958.

[La3] S. Lang, *Abelian Varieties,* Interscience Tracts in Pure and Applied Mathematics **7**, Interscience Publishers, New York, 1959.

[Lor] F. Lorenz *Einführung in die Algebra II* BI, Wissenschaftsverlag, Mannheim 1990.

[MaM] G. Malle, B. H. Matzat, Inverse Galois Theory, *Manuscript, Heidelberg, 1997.*

[Mum] D. Mumford, *Abelian Varieties,* Oxford University Press, London, 1974.

[Pop] *Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture.* Inventiones mathematicae **120** (1995), 555–578.

[Rib] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology,* Queen's papers in Pure and Applied Mathematics **24**, Queen's University, Kingston, 1970.

[Ser] J.-P. Serre, *Construction de revêtement étales de la droite affine en caractéristique $p$*, Comptes Rendus de l'Académie des Sciences **311** (1990), 341–346.

[Sha] I.R. Shafarevich, *On the construction of fields with a given Galois group of order $l^a$* Collected Mathematical Papers 107–142, Springer, Berlin, 1989.

[Son] J. Sonn, *Brauer groups, embedding problems, and nilpotent groups as Galois groups*, Israel Journal of Mathematics **85** (1994), 391–405.

9 February, 2007