THE ABSOLUTE GALOIS GROUP OF $C(x)$*

by

Dan Haran and Moshe Jarden

School of Mathematical Sciences, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: `haran@math.tau.ac.il` and `jarden@math.tau.ac.il`

Abstract

We use elementary algebraic methods to reprove a theorem which was proved by Pop using rigid analytic geometry and in a less general form by Harbater using formal algebraic patching:

Let C be an algebraically closed field of cardinality m. Consider a subset S of $\mathbb{P}^1(C)$ of cardinality m. Then the fundamental group of $\mathbb{P}^1(C) \smallsetminus S$ is isomorphic to the free profinite group of rank m.

We also observe that if $\mathrm{char}(C) \neq 0$ and $0 < \mathrm{card}(S) < m$, then $\pi_1(\mathbb{P}^1(C) \smallsetminus S)$ is not isomorphic to a free profinite group.

MR Classification: 12F12

March 7, 2000

* Research supported by the Minkowski Center for Geometry at Tel Aviv University.

Introduction

The goal of this note is to provide an elementary algebraic proof of the following result:

Main Theorem: *Let C be an algebraically closed field of cardinality m. Let x be a transcendental element over C. Then the absolute Galois group of $C(x)$ is the free profinite group $\hat{F}_m$ of rank m.*

The Main Theorem was first proved in characteristic 0 [Dou, Thm 2]. The essential part of the proof, for $C = \mathbb{C}$, uses algebraic topology and complex analysis, specifically, the Riemann Existence Theorem, to give a detailed description of the relative Galois group of the maximal Galois extension of $C(x)$ ramified at most at finitely many given points of $\mathbb{P}^1(C)$. (See the survey [Ja1, §1].) Unfortunately, this proof fails in positive characteristic. Worse, in this case, the structure of the relative Galois group is still unknown. Nevertheless, it is possible to prove that $G(C(x))$ is free by solving finite embedding problems over $C(x)$. Indeed, if $\mathrm{card}(C) = \aleph_0$, a criterion of Iwasawa reduces the proof to showing that each finite embedding problem over $C(x)$ has a solution. If $m > \aleph_0$, then, by Chatzidakis' criterion, it suffices to prove that each finite embedding problem over $C(x)$ has m distinct solutions.

There is a standard way to construct m solutions to a given embedding problem. If β is an ordinal number of cardinality less than m and if for each $\alpha < \beta$, $\mathrm{Solution}_\alpha$ is a solution to the embedding problem, then one constructs $\mathrm{Solution}_\beta$ such that it has a new branch point.

Harbater [Har] and Pop [Pop] have (independently) carried out this construction. Harbater uses formal patching in his construction. Pop applies methods of rigid analytic geometry. Both methods rely on heavy machineries, which have also been applied in Raynaud's proof of Abhyankar's conjecture and its generalization by both authors.

For the purpose of proving the Main Theorem, it suffices, however, to use the more elementary technique of algebraic patching which Völklein and the first author introduced in [HaV] and which resulted, among others, in the proof of the Main Theorem for $m = \aleph_0$. The work [HaV] was followed by [HJ1] and [HJ2]. Both works apply algebraic patching to solve embedding problems, however, ignoring ramification. The present note therefore complements [HaV], [HJ1], and [HJ2] and fills up the gap of [HJ1] and [HJ2] by taking care of ramification. As a result we provide here an elementary algebraic proof of the Main Theorem.

It turns out that the same method allows us to prove the freeness of certain fundamental groups. Let S be a subset of $C \cup \{\infty\}$ with $\mathrm{card}(S) = m$. Denote the compositum of all finite Galois extensions of $C(x)$ unramified outside S by E_S. Then $\mathcal{G}(E_S/C(x))$ is called the **fundamental group** of $\mathbb{P}^1(C) \smallsetminus S$ and is usually denoted by $\pi_1(\mathbb{P}^1(C) \smallsetminus S)$. If $S = C \cup \{\infty\}$, then E_S is the separable closure of E and $\pi_1(\mathbb{P}^1(C) \smallsetminus S) = G(C(x))$. We prove by algebraic patching that $\pi_1(\mathbb{P}^1(C) \smallsetminus S) \cong \hat{F}_m$ (Theorem 3.4). Harbater [Har] uses formal patching to prove the same result in the case where $C \smallsetminus S$ is a finite set. Pop [Pop] uses rigid patching to prove a stronger result: $\pi_1(X(C) \smallsetminus S) \cong \hat{F}_m$ for any irreducible projective curve X over C and for each subset S of $X(C)$ of cardinality m.

Using complex analytic methods, notably the Riemann Existence Theorem, one proves in characteristic 0 that if S is finite, then $\pi_1(\mathbb{P}^1(\mathbb{C}) \smallsetminus S)$ is a free profinite group. Indeed, the result is much stronger and allows to deduce the freeness of $\pi_1(\mathbb{P}^1(C) \smallsetminus S)$ for an arbitrary algebraically closed field C of characteristic 0 and for an arbitrary subset of $C \cup \{\infty\}$. If $\mathrm{char}(C) > 0$ and S is finite, then by [Ser], $\pi_1(\mathbb{P}^1(C) \smallsetminus S)$ is not free. We point out here (Theorem 3.6), that if $\mathrm{card}(S) < m$, then $\pi_1(\mathbb{P}^1(C) \smallsetminus S)$ is not free. So, the results of the preceding paragraph are optimal.

1. Ramification

Let K be a field and let E be the field of rational functions of one variable over K, say, $E = K(x)$. Each $\alpha \in \tilde{K} \cup \{\infty\}$ defines a K-place φ: $E \to \tilde{K} \cup \{\infty\}$ by $\varphi(x) = \alpha$. Let us denote the corresponding prime divisor of E/K (the equivalence class of φ) by $\mathfrak{p}_{x,\alpha}$. Then $\mathfrak{p}_{x,\alpha} = \mathfrak{p}_{x,\beta}$ if and only if α, β are conjugate over K (letting ∞ to be conjugate only to itself). Thus we may identify the prime divisors of E/K with the conjugacy classes of $\tilde{K} \cup \{\infty\}$.

Let F/E be a finite extension. An element $\alpha \in \tilde{K} \cup \{\infty\}$ is a **branch point** of F/E (with respect to x) if $\mathfrak{p}_{x,\alpha}$ is ramified in F. Denote the set of all branch points of F/E with respect to x by $\mathrm{Branch}_x(F/E)$; this set is finite.

Remark 1.1: Every K-automorphism θ of $E = K(x)$ is given by $\theta(x) = \frac{ax+b}{cx+d}$, where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Gl}_2(K)$. It induces

(i) a permutation θ' of $\tilde{K} \cup \{\infty\}$ by $\theta'(\alpha) = \frac{a\alpha+b}{c\alpha+d}$; and

(ii) a permutation θ^* of the set of prime divisors of E/K by mapping the equivalence class of the place φ onto the equivalence class of $\varphi \circ \theta$.

In particular, $\theta(x)$ is another generator of E/K. It is easy to check that

$$\theta^*(\mathfrak{p}_{x,\alpha}) = \mathfrak{p}_{x,\theta'(\alpha)} \quad \text{and} \quad \mathfrak{p}_{\theta(x),\theta'(\alpha)} = \mathfrak{p}_{x,\alpha}. \tag{1}$$

Furthermore, let F/E be a finite extension, and extend θ to an isomorphism of fields $F \to \theta(F)$. Then $\theta(F)$ is a finite extension of E and we have

$$\begin{aligned} \theta'\bigl(\mathrm{Branch}_x(\theta(F)/E)\bigr) &= \mathrm{Branch}_x(F/E), \\ \theta'\bigl((\mathrm{Branch}_x(F/E))\bigr) &= \mathrm{Branch}_{\theta(x)}(F/E). \end{aligned} \tag{2}$$

Indeed, let $\alpha \in \tilde{K} \cup \{\infty\}$ and let φ': $E \to \tilde{K} \cup \{\infty\}$ be the representative of $\mathfrak{p}_{x,\alpha}$ given by $\varphi'(x) = \alpha$. Then $\varphi' \circ \theta$: $E \to \tilde{K} \cup \{\infty\}$ represents $\theta^*(\mathfrak{p}_{x,\alpha}) = \mathfrak{p}_{x,\theta'(\alpha)}$. If ψ': $\theta(F) \to \tilde{K} \cup \{\infty\}$ extends φ', then $\psi' \circ \theta$: $F \to \tilde{K} \cup \{\infty\}$ extends $\varphi' \circ \theta$. Clearly ψ' ramifies in $\theta(F)/E$ if and only if $\psi' \circ \theta$ ramifies in F/E. Therefore $\mathfrak{p}_{x,\alpha}$ is ramified in $\theta(F)/E$ if and only if $\mathfrak{p}_{x,\theta'(\alpha)}$ is ramified in F/E. This proves the first equation of (2).

Furthermore, $\alpha \in \mathrm{Branch}_x(F/E)$ if and only if $\mathfrak{p}_{x,\alpha}$ is ramified in F/E if and only if $\mathfrak{p}_{\theta(x),\theta'(\alpha)}$ is ramified in F/E if and only if $\theta'(\alpha) \in \mathrm{Branch}_{\theta(x)}(F/E)$. ∎

To simplify the notation, write $\mathrm{Branch}(F/E)$ instead of $\mathrm{Branch}_x(F/E)$ from now on.

For the rest of this section assume that K is complete under a non-trivial ultrametric absolute value $|\ |$. Extend $|\ |$ from K to E by $|\sum a_n x^n| = \max_n |a_n|$, $a_n \in K$.

Let $I \neq \emptyset$ be a finite set. Let $c_i \in K$, for $i \in I$, such that $|c_i| \le |c_i - c_j| = 1$ for $i \neq j$. For each $i \in I$ put $w_i = \frac{1}{x-c_i} \in K(x)$. Let $R = K\{w_i|\ i \in I\}$ be the completion of the subring $K[w_i|\ i \in I]$ of E. Thus (cf. [HJ1, Lemma 3.3]) each element f of R has a unique presentation as a multiple power series:

$$f = a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in} w_i^n,$$

where $a_0, a_{in} \in K$, and $|a_{in}| \to 0$ as $n \to \infty$. Moreover, $|f| = \max_{i,n}\{|a_0|, |a_{in}|\}$. Let $Q = \mathrm{Quot}(R)$ be the quotient field of R.

Extend the absolute value $|\ |$ from K to $\tilde{K}$ (uniquely, since K is complete).

Lemma 1.2: *Let $\mathfrak{p}_{x,\alpha}$ be a prime divisor of E/K and let v be be the associated discrete valuation of E/K.*

(a) *If $|\alpha - c_i| \ge 1$ for all $i \in I$, then v extends to a valuation $\hat{v}$ of Q such that the extension $(Q,\hat{v})/(E,v)$ is immediate.*

(b) *Let F/E be a finite Galois extension such that $F \subseteq Q$. If $\alpha \in \mathrm{Branch}(F/E)$, then there is $i \in I$ such that $|\alpha - c_i| < 1$.*

Proof: (a) The map $\varphi\colon R \to K(\alpha)$ given by

$$a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in} w_i^n \quad \mapsto \quad a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in}\Big(\frac{1}{\alpha - c_i}\Big)^n$$

is clearly an epimorphism of rings. Fix $i \in I$. By [HJ1, Prop. 3.9] and its proof, R is a principal ideal domain and the ideal $\mathrm{Ker}(\varphi)$ of R is generated by an element $q \in K[w_i]$ such that $\mathrm{Ker}(\varphi) \cap K[w_i] = qK[w_i]$.

Since q is irreducible in R, the localization R_{qR} is a discrete valuation ring, and hence φ uniquely extends to a place $\varphi\colon Q \to K(\alpha) \cup \{\infty\}$. Clearly, φ extends $\mathfrak{p}_{x,\alpha}$. Thus the corresponding discrete valuation $\hat{v}$ on Q extends v. It has the same residue field $K(\alpha)$ as v has, and q is a uniformizer for both v and $\hat{v}$. Therefore $\hat{v}/v$ is immediate.

(b) Suppose that $|\alpha - c_i| \geq 1$ for each $i \in I$. By (a), v extends to Q such that the extension is immediate; in particular, it is unramified. But $E \subseteq F \subseteq Q$, hence v is unramified in F. ▮

Now assume that I has at least 2 elements. For each $i \in I$ let

$$Q_i = \mathrm{Quot}(K\{w_j |\, j \neq i\}) \qquad \text{and} \qquad Q_i' = \mathrm{Quot}(K\{w_i\}).$$

Then

(3a) $\bigcap_{i\in I} Q_i = E$ and $Q_i' = \bigcap_{j\neq i} Q_j$, for each $i \in I$ [HJ1, Prop. 3.10];

(3b) For each positive integer n and for all $B \in \mathrm{GL}_n(Q)$ and $i \in I$ there exist $B_1 \in \mathrm{GL}_n(Q_i)$ and $B_2 \in \mathrm{GL}_n(Q_i')$ such that $B = B_1 B_2$ [HJ1, Cor. 4.5].

Furthermore, let $G_i \leq G$, $i \in I$, be finite groups and F_i, $i \in I$, be fields such that

(3c) F_i/E is a Galois extension with group G_i, $i \in I$;

(3d) $F_i \subseteq Q_i'$;

(3e) $G = \langle G_i |\, i \in I\rangle$.

Remark 1.3: Conditions (3a)-(3e) amount to saying that $\mathcal{E} = (E, F_i, Q_i, Q; G_i, G)_{i\in I}$ is a **patching data** in the sense of [HaV, Definition 3.3], [HJ1, Definition 1.1], and [HJ2, Definition 3.1]. In what follows we shall consider the **compound** F of $\mathcal{E}$. As explained in [HaV, Lemma 3.6], F is a certain Galois extension of E contained in Q with Galois group G. More precisely, by (3a) we have for each $i \in I$ that $Q_i \cap Q_i' = E$, and hence the restriction map of Galois groups $\mathcal{G}(F_iQ_i/Q_i) \to \mathcal{G}(F_i/E) = G_i$ is an isomorphism. If we identify $\mathcal{G}(F_iQ_i/Q_i)$ with G_i via this map, then F is the largest subfield of $\bigcap_{i\in I} F_iQ_i$, on which G acts so that each subgroup G_i of G acts via the restriction of automorphisms to F [HaV, Lemma 3.6(b),(c)]. ▮

Lemma 1.4: *Let F be the compound of $\mathcal{E} = (E, F_i, Q_i, Q; G_i, G)_{i\in I}$.*

(a) *Let $i \in I$. If $\alpha \in \mathrm{Branch}(F_i/E)$, then $|\alpha - c_i| < 1$. In particular, the sets $\mathrm{Branch}(F_i/E)$, for $i \in I$, are disjoint.*

(b) $\mathrm{Branch}(F/E) = \dot\bigcup_{i\in I} \mathrm{Branch}(F_i/E)$.

(c) *Suppose that the set I contains the symbol 1 and $G = H \ltimes G_1$, where $H = \langle G_i |\, i \in I \smallsetminus \{1\}\rangle \lhd G$. Then $F^H = F_1$ and $\mathrm{Branch}(F^{G_1}/E) = \dot\bigcup_{\substack{i\in I\\ i\neq 1}} \mathrm{Branch}(F_i/E)$.*

Proof: (a) By assumption, $F_i \subseteq Q_i'$. By Lemma 1.2(b), with $I = \{i\}$, each $\alpha \in \mathrm{Branch}(F_i/E)$ satisfies $|\alpha - c_i| < 1$.

(b) Let $\mathfrak{p}_{x,\alpha}$ be prime divisor of E/K and let v be the corresponding discrete valuation of E. Assume first that v is ramified in F_i. By (a), $|\alpha - c_i| < 1$. For each $j \neq i$ we have $|c_i - c_j| = 1$, hence $|\alpha - c_j| = 1$. By Lemma 1.2(a), v extends to a valuation v_i on Q_i which is immediate in Q_i/E. By [HaV, Lemma 3.6(e)], v is ramified in F.

Conversely, assume that v is ramified in F. We claim that there is $i \in I$ such that

(*) $|\alpha - c_j| \geq 1$ for all $j \neq i$.

Indeed, if there is $i \in I$ such that $|\alpha - c_i| < 1$, then i satisfies (*), because $|c_i - c_j| = 1$ for all $j \neq i$. Otherwise each $i \in I$ satisfies (*).

Fix $i \in I$ that satisfies (*). By Lemma 1.2(a), v extends to a valuation v_i on Q_i which is immediate in Q_i/E. By [HaV, Lemma 3.6(e)], v is ramified in F_i.

(c) We have $F^H = F_1$ by [HJ2, Cor. 3.4(d)] with $\Gamma = 1$. It follows that $F_1 \cap F^{G_1} = E$ and $F_1 F^{G_1} = F$. Hence $\mathrm{Branch}(F/E) = \mathrm{Branch}(F_1/E) \cup \mathrm{Branch}(F^{G_1}/E)$.

Let $\alpha \in \bigcup_{i \neq 1} \mathrm{Branch}(F_i/E)$. By (b), $\alpha \in \mathrm{Branch}(F/E)$; but, by (a), $\alpha \notin \mathrm{Branch}(F_1/E)$. Hence $\alpha \in \mathrm{Branch}(F^{G_1}/E)$.

Conversely, let $\alpha \in \mathrm{Branch}(F^{G_1}/E)$. Then $\alpha \in \mathrm{Branch}(F/E)$. By (b), there is $i \in I$ such that $\alpha \in \mathrm{Branch}(F_i/E)$. If $i = 1$, then, as in the first paragraph of the proof of (b), the valuation v corresponding to $\mathfrak{p}_{x,\alpha}$ extends to a valuation v_i on Q_i which is immediate in Q_i/E. But $F^{G_1} \subseteq (F_1 Q_1)^{G_1} = Q_1$, so v_i is ramified over v. A contradiction. Therefore $\alpha \in \bigcup_{i \neq 1} \mathrm{Branch}(F_i/E)$. ∎

2. The fundamental group of a subset of a line

Let K be an algebraically closed field, and fix a transcendental element x over K. The set P of prime divisors of $E = K(x)$ can be identified with $K \cup \{\infty\}$. For each subset S of P let E_S be the maximal Galois extension of E unramified outside S, and let $G_S(E) = \mathcal{G}(E_S/E)$. In particular, $G_P(E)$ is the absolute Galois group $G(E)$ of E.

The main result of this section is that if K is complete with respect to a non-trivial ultrametric absolute value, and $\mathrm{card}(K \smallsetminus S) < \mathrm{card}(K)$, then $G_S(E)$ is the free profinite group of cardinality $\mathrm{card}(K)$.

Recall [FrJ, p. 289] that a **finite embedding problem** for a profinite group G

$$(1) \qquad (\alpha\colon B \to A,\ \varphi\colon G \to A)$$

consists of an epimorphism $\alpha\colon B \to A$ of finite groups and a continuous epimorphism $\varphi\colon G \to A$. The **kernel** of (1) is $\mathrm{Ker}\,\alpha$. A **solution** (resp., a **weak solution**) is a continuous epimorphism (resp. homomorphism) $\psi\colon G \to B$ such that $\alpha \circ \psi = \varphi$.

Without loss of generality φ is the quotient map modulo $\mathrm{Ker}\,\varphi$. Thus if G is a Galois group, say $G = \mathcal{G}(\hat{E}/E)$, then $A = \mathcal{G}(F_1/E)$, where F_1 is a finite Galois extension of E contained in $\hat{E}$, and φ is the restriction map from $\hat{E}$ to F_1. In this case we usually abbreviate (1) as

$$(2) \qquad \alpha\colon B \to \mathcal{G}(F_1/E).$$

A **solution field** of (2) is a Galois extension F of E such that $E \subseteq F_1 \subseteq F \subseteq \hat{E}$, and an isomorphism $\lambda\colon \mathcal{G}(F/E) \to B$ such that $\alpha \circ \lambda = \mathrm{res}_{F/F_1}$. By Galois theory, the solutions fields F of (2) correspond to the kernels of the solutions $\psi\colon G(\hat{E}/E) \to B$. Notice that only finitely many solutions may have the same kernel.

We begin with a weaker assertion:

LEMMA 2.1: *Let $S \subseteq P$. Then $G_S(E)$ is projective, i.e., every finite embedding problem for $G_S(E)$ has a weak solution.*

Proof: If S is finite, this is the content of [Ser, Prop. 1] or [Ja2, Theorem 2.7]. (If $S = \emptyset$ then $G_S(E) = 1$ by the Riemann-Hurwitz genus formula [FrJ, Prop. 2.15].)

In the general case we have to show that each finite embedding problem (2) for $G_S(E)$ has a weak solution. Here $F_1 \subseteq E_S$.

Let $T = \mathrm{Branch}(F_1/E)$. Then $T \subseteq S$, and hence $F_1 \subseteq E_T \subseteq E_S$. Factor the restriction $\varphi\colon G_S(E) \to \mathcal{G}(F_1/E)$ into the restrictions $\mathrm{res}_1 : G_S(E) \to G_T(E)$ and $\mathrm{res}_2 : G_T(E) \to \mathcal{G}(F_1/E)$. As T is finite, by the above quoted result there is a homomorphism $\psi_2\colon G_T(E) \to B$ such that $\alpha \circ \psi_2 = \mathrm{res}_2$. Put $\psi = \psi_2 \circ \mathrm{res}_1$. Then $\alpha \circ \psi = \mathrm{res}_{F_1}$. ∎

Lemma 2.2: *For each integer $n > 1$ there exists a cyclic extension F/E of degree n such that* $\mathrm{Branch}(F/E) = \{1, \infty\}$. *If* $\mathrm{char}(K) > 0$ *and n is a power of* $\mathrm{char}(K)$, *then there exists a cyclic extension F/E of degree n such that* $\mathrm{Branch}(F/E) = \{\infty\}$.

Proof: If $\mathrm{char}(K) \nmid n$, let $F = E(y)$, where $y^n = x - 1$. If $n = p = \mathrm{char}(K) > 0$, let $F = E(y)$, where either $y^p - y = x$ or $y^p - y = \frac{x^2}{x-1}$. In the first case $\mathrm{Branch}(F/E) = \{\infty\}$ and in the second case $\mathrm{Branch}(F/E) = \{1, \infty\}$.

The rest of the proof reduces the general case to these two cases.

Part A: *Without loss of generality n is a prime power.* Indeed, if $n = \prod_{i=1}^m p_i^{r_i}$, where $p_1, \ldots, p_m$ are distinct primes, and for each $1 \le i \le m$ there is a cyclic extension F_i/E of degree $p_i^{r_i}$, ramified at $\{1, \infty\}$, then the compositum $F = \prod_{i=1}^m F_i$ has the required properties.

Part B: *Without loss of generality n is prime.* Indeed, assume that n is a power of a prime p and there is a cyclic extension F_1/E of degree p, ramified at $\{1, \infty\}$. Let $S = \{1, \infty\}$. By Lemma 2.1, the embedding problem

$$(\alpha\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathcal{G}(F_1/E), \quad \mathrm{res}\colon G_S(E) \to \mathcal{G}(F_1/E))$$

for $G_S(E)$ has a weak solution, say, $\psi\colon G_S(E) \to \mathbb{Z}/n\mathbb{Z}$. But ψ is surjective, since $\alpha(\psi(\mathbb{Z}/n\mathbb{Z})) = \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ is the only subgroup H of $\mathbb{Z}/n\mathbb{Z}$ with $\alpha(H) = \mathbb{Z}/p\mathbb{Z}$. The fixed field F of $\mathrm{Ker}\,\psi$ has the required properties. ∎

Lemma 2.3: *Assume that K is complete with respect to a non-trivial ultrametric absolute value $|\ |$. Let $c \in K$ and put $w = \frac{1}{x-c}$. Let $n > 1$ be an integer. Then there is*

$0 < r < 1$ *such that for all* $b_1, b_2 \in K$ *with* $|b_1 - c|, |b_2 - c| \le r$ *there is a cyclic extension* F/E *of degree* n*, with* $\mathrm{Branch}(F/E) = \{b_1, b_2\}$ *and* $F \subseteq \mathrm{Quot}(K\{w\})$*.*

Proof: Lemma 2.2 produces a cyclic extension F_1/E of degree n with $\mathrm{Branch}(F_1/E) = \{1, \infty\}$. Since F_1/E is unramified at 0, we have $F_1 \subseteq K((x))$. By [HaV, Lemma 4.2(b)] there is $r > 0$ with the following property: If $a \in K^\times$ and $|a| \le r$, then the K-automorphism of E given by $x \mapsto ax$ extends to an embedding $\mu_a \colon F_1 \to \mathrm{Quot}(K\{x\})$. Without loss of generality $r < 1$. Let $b_1, b_2 \in K$ such that $|b_1 - c|, |b_2 - c| \le r$. Put $a = b_2 - b_1$ and denote $F_2 = \mu_a(F_1)$. By Remark 1.1,

$$\mathrm{Branch}(F_2/E) = (\mu_a')^{-1}(\mathrm{Branch}(F_1/E)) = \frac{1}{a}\{1, \infty\} = \{\frac{1}{b_2 - b_1}, \infty\}.$$

Let θ be the K-automorphism of E given by $\theta(x) = w$. Extend θ to an isomorphism of fields $\theta \colon F_2 \to F_3$. Then $F_3 \subseteq \mathrm{Quot}(K\{w\})$. We have

$$\mathrm{Branch}(F_3/E) = (\theta')^{-1}(\mathrm{Branch}(F_2/E)) = (\theta')^{-1}\{\frac{1}{b_2 - b_1}, \infty\} = \{c + b_2 - b_1, c\}.$$

Let $d = c - b_1$. Then $|d| \le r \le 1$. Let λ be the automorphism of $K[[w]]$ that maps $f = \sum_{n=0}^\infty a_n w^n$ onto

$$\lambda(f) = \sum_{n=0}^\infty a_n (w + d)^n = \sum_{n=0}^\infty a_n \sum_{k=0}^n \binom{n}{k} d^{n-k} w^k = \sum_{k=0}^\infty \Big(\sum_{n=k}^\infty \binom{n}{k} a_n d^{n-k} \Big) w^k$$

Then

$$|\sum_{n=k}^\infty \binom{n}{k} a_n d^{n-k}| \le \max_{n \ge k} |a_n|$$

and hence $\lambda(K\{w\}) \subseteq K\{w\}$. Therefore we can extend λ to an automorphism of $\mathrm{Quot}(K\{w\})$. The restriction of λ to E is the map $w \mapsto w + d$. Let $F = \lambda(F_3)$. Then $F \subseteq \mathrm{Quot}(K\{w\})$ and

$$\mathrm{Branch}(F/E) = (\lambda')^{-1}(\mathrm{Branch}(F_3/E)) = \{c + b_2 - b_1 - d, c - d\} = \{b_2, b_1\}. \qquad \blacksquare$$

To prove that a projective group is free, we need the following criterion, essentially due to Iwasawa [FrJ, Cor. 24.2] and Chatzidakis [FrJ, Lemma 24.14 and Prop. 24.18].

Lemma 2.4: *Let m be an infinite cardinal number and let G be a projective group of rank $\le m$. Put*

$$m' = \begin{cases} 1 & \textit{if } m = \aleph_0, \\ m & \textit{if } m > \aleph_0, \end{cases}$$

and assume that each finite split embedding problem for G with a nontrivial kernel has m' distinct solutions. Then $G \cong \hat{F}_m$.

Proof: The existence of m solutions of (1) for $A = 1$ and $B = \mathbb{Z}/2\mathbb{Z}$ implies that G is of rank m.

By [FrJ, Cor. 24.2] in the first case and by [FrJ, Lemma 24.14 and Prop. 24.18] or [Ja1, Lemma 2.1] in the second case, it suffices to prove that each (i.e., not necessarily split) finite embedding problem (1) for G with $\mathrm{Ker}\,\alpha \ne 1$ has m' distinct solutions. As G is projective, there exists a homomorphism $\psi\colon G \to B$ such that $\alpha \circ \psi = \varphi$. Then $\hat{A} = G/\mathrm{Ker}\,\psi$ is a finite group and there exist homomorphisms $\hat{\varphi}\colon \hat{A} \to A$ and $\hat{\psi}\colon \hat{A} \to B$ such that $\hat{\varphi} \circ \pi = \varphi$, $\hat{\psi} \circ \pi = \psi$, and $\alpha \circ \hat{\psi} = \hat{\varphi}$, where $\pi\colon G \to \hat{A}$ is the quotient map. Let $\hat{B} = B \times_A \hat{A}$ and let $\hat{\alpha}\colon \hat{B} \to \hat{A}$ and $\beta\colon \hat{B} \to B$ be the projections from $\hat{B}$. Then there exists $\theta\colon \hat{A} \to \hat{B}$ such that $\hat{\alpha} \circ \theta = \mathrm{id}_{\hat{A}}$ and $\beta \circ \theta = \hat{\psi}$ [FrJ, Lemma 20.6]. So, $(\pi\colon G \to \hat{A},\ \hat{\alpha}\colon \hat{B} \to \hat{A})$ is a finite split embedding problem for G and $\mathrm{Ker}\,\hat{\alpha} \cong \mathrm{Ker}\,\alpha \ne 1$.

By assumption, there exist m' distinct epimorphisms $\psi_i\colon G \to \hat{B}$ such that $\hat{\alpha} \circ \psi_i = \pi$, $i \in I$. If $i, i' \in I$ and $\beta \circ \psi_i = \beta \circ \psi_{i'}$, then $\psi_i = \psi_{i'}$ [FrJ, Lemma 20.6]. Conclude that $\beta \circ \psi_i$, $i \in I$, are m' distinct solutions of embedding problem (1). ∎

A **disk** in $K \cup \{\infty\}$ is a set of the form

$$D = \theta(\{a \in K \mid |a| \le r\})$$

where $r > 0$ and θ is a Möbius transformation over K. Thus each set of the form $D = \{a \in K \mid |a - c| \le r'\}$ or $D = \{a \in K \mid |a| \ge r'\} \cup \{\infty\}$, where $r' > 0$ and $c \in K$, is a disk. (In fact, each disk is of this form; but we shall not use this fact.) Note that the cardinality of a disk is the same as the cardinality of K.

Lemma 2.5: *Assume that K is complete with respect to a non-trivial ultrametric absolute value. Let F_1/E be a finite Galois extension with group G_1. Let*

$$\alpha\colon G = H \rtimes G_1 \to G_1 = \mathcal{G}(F_1/E) \tag{3}$$

be a finite split embedding problem for $G(E)$. Suppose that $H = \mathrm{Ker}\,\alpha$ is generated by a finite family $\{G_i\}_{i\in J}$ of nontrivial cyclic subgroups. Then there exists a family of pairwise disjoint disks $\{D_i\}_{i\in J}$ in $K \cup \{\infty\}$ such that for every $B \subset \bigcup_{i\in J} D_i$ with $\mathrm{card}(B\cap D_i) = 2$, for each $i \in J$, there exists a solution field F to (3) with $\mathrm{Branch}(F^{G_1}/E) = B$.

Proof: For the sake of compatibility with [HJ2] assume that J does not contain the symbol 1 and put $I = J \cup \{1\}$. Then $G = \langle G_i |\ i \in I\rangle$. For each $i \in I$ let $c_i \in K$, w_i, etc., be as in Section 1 (see Remark 1.3). In particular, $Q_i = \mathrm{Quot}(K\{w_j |\ j \neq i\})$ and $Q_i' = \mathrm{Quot}(K\{w_i\})$.

Claim: *We may assume that $F_1 \subseteq Q_1'$.* Indeed, as K is algebraically closed, every prime divisor of F_1/K is of degree 1. In particular, F_1/K has an unramified prime divisor of degree 1. By [HaV, Lemma 4.2] there is a K-automorphism of E that extends to an embedding θ: $F_1 \to Q_1'$. Let $F_1' = \theta(F_1)$ and extend θ to an automorphism of $\tilde{E}$. Then θ defines isomorphisms θ_*: $\mathcal{G}(F_1/E) \to \mathcal{G}(F_1'/E)$ and θ_*: $G(E) \to G(E)$ such that the following diagram commutes

$$\begin{tikzcd}
 & G(E) \arrow[r, "\theta_*"] \arrow[d, "\mathrm{res}"] & G(E) \arrow[d, "\mathrm{res}"] \\
G \arrow[r, "\alpha"] & \mathcal{G}(F_1/E) \arrow[r, "\theta_*"] & \mathcal{G}(F_1'/E).
\end{tikzcd}$$

Suppose that there is a family of disks $\{D_i'\}_{i\in J}$ such that for every $B' \subset \bigcup_{i\in J} D_i'$ with $\mathrm{card}(B'\cap D_i') = 2$, for each $i \in J$, there exists a solution field F' to the embedding problem

$$(\theta_* \circ \alpha \colon G \to \mathcal{G}(F_1'/E),\ \mathrm{res}\colon G(E) \to \mathcal{G}(F_1'/E))$$

with $\mathrm{Branch}(F'^{G_1}/E) = B'$. Then the disks $D_i = \theta'(D_i)$, for $i \in J$, have the required property.

Indeed, if $B \subset \bigcup_{i\in J} D_i$ and $\mathrm{card}(B \cap D_i) = 2$, for each $i \in J$, put $B' = (\theta')^{-1}(B)$, and let F' be as above. Clearly, $F = \theta^{-1}(F')$ solves (3). By Remark 1.1, $\mathrm{Branch}(F^{G_1}/E) = B$.

Thus, replacing F_1 by F_1' we may assume that $F_1 \subseteq Q_1'$.

By Lemma 2.3 there is $0 < r < 1$ such that the (necessarily disjoint) disks $D_i = \{a \in K| \ |a - c_i| \leq r\}$, for $i \in J$, have the following property. For every $B \subset \bigcup_{i \in J} D_i$ with $\mathrm{card}(B \cap D_i) = 2$, for each $i \in J$, there exist Galois extensions F_i/E with the cyclic Galois group G_i and $\mathrm{Branch}(F_i/E) = B \cap D_i$ and $F_i \subseteq \mathrm{Quot}(K\{w_i\})$, for each $i \in J$.

By Remark 1.3, $\mathcal{E} = (E, F_i, Q_i, Q; G_i, G)_{i \in I}$ is a patching data. Its compound F is, by [HJ2, Cor. 3.4(d)] with $\Gamma = 1$, a Galois extension of E that solves (3). By Lemma 1.4(c),

$$\mathrm{Branch}(F^{G_1}/E) = \bigcup_{i \in J} \mathrm{Branch}(F_i/E) = \bigcup_{i \in J} B \cap D_i = B. \qquad \blacksquare$$

3. Descent

We wish to apply Lemma 2.5 to a sufficiently large complete extension of a given algebraically closed field.

Thus we consider the following situation. Let $C_1 \subseteq C_2$ be two algebraically closed fields and let x be transcendental over C_2. Denote $E_1 = C_1(x)$ and $E_2 = C_2(x)$. Let

$$\rho\colon G = H \ltimes G_1 \to G_1 = \mathcal{G}(F_1/E_1) \tag{1}$$

be a finite split embedding problem for $G(E_1)$ with a nontrivial kernel. Let $F_2 = F_1E_2$. Then the restriction $\mathcal{G}(F_2/E_2) \to \mathcal{G}(F_1/E_1)$ is an isomorphism. Identify $\mathcal{G}(F_2/E_2)$ with $G_1 = \mathcal{G}(F_1/E_1)$ via this map. Then (1) induces a finite split embedding problem

$$\rho\colon G = H \ltimes G_1 \to G_1 = \mathcal{G}(F_2/E_2) \tag{2}$$

for $G(E_2)$ with a nontrivial kernel.

Before dealing with embedding problems let us notice a simple fact:

Remark 3.1: Let A be an infinite subset of a field K. Then every nonempty Zariski K-open subset of $\mathbb{A}^n$ meets A^n. Indeed, the only polynomial in n variables over K that vanishes on A^n is 0. ∎

LEMMA 3.2: *Let A be an infinite subset of C_1. Assume that (2) has a solution field L_2 such that $\infty \notin \mathrm{Branch}(L_2^{G_1}/E_2)$ and the elements of $\mathrm{Branch}(L_2^{G_1}/E_2)$ are algebraically independent over C_1. Then (1) has a solution field L_1 with $\mathrm{Branch}(L_1^{G_1}/E_1) \subseteq A$.*

Proof: There is an irreducible monic polynomial $h \in C_2[x, Z]$ such that $L_2 = E_2(z)$, where $h(x, z) = 0$. Furthermore, there are irreducible polynomials $f_1, \ldots, f_r \in C_2[x, Z]$ such that a root z_i of f_i is a primitive element of $L_2^{G_1}/E_2$ (and hence also of L_2/F_2), and

$$\mathrm{Branch}(L_2^{G_1}/E_2) = \bigcap_{j=1}^{r} \mathrm{Discr}(f_j) \tag{3}$$

[Has, p. 64].

There is an integer l and a l-tuple $\mathbf{u} = (u_1, \ldots, u_l)$ of elements of C_2 such that $h, f_1, \ldots, f_r \in C_1[\mathbf{u}][x, Z]$. Without loss of generality $\mathrm{Branch}(L_2^{G_1}/E_2) \subseteq \{u_1, \ldots, u_l\}$, say, $\mathrm{Branch}(L_2^{G_1}/E_2) = \{u_1, \ldots, u_k\}$, where $k \leq l$.

Now, $\mathbf{u}$ generates a variety $U = \mathrm{Spec}(C_1[\mathbf{u}])$ over C_1. For each $\mathbf{u}' \in U(C_1)$ the C_1-specialization $\mathbf{u} \to \mathbf{u}'$ extends to a $C_1(x)$-homomorphism $'\colon C_1(x)[\mathbf{u}] \to C_1(x)$, and from there to an F_1-homomorphism $'\colon F_1[\mathbf{u}] \to F_1$. Extend it to an F_1-place from L_2 into the algebraic closure of F_1. Let $B = \{u_1', \ldots, u_k'\} \subseteq C_1$ be the image of $\mathrm{Branch}(L_2^{G_1}/E_2) = \{u_1, \ldots, u_k\}$.

The variety U has a nonempty Zariski open subset U' such that if $\mathbf{u}' \in U'$, then, in the above notation,

(4a) $h, f_1', \ldots, f_r' \in C_1[x, Z]$ are irreducible over $C_1(x)$ [FrJ, Prop. 8.8];

(4b) $L_1 = E_1(z')$ is Galois over E_1 and $\mathcal{G}(L_1/E_1) \cong \mathcal{G}(L_2/E_2) = G$ [FrJ, Lemma 5.5];

(4c) the respective roots $z_1', \ldots, z_r'$ of $f_1', \ldots, f_r'$ are primitive elements for $L_1^{G_1}/E_1$.

Thus L_1 solves (1). From (3), $B = \bigcap_{j=1}^{r} \mathrm{Discr}(f_j')$. In particular, since $L_1^{G_1}/E_1$ is unramified at each point outside $\mathrm{Discr}(f_1')$,

(4d) $\mathrm{Branch}(L_1^{G_1}/E_1) \subseteq B$.

By assumption, $u_1, \ldots, u_k$ are algebraically independent over C_1. Thus the projection on the first k coordinates $\mathrm{pr}\colon U \to \mathbb{A}^k$ is a dominant map, and hence $\mathrm{pr}(U')$ contains a Zariski open subset of $\mathbb{A}^k$ [Lan, Prop. 4 on p. 88]. By Remark 3.1 we may choose $\mathbf{u}'$ so that $B = \{u_1', \ldots, u_k'\} \subseteq A$. Thus $\mathrm{Branch}(L_1^{G_1}/E_1) \subseteq A$. ∎

To achieve the algebraic independence in Lemma 3.2 we use:

LEMMA 3.3: *Let $C_1 \subseteq C_2$ be two algebraically closed fields such that* $\mathrm{card}(C_1) < \mathrm{card}(C_2)$. *Let $\{D_j\}_{j \in J}$ be a finite collection of pairwise disjoint subsets of C_2 of cardinality* $\mathrm{card}(C_2)$. *Then there exists a set $B \subseteq \bigcup_{j \in J} D_j$ such that* $\mathrm{card}(B \cap D_j) = 2$ *for each $j \in J$ and the elements of B are algebraically independent over C_1.*

Proof: Write J as $\{1, \ldots, k\}$, and suppose, by induction, that we have already found $b_j, b_j' \in D_j$, for $j = 1, \ldots, k-1$, such that $b_1, b_1', \ldots, b_{k-1}, b_{k-1}'$ are algebraically independent over C_1. The cardinality of the algebraic closure $\tilde{C}_1$ of $C_1(b_1, b_1', \ldots, b_{k-1}, b_{k-1}')$

in C_2 is $\mathrm{card}(C_1) < \mathrm{card}(C_2) = \mathrm{card}(D_k)$, so there exist $b_k, b_k' \in D_k$ algebraically independent over $\tilde{C}_1$. Thus $b_1, b_1', \ldots, b_k, b_k'$ are algebraically independent over C_1. ∎

The preceding lemmas yield the main result:

THEOREM 3.4: *Let C be an algebraically closed field of cardinality m and let $E = C(x)$ be the field of rational functions over C. Let $S \subseteq C \cup \{\infty\}$ of cardinality m. Then $G_S(E)$ is isomorphic to the free profinite group of rank m.*

Proof: Put $C_1 = C$ and $E_1 = E$. By Lemma 2.1, $G_S(E)$ is projective. Therefore, by Lemma 2.4, it suffices to show that every finite split embedding problem (1) for $G_S(E)$ has m' solution fields, where $m' = 1$ if $m = \aleph_0$, and $m' = m$ otherwise.

Let $\beta < m$ be an ordinal number. Suppose, by transfinite induction, that $\{L_\alpha\}_{\alpha<\beta}$ is a family of distinct solution fields of (1). For each α, the set $\mathrm{Branch}(L_\alpha/E)$ is finite. Hence, $\mathrm{A} = S \smallsetminus \bigcup_{\alpha<\beta} \mathrm{Branch}(L_\alpha/E)$ is infinite.

Choose an algebraically closed field $K = C_2$ which contains C, complete with respect to a non-trivial ultrametric absolute value, such that $\mathrm{card}(C) < \mathrm{card}(K)$. For instance, choose a field C' that contains C such that $\mathrm{card}(C) < \mathrm{card}(C')$, and let K be the completion of the algebraic closure of $C'((t))$. Consider the induced embedding problem (2).

By Lemma 2.5 there exists a family of disks $\{D_j\}_{j\in J}$ in $K \cup \{\infty\}$ such that for every $B \subset \bigcup_{j\in J} D_j$ with $\mathrm{card}(B \cap D_j) = 2$, for each $j \in J$, there exists a solution field L_2 to (2) with $\mathrm{Branch}(L_2^{G_1}/K(x)) = B$. Choose such a set B. By Lemma 3.3, with $D_j \smallsetminus \{\infty\}$ instead of D_j, we may assume that the elements of B are algebraically independent over C. Therefore by Lemma 3.2, (1) has a solution field F such that $\mathrm{Branch}(F^{G_1}/E) \subseteq A$.

Since $F = F_1 F^{G_1}$, we have $\mathrm{Branch}(F/E) = \mathrm{Branch}(F_1/E) \cup \mathrm{Branch}(F^{G_1}/E)$. Furthermore, $\mathrm{Branch}(F_1/E), \mathrm{Branch}(F^{G_1}/E) \subseteq S$. Thus $\mathrm{Branch}(F/E) \subseteq S$. Also, let $\alpha < \beta$. Then $\mathrm{Branch}(F^{G_1}/E) \cap \mathrm{Branch}(L_\alpha/E) = \emptyset$. But $\mathrm{Branch}(F^{G_1}/E) \neq \emptyset$ by the Riemann-Hurwitz genus formula [FrJ, Prop. 2.15] and $\mathrm{Branch}(F^{G_1}/E) \subseteq \mathrm{Branch}(F/E)$. Therefore $\mathrm{Branch}(F/E) \neq \mathrm{Branch}(L_\alpha/E)$, whence $F \neq L_\alpha$. ∎

COROLLARY 3.5: *Let C be an algebraically closed field of cardinality m. Let E be a field of algebraic functions in one variable over C. Then $G(E)$ is isomorphic to the free profinite group of rank m.*

Proof: If E is the field of rational functions, apply Theorem 3.4 with $S = P$. In the general case E is a finite separable extension of $C(x)$. Therefore $G(E)$ is an open subgroup of $G(C(x))$. The assertion follows from [FrJ, Prop. 15.27]. ∎

If $\mathrm{char}(C) = 0$ and S is an arbitrary subset of $C \cup \{\infty\}$, then, using the Riemann Existence Theorem and a result of Douady for the case when S is finite, one can prove that $G_S(E)$ is a free profinite group of rank $\mathrm{card}(S)$ (as in [Ja1, §1.8]). If, however, $\mathrm{char}(C) > 0$ and $\mathrm{card}(S) < \mathrm{card}(C)$, then this is no longer true. In fact, $G_S(E)$ is even not free:

THEOREM 3.6: *Let C be an algebraically closed field of positive characteristic and of cardinality m. Let E be a finite extension of $C(x)$ and let S be a nonempty subset of prime divisors of E/C of cardinality less than m. Denote the maximal Galois extension of E unramified outside S by E_S. Then $\mathcal{G}(E_S/E)$ is not a free profinite group.*

Proof: Assume that $\mathcal{G}(E_S/E)$ is isomorphic to the free profinite group of rank k. For each prime number p let $d_S(p)$ be the cardinality of the family $\mathcal{D}_S(p)$ of Galois extensions of E of degree p in S. Then $d_S(p)$ is the cardinality of the family of open normal subgroups of $\mathcal{G}(E_S/E)$ of index p. Hence $d_S(p) = 2^k$, if k is finite, and $d_S(p) = k$, if k is infinite. But this contradicts the conjunction of the following two claims.

CLAIM A: *If $p \neq \mathrm{char}(C)$, then $d_S(p) < m$.*

Indeed, if S is a finite set, then $d_S(p)$ is finite [Ja2, Prop. 3.2]. In the general case, let $\mathcal{A}$ be the collection of all finite nonempty subsets of S. Its cardinality is, like that of S, less than m. As $\mathcal{D}_S(p) = \bigcup_{A\in\mathcal{A}} \mathcal{D}_A(p)$, we have $d_S(p) \le \sum_{A\in\mathcal{A}} d_A(p) < m$.

CLAIM B: *If $p = \mathrm{char}(C)$, then $d_S(p) = m$.*

Indeed, the case where $m = \aleph_0$ is covered by [Ja2, Prop. 3.3]. So, assume $m > \aleph_0$. Since $E/C(x)$ is a finite extension, it suffices to construct m linearly disjoint cyclic extensions of $C(x)$ of degree p unramified outside $S|_{C(x)}$. We may therefore assume without loss that $E = C(x)$. Also, apply a Möbius transformation on E, if necessary, to assume that $\infty \in S$.

For each ordinal number $\alpha < m$ choose $a_\alpha \in C$ such that the transfinite sequence $(a_\alpha | \ \alpha < m)$ is linearly independent over $\mathbb{F}_p$. Each of the fields $E(z_\alpha)$ with $z_\alpha^p - z_\alpha = a_\alpha x$ is a cyclic extension of E of degree p. Moreover, $\mathrm{Branch}_x(E(z_\alpha)/E) = \{\infty\}$. Finally, the field extensions $E(z_\alpha)$, $\alpha < m$, of E are linearly disjoint.

Indeed, by the theory of Artin-Schreier, it suffices to prove that the set $\{a_\alpha x | \ \alpha < m\}$ is linearly independent over $\mathbb{F}_p$ modulo $\wp(E)$, where $\wp(y) = y^p - y$. Suppose that there exist relatively prime polynomials f and g in $C[x]$ such that $\sum_{\alpha<m} u_\alpha a_\alpha x = \frac{f(x)^p}{g(x)^p} - \frac{f(x)}{g(x)}$, with elements u_α in $\mathbb{F}_p$ which are zero for all but finitely many α. 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 $f(x) = \sum_{j=0}^n c_j x^j$ with $c_j \in C$ and $c_n \neq 0$. It follows that $\sum_{\alpha<m} u_\alpha a_\alpha x = \sum_{j=0}^n c_j^p x^{jp} - \sum_{j=0}^n c_j x^j$. Comparison of the coefficients of x^{jn} proves that $n = 0$ and $\sum_{\alpha<m} u_\alpha a_\alpha = 0$. Hence, by assumption, $u_\alpha = 0$ for each α. ∎

References

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

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

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

[HJ1] D. Haran and M. Jarden, *Regular split embedding problems over complete valued fields,* Forum Mathematicum **10** (1998), 329–351 .

[HJ2] D. Haran and M. Jarden, *Regular split embedding problems over function fields of one variable over ample fields,* Journal of Algebra, **208** (1998), 147–164.

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

[Has] H. Hasse, *Number Theory,* Grundlehren der Math. Wissenschaften **229**, Springer, Berlin, 1980.

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

[Ja2] M. Jarden, *The projectivity of the fundamental group of the affine line,* Turkish Journal of Mathematics, to appear.

[Lan] S. Lang, *Introduction to Algebraic Geometry,* Interscience Publishers, New York, 1958.

[Pop] F. Pop, *Étale Galois covers of affine smooth curves,* Inventiones mathematicae **120** (1995), 555–578.

[Ser] J.-P. Serre, *Construction de revêtements étales de la droite affine en caracteristique p,* Comptes Rendus de Académie des Sciences Paris **311** (1990), 341–346.