# The inverse Galois problem over formal power series fields

by

Moshe Jarden, Tel Aviv University

Israel Journal of Mathematics **85** (1994), 263–275.

## Introduction

The **inverse Galois problem** asks whether every finite group $G$ occurs as a Galois group over the field $\mathbb{Q}$ of rational numbers. We then say that $G$ is **realizable** over $\mathbb{Q}$. This problem goes back to Hilbert [Hil] who realized $S_n$ and $A_n$ over $\mathbb{Q}$. Many more groups have been realized over $\mathbb{Q}$ since 1892. For example, Shafarevich [Sha] finished in 1958 the work started by Scholz 1936 [Slz] and Reichardt 1937 [Rei] and realized all solvable groups over $\mathbb{Q}$. The last ten years have seen intensified efforts toward a positive solution of the problem. The area has become one of the frontiers of arithmetic geometry (see surveys of Matzat [Mat] and Serre [Se1]).

Parallel to the effort of realizing groups over $\mathbb{Q}$, people have generalized the inverse Galois problem to other fields with good arithmetical properties. The most distinguished field where the problem has an affirmative solution is $\mathbb{C}(t)$. This is a consequence of the Riemann Existence Theorem from complex analysis.

Winfried Scharlau and Wulf-Dieter Geyer asked what is the absolute Galois group of the field of formal power series $F = K((X_1, \ldots, X_r))$ in $r \geq 2$ variables over an arbitrary field $K$. The full answer to this question is still out of reach. However, a theorem of Harbater (Proposition 1.1a) asserts that each Galois group is realizable over the field of rational function $F(T)$. By a theorem of Weissauer (Proposition 3.1), $F$ is Hilbertian. So, $G$ is realizable over $F$. Thus, the inverse Galois problem has an affirmative solution over $F$.

The goal of this note is to prove the same result in a more general setting.

Theorem A: *Let $R$ be the valuation ring of a discrete Henselian field $K$, let $r$ be a positive integer, and let $F$ be the quotient field of $R[[X_1, \ldots, X_r]]$. Then every finite group $G$ is realizable over $F$.*

Corollary B:

(a) *Let $K_0$ be an arbitrary field and let $r \geq 2$. Then every finite group is realizable over $K_0((X_1,\ldots,X_r))$.*

(b) *Let $r \geq 1$ and let $F$ be the quotient field of $\mathbb{Z}_p[[X_1,\ldots,X_r]]$ of $\mathbb{Z}_{p,\mathrm{alg}}[[X_1,\ldots,X_r]]$. Then every finite group is realizable over $F$. Here $\mathbb{Z}_p$ is the ring of $p$-adic numbers and $\mathbb{Z}_{p,\mathrm{alg}}$ is the subring of all $p$-adic numbers which are algebraic over $\mathbb{Q}$.*

*Proof:* Apply Theorem A to $R = K_0[[X_1]]$, to $R = \mathbb{Z}_p$, and to $R = \mathbb{Z}_{p,\mathrm{alg}}$. ∎

The proof of Theorem A is a combination of several known results which we bring in this note.

Acknowledgement: The author is indebted to Wulf-Dieter Geyer and Dan Haran for their help to improve older versions of this note.

## 1. The theorem of Harbater and Liu

Let $K$ be a field and let $G$ be a finite group. We say that $G$ is **regular** over $K$ if there exists an absolutely irreducible polynomial $f \in K[T,X]$ which is Galois over $K(T)$ whose Galois group, namely, $\mathcal{G}(f(T,X),K(T))$ is isomorphic to $G$.

Alternatively, $K(T)$ has a Galois extension $F$ which is regular over $K$ such that $\mathcal{G}(F/K(T)) \cong G$.

We say that $G$ is **regular over $K$ with a rational point** if there exists a dominating Galois rational map of irreducible affine curves $\varphi: C \to \mathbb{A}^1$ defined over $K$ such that $C$ has a simple $K$-rational point and $\mathcal{G}(C/\mathbb{A}^1) \cong G$.

*Remark 1.1: Base field extension.* Note that if $G$ is regular over a field $K$, then it is regular over every extension $L$ of $K$. Indeed, we may take $F$ as free from $L$ and therefore as linearly disjoint from $L$ over $K$ [FrJ, Lemma 9.9].

Similarly, if $G$ is regular over $K$ with a rational point, then $G$ is regular with a rational point over each extension of $K$. ∎

The condition on $C$ to have a $K$-rational point implies that $F$ is regular over $K$. Thus, "$G$ is regular over $K$ with a rational point" implies that "$G$ is regular over $K$".

Indeed, let $E = K(T)$ be the function field of $\mathbb{A}^1$ and let $F$ be the function field of $C$ over $K$. By assumption, $F/E$ is Galois with $\mathcal{G}(F/E) \cong G$. Also, there exists a place $\varphi$: $F \to K \cup \{\infty\}$ over $K$ [JaR, Cor. A2]. It follows from the following well known lemma that $F/K$ is regular.

LEMMA 1.2: *Let $F/K$ be an extension of fields. If there exists a $K$-place $\varphi$: $F \to K \cup \{\infty\}$, then $F/K$ is regular.*

*Proof:* Indeed, let $w_1, \ldots, w_n \in \tilde{K}$ be linearly independent over $K$ and let $u_1, \ldots, u_n \in F$ such that $\sum_{i=1}^n u_i w_i = 0$ and not all $u_i$ are 0. Assume without loss that $\varphi(u_i/u_1) \in K$, $i = 1, \ldots, n$ and extend $\varphi$ to a $\tilde{K}$-place $\tilde{\varphi}$: $F\tilde{K} \to \tilde{K} \cup \{\infty\}$. Then apply $\tilde{\varphi}$ to $\sum_{i=1}^n \frac{u_i}{u_1} w_i = 0$ to get the relation $\sum_{i=1}^n \varphi\big(\frac{u_i}{u_1}\big) w_i = 0$. It follows that $1 = \varphi\big(\frac{u_1}{u_1}\big) = 0$. This contradiction proves that $F$ is linearly disjoint from $\tilde{K}$ over $K$. In other words, $F/K$ is regular. ∎

Suppose now that $K$ is an infinite field and that $\varphi$: $C \to \mathbb{A}^1$ is as above, with $C \subseteq \mathbb{A}^n$, $n \geq 2$. Then we may project $C$ from an appropriate point of $\mathbb{A}^n(K)$ onto a curve $C' \subseteq \mathbb{A}^2$ such that $C'$ is $K$-birationally equivalent to $C$ and the $K$-rational simple point of $C$ is mapped on a simple $K$-rational point of $C'$. Thus there exists an absolutely irreducible polynomial $f \in K[T, X]$ with $\mathcal{G}(f(T, X), K(T)) \cong G$ and there exists $a, b \in K$ such that $f(a, b) = 0$ and $\frac{\partial f}{\partial T}(a, b) \neq 0$ or $\frac{\partial f}{\partial X}(a, b) \neq 0$.

PROPOSITION 1.3: *Let $R$ be local integral domain with a quotient field $K$ such that $R \neq K$.*

(a) *(Harbater [Ha1, Thm. 2.3]) If $R$ is complete, then each finite group is regular over $K$ with a rational point.*

(b) *(Liu [Liu]) If $R$ is a complete discrete valuation ring, then each finite group $G$ is regular over $K$ with a rational point.*

*Remark 1.4: About the proofs of Harbater and Liu.*

(a) Harbater uses ‘mock covers’ and ‘Grothendieck’s existence theorem’ [GrD, (5.1.6)] in his proof. The rationality of the group over $K$ is not explicitly stated in [Ha1, Thm. 2.3], but it can be deduced from the properties of the ‘mock covers’.

(b) Liu [Liu] translates Harbater's method into 'rigid analytic geometry' for the case where $R$ is a complete discrete valuation ring. We prove however, that this special case of Harbater's result implies the more general theorem. ∎

Lemma 1.5: *Each complete local integral domain $R$ which is not a field contains a complete discrete valuation ring.*

*Proof:* Let $\mathfrak{m}$ be the maximal ideal of $R$. Suppose first that $\mathrm{char}(R) = 0$. Then $\mathbb{Z} \subseteq R$ and there are two possibilities:

Case A: $\mathbb{Z} \cap \mathfrak{m} \neq 0$. Then $\mathbb{Z} \cap \mathfrak{m} = p\mathbb{Z}$ for some prime number $p$. Since $R$ is complete, $\mathbb{Z}_p \subseteq R$.

Case B: $\mathbb{Z} \cap \mathfrak{m} = 0$. Since $R$ is not a field, there exists $0 \neq x \in \mathfrak{m}$. If $x$ were algebraic over $\mathbb{Q}$, then $a_n x^n + \cdots + a_1 x + a_0 = 0$ with $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ and $a_0 \neq 0$. But then $a_0 \in \mathbb{Z} \cap \mathfrak{m}$. This contradiction proves that $x$ is transcendental over $\mathbb{Q}$. It follows that $\mathbb{Q}[x] \subseteq R$ and $\mathbb{Q}[x] \cap \mathfrak{m} = x\mathbb{Q}[x]$. The completion of $\mathbb{Q}[x]$ with respect to $x$ is a discrete valuation ring which is contained in $R$.

Now suppose that $\mathrm{char}(R) = p$. Then $\mathbb{F}_p \cap \mathfrak{m} = 0$ and one continues as in Case B, replacing $\mathbb{Q}$ by $\mathbb{F}_p$. ∎

Corollary 1.6: *Proposition 1.3(b) implies Proposition 1.3(a).*

*Proof:* Let $R$ be as in Proposition 1.3. Lemma 1.5 gives a complete valuation subring $R_0$ of $R$. By Proposition 1.3(b), $G$ is regular over the quotient field of $R_0$ with a rational point. Hence $G$ is also regular over $K$ with a rational point. So, Proposition 1.3(a) is valid. ∎

## 2. Henselian fields

A field $K$ is **defectless** with respect to a valuation $v$ if each finite extension $L$ of $K$ satisfies

$$[L : K] = \sum_{w|v} e(w/v) f(w/v), \tag{1}$$

where $w$ ranges over all valuations of $L$ that extend $v$, $e(w/v)$ is the ramification index, and $f(w/v)$ is the relative residue degree of $w/v$. If $(K,v)$ is Henselian, then $v$ has a unique extension $w$ to $L$. In this case we write $e(L/K)$ (resp., $f(L/K)$) instead of $e(w/v)$ (resp., $f(w/v)$). Then condition (1) simplifies to

$$[L:K] = e(L/K)f(L/K) \tag{2}$$

For example, each complete discrete valued field $(K,v)$ is defectless [Rbn, p. 236].

LEMMA 2.1*: *Let $(K,v)$ be a defectless Henselian discrete valued field, and let $(\hat{K},\hat{v})$ be its completion. Then $\hat{K}/K$ is a regular extension.*

*Proof:* We have to prove that each finite extension $L$ of $K$ is linearly disjoint from $\hat{K}$ over $K$.

Indeed, as $\hat{K}/K$ is an immediate extension $e(\hat{K}/K) = 1$. Thus $e(\hat{K}L/\hat{K}) = e(\hat{K}L/K) = e(\hat{K}L/L)e(L/K) \geq e(L/K)$. Similarly we have $f(\hat{K}L/\hat{K}) \geq f(L/K)$ for the residue degrees. Hence, by (2)

$$[\hat{K}L:\hat{K}] \leq [L:K] = e(L/K)f(L/K) \leq e(\hat{K}L/\hat{K})f(\hat{K}L/\hat{K}) = [\hat{K}L:\hat{K}].$$

Thus $[\hat{K}L:\hat{K}] = [L:K]$. Conclude that $L$ is linearly disjoint from $\hat{K}$ over $K$. ∎

Suppose now that $v$ is a discrete valuation of $K$ (i.e., $v(K) = \mathbb{Z}$). Let $O$ be its valuation ring, let $L$ be a finite extension of $K$ and let $O'$ be the integral closure of $K$ in $L$. If $O'$ is a finitely generated $O$-module, then (1) holds [Se2, p. 26]. This is in particular the case if $L/K$ is separable [Se2, p. 24]. Hence, if $\mathrm{char}(K) = 0$, then $K$ is defectless with respect to $v$. If $K$ is a function field of one variable over a field $K_0$, and $v$ is a valuation of $K$ which is trivial on $K_0$, then there exists a finitely generated ring $R$ over $K_0$ and a prime ideal $\mathfrak{p}$ of $R$ such that $R_\mathfrak{p}$ is the valuation ring of $v$. Since the integral closure of $R$ in $L$ is finitely generated as an $R$-module [La1, p. 120], the same holds for $R_\mathfrak{p}$. It follows that $(K,v)$ is defectless.

* Lemmas 2.1 and 2.2 overlap with Lemma 2.13 and Corollary 2.14 of [Kul].

Lemma 2.2: *Let $(K,v)$ be a discrete Henselian valued field and let $(\hat{K},\hat{v})$ be the completion of $(K,v)$. Then $(K,v)$ is defectless in each of the following cases:*

(a) $\mathrm{char}(K)=0$.

(b) *$(K,v)$ is the Henselization of a valued field $(K_1,v_1)$, where $K_1$ is a function field of one variable over a field $K_0$ and $v_1$ is a valuation of $K_1$ which is trivial on $K_0$.*

*Hence, by Lemma 2.1, in each of these cases, $\hat{K}/K$ is a regular extension.*

*Proof:* By the paragraph that precedes the lemma, it suffices to consider only Case (b). Since (1) holds if $L/K$ is separable, it suffices to prove (2) only in the case where $L/K$ is a purely inseparable extension of degree $q$. Then there exists a finite extension $K_2$ of $K_1$ which is contained in $K$ and a finite purely inseparable extension $L_2$ of $K_2$ of degree $q$ such that $K\cap L_2=K_2$ and $KL_2=L$. Since $K_2$ is a function field of one variable over a finite extension of $K_0$, $K_2$ is defectless. Also $v_2=v|_{K_2}$ has a unique extension $w_2$ to $L_2$. Hence, $e(w_2/v_2)f(w_2/v_2)=q$.

Denote now the unique extension of $v$ to $L$ by $w$. Then $w|_{L_2}=w_2$. Since $(K,v)$ is also the Henselization of $(K_2,v_2)$, we have $f(L/K)\geq f(w_2/v_2)$ (actually both degrees are 1) and $e(L/K)\geq e(w_2/v_2)$. So,

$$q=[L:K]\geq e(L/K)f(L/K)\geq e(w_2/v_2)f(w_2/v_2)=q$$

and therefore (2) holds, as desired. ∎

Lemma 2.3: *Let $(K,v)$ be a Henselian valued field and let $(\hat{K},\hat{v})$ be its completion. Suppose that $\hat{K}/K$ is a regular extension. Then for each $0\neq g\in K[X_1,\ldots,X_n]$ each point $\mathbf{x}\in(\hat{K})^n$ with $g(\mathbf{x})\neq 0$ has a $K$-rational specialization $\mathbf{a}$ such that $g(\mathbf{a})\neq 0$. Thus $K$ is* **existentially closed** *in $\hat{K}$.*

*Proof:* Adding $g(\mathbf{x})^{-1}$ to $x_1,\ldots,x_n$ if necessary, we may assume that $g=1$. By assumption, $K(\mathbf{x})$ is a separable extension of $K$. Let $u_1,\ldots,u_r$ be a separating transcendence base for $K(\mathbf{x})/K$ and let $z$ be a primitive element for the finite separable extension $K(\mathbf{x})/K(\mathbf{u})$ which is integral over $K[\mathbf{u}]$. Then there exists an irreducible polynomial $f\in K[U_1,\ldots,U_r,Z]$ such that $f(\mathbf{u},z)=0$ and $f'(\mathbf{u},z)\neq 0$ (the prime stands for derivative with respect to $Z$). Also, $x_i=h_i(\mathbf{u},z)/h_0(\mathbf{u})$, for $h_i\in K[\mathbf{U},Z]$ and $0\neq h_0\in K[\mathbf{U}]$.

Since $(K, v)$ is dense in $(\hat{K}, \hat{v})$ we may approximate $u_1, \ldots, u_r, z$ by elements of $K$ to any desired degree. Since $K$ is Henselian, there exist $b_1, \ldots, b_r, c \in K$ such that $f(\mathbf{b}, c) = 0$ and $h_0(\mathbf{b}) \neq 0$. It follows that $(\mathbf{b}, c)$ is a $K$-specialization of $(\mathbf{u}, z)$.

Let now $a_i = h_i(\mathbf{b}, c)/h_0(\mathbf{b})$, $i = 1, \ldots, n$. Then $\mathbf{a}$ is a $K$-specialization of $\mathbf{x}$. ∎

LEMMA 2.4: *Let $K$ be an existentially closed subfield of a field $\hat{K}$. If a finite group $G$ is regular over $\hat{K}$ (resp., with a rational point), then $G$ is also regular over $K$ (resp., with a rational point).*

*Proof:* Suppose for example that $G$ is regular over $\hat{K}$ with a rational point. Then, there exists an absolutely irreducible polynomial $f \in \hat{K}[T, X]$ which is Galois and monic in $X$ such that $\mathcal{G}(f(T, X), \hat{K}(T)) \cong G$, and there exist $t, x \in \hat{K}$ such that $f(t, x) = 0$ and $\frac{\partial f}{\partial T}(t, x) \neq 0$ or $\frac{\partial f}{\partial X}(t, x) \neq 0$. Find $u_1, \ldots, u_n \in \hat{K}$ and a polynomial $g \in K(\mathbf{U})[T, X]$ such that $K[\mathbf{u}]$ is integrally closed, $g(\mathbf{u}, T, X) = f(T, X)$, $\mathcal{G}(g(\mathbf{u}, T, X), K(\mathbf{u}, T)) \cong G$, and there exist rational functions $p, q \in K(\mathbf{U})$ such that $t = p(\mathbf{u})$ and $x = q(\mathbf{u})$. By the Bertini-Noether theorem there exists $0 \neq h \in K(\mathbf{U})$ such that if a specialization $\mathbf{a}$ of $\mathbf{u}$ satisfies $h(\mathbf{a}) \neq 0$, then $g(\mathbf{a}, T, X)$ is well defined, Galois in $X$, and absolutely irreducible [FrJ, Prop. 9.29]. Also, $p(\mathbf{a})$ and $q(\mathbf{a})$ are well defined and $\frac{\partial f}{\partial T}(p(\mathbf{a}), q(\mathbf{a})) \neq 0$ or $\frac{\partial f}{\partial X}(p(\mathbf{a}), q(\mathbf{a})) \neq 0$. Choosing $h$ such that the discriminant of $g(\mathbf{a}, T, X)$ with respect to $X$ is nonzero, $\mathcal{G}(g(\mathbf{a}, T, X), K(\mathbf{a}))$ becomes isomorphic to a subgroup of $\mathcal{G}(g(\mathbf{u}, T, X), K(\mathbf{u}, T))$ [La2, p. 248, Prop. 15]. Since

$$\begin{aligned} |\mathcal{G}(g(\mathbf{a}, T, X), K(\mathbf{a}, T))| &= \deg_X g(\mathbf{a}, T, X) \\ &= \deg_X g(\mathbf{u}, T, X) = |\mathcal{G}(g(\mathbf{u}, T, X), K(\mathbf{u}, T))|, \end{aligned}$$

we have $\mathcal{G}(g(\mathbf{a}, T, X), K(\mathbf{a})) \cong G$. Since $K$ is existentially closed in $\hat{K}$, we can choose $\mathbf{a}$ in $K^n$. Hence $G$ is regular over $K$ with a rational point.

Similarly one proves that if $G$ is regular over $\hat{K}$, then it is also regular over $K$. ∎

THEOREM 2.5 (Florian Pop*): *Let $(F, w)$ be a Henselian valued field. Then every finite group $G$ is regular over $F$ with a rational point.*

* Communicated to the author by Peter Roquette.

*Proof:* It is implicit in our assumptions that $w$ is a nontrivial valuation.

CLAIM: $(F,w)$ *is an extension of a discrete Henselian valued field* $(K,v)$ *which satisfies the conclusion of Lemma 2.3.*

Suppose first that $\mathrm{char}(F)=0$ and that $w$ is nontrivial on $\mathbb{Q}$. Then $F_0=\tilde{\mathbb{Q}}\cap F$ is Henselian with respect to $w_0=w|_{F_0}$ [Jar, Cor. 11.2]. Hence, there exists $p$ such that $(F_0,w_0)$ is an extension of the Henselization $(\mathbb{Q}_{p,\mathrm{alg}},v_p)$ of $(\mathbb{Q},v_p)$, where $v_p$ denotes the $p$-adic valuation. Let $K=\mathbb{Q}_{p,\mathrm{alg}}$ and $v=v_p$.

Next suppose that $\mathrm{char}(F)=0$ and that $w$ is trivial on $\mathbb{Q}$. Then there exists $x\in F\smallsetminus\mathbb{Q}$ such that $w(x)\neq 0$. This element is transcendental over $\mathbb{Q}$. Thus $w$ induces a nontrivial valuation $v_0$ on $\mathbb{Q}(x)$. Then $F_0=\widetilde{\mathbb{Q}(x)}\cap F$ contains the Henselization $K$ of $\mathbb{Q}(x)$ with respect to $v_0$.

If $\mathrm{char}(F)=p$, then $w$ is trivial on $\mathbb{F}_p$. Hence, as in the preceding paragraph, there exists $x\in F$ which is transcendental over $\mathbb{F}_p$ such that $F$ contains a Henselization $K$ of $\mathbb{F}_p(x)$.

In each case Lemma 2.2 asserts that $(K,v)$ satisfies the conclusion of Lemma 2.3.

Let $\hat{K}$ be the completion of $K$ with respect to $v$. By Proposition 1.3b, $G$ is regular over $\hat{K}$ with a rational point. Hence, by Lemma 2.4, $G$ is regular over $F$ with a rational point. ∎

Recall that a field $K$ is **PAC** if each nonempty absolutely irreducible variety which is defined over $K$ has a $K$-rational point. Fried and Völklein [FV1] use complex analysis to prove that if $K$ is a PAC field of characteristic 0, then each finite group $G$ is regular over $K$. Völklein informed the author that the construction in [Voe] implies that $G$ is even regular over $K$ with a rational point. Pop has observed that the methods of this note imply the same result without any restriction on the characteristic:

THEOREM 2.6: *Let $K$ be a PAC field and let $G$ be a finite group. Then $G$ is regular over $K$ with a rational point.*

*Proof:* The field $\hat{K}=K((X))$ is regular over $K$, because the map $X\to 0$ extends to a place $\hat{K}\to K\cup\{\infty\}$ (Lemma 1.2). Since $K$ is PAC this implies that $K$ is existentially closed in $\hat{K}$ [FrJ, p. 139, Exer. 7]. By Proposition 1.3(b), $G$ is regular over $\hat{K}$ with a rational point. Hence, by Lemma 2.4, $G$ is regular also over $K$ with a rational point. ∎

## 3. Hilbertian fields

An integral domain $S$ with a quotient field $F$ is a **Krull domain** if $F$ has a family $\mathcal{V}$ of discrete valuations such that the intersection of their valuation rings is $S$ and for each $0 \neq a \in K$ there are only finitely many $v \in \mathcal{V}$ such that $v(a) \neq 0$. For example, each Dedekind domain is a Krull domain. Also, if $S$ is a Krull domain with a quotient field $F$, then the integral closure of $S$ in any finite extension of $F$, the polynomial ring $S[X]$, and the ring of power series $S[[X]]$ are again Krull domains [Bou, pp. 487, 489, and 547].

The **dimension** of $S$ is greater than 1, if $S$ has a maximal ideal $M$ which properly contains a nonzero prime ideal. ∎

PROPOSITION 3.1 (Weissauer [FrJ, Thm. 14.7]): *The quotient field of a Krull domain of dimension exceeding* 1 *is separably Hilbertian.*

*Example 3.2: Ring of formal power series.* Let $R$ be either a field or a discrete valuation ring with maximal ideal $\mathfrak{m}$. Then, $S = R[[X_1, \ldots, X_r]]$ is a Krull domain. Indeed, it is even a unique factorization domain [Bou, p. 511].

Consider the ideal $M$ of $S$ which consists of all power series $\sum_{i=0}^{\infty} f_i$, where $f_i \in R[X_1, \ldots, X_r]$ is a form of degree $i$, $f_0 = 0$ if $R$ is a field, and $f_0 \in \mathfrak{m}$ if $R$ is a discrete valuation ring. Since $S/M \cong R$ if $R$ is a field and $S/M \cong R/\mathfrak{m}$ if $R$ is a discrete valuation ring, $M$ is a maximal ideal. If $R$ is a field (resp., discrete valuation ring) and $r \geq 2$ (resp., $r \geq 1$), then $M$ contains the prime ideals generated by $X_1$ and by $X_2$ (resp., $\mathfrak{m}$ and by $X_1$) and neither of them is contained in the other. Hence $\dim(S) \geq 2$. It follows from Proposition 3.1 that the quotient field of $S$ is separably Hilbertian. ∎

THEOREM A: *Let $R$ be the valuation ring of a discrete Henselian field $K$, let $r$ be a positive integer, and let $F$ be the quotient field of $R[[X_1, \ldots, X_r]]$. Then every finite group $G$ is realizable over $F$.*

*Proof:* Let $G$ be a finite group. By Theorem 2.5, $G$ is regular over the quotient field of

$R$ with a rational point. Hence, $G$ is regular over $F$ with a rational point. In particular, $G$ is realizable over $F(T)$. By Example 3.2, $F$ is separably Hilbertian. Hence $G$ is realizable over $F$ [FrJ, Lemma 12.12]. ∎

*Remark 3.3: The case* $r = 1$. By Puiseux's theorem, $G(\mathbb{C}((X))) \cong \hat{\mathbb{Z}}$. Hence, only cyclic groups can be realized over $\mathbb{C}((X))$. Thus, Corollary B(a) is false for $r = 1$. ∎

*Remark 3.4: Cohomological dimension.* We have already mentioned that every finite group is realizable over $\mathbb{C}(t)$. Moreover, the absolute Galois group, $G(\mathbb{C}(t))$, of $\mathbb{C}(t)$ is even a free profinite group of uncountable rank [Rib, p. 70]. In particular, $G(\mathbb{C}(t))$ is projective, that is, of cohomological dimension 1. On the other hand, use the notation of Theorem A and assume that there exists a prime $p \neq \mathrm{char}(K)$ such that $1 \leq \mathrm{cd}_p(G(K)) < \infty$. Then, as we explain in the next paragraph, $\mathrm{cd}_p(G(F)) \geq r+1$. In particular, although every group is realizable over $F$, not every embedding problem for $G(F)$ is solvable.

Indeed, let $E$ be the quotient field of $R[[X_1, \ldots, X_{r-1}]]$. Induction on $r$ gives, $\mathrm{cd}(G(E)) \geq r$. Hence, $\mathrm{cd}(G(E((X_r))) \geq r+1$ [Rib, p. 277]. Also, $E \subseteq E(X_r) \subseteq F \subseteq E((X_r))$. By Krasner's lemma [Jar, Prop. 12.3] $E(X_r)_s E((X_r)) = E((X_r))_s$ ($L_s$ is the separable closure of a field $L$.) Hence $F_s E((X_r)) = E((X_r))_s$, and therefore, by Galois theory, $G(E((X_r)))$ is isomorphic to the closed subgroup $G(F_s \cap E((X_r))$ of $G(F)$. Conclude that $\mathrm{cd}(G(F)) \geq \mathrm{cd}_p(G(E((X_r))) \geq r+1$ [Rib, p. 204], as was to be shown. ∎

Denote the free profinite group of countable rank by $\hat{F}_\omega$.

*Example 3.5: A field $K$ over which every finite group is realizable but $\hat{F}_\omega$ is not realizable over $K$.*

Let $G_1, G_2, G_3, \ldots$ be a listing of all finite groups. Consider the direct product $G = \prod_{i=1}^{\infty} G_i$. Then $G$ is a profinite group of rank $\aleph_0$. Let $\varphi\colon \tilde{G} \to G$ be the universal Frattini cover of $G$. Then $\tilde{G}$ is projective [FrJ, Prop. 20.33] of rank $\aleph_0$ [FrJ, Cor. 20.26]. Hence, there exists an algebraic extension $K$ of $\mathbb{Q}$ which is PAC with $G(K) \cong \tilde{G}$. Then, each finite group is a quotient of $\tilde{G}$ and therefore it is realizable over $K$.

Assume now that $\hat{F}_\omega$ is realizable over $K$. Then, $\hat{F}_\omega$ is a quotient of $\tilde{G}$. It follows that there exists a Frattini cover $\varphi$ of $\hat{F}_\omega$ onto a quotient $\bar{G}$ of $G$ [FrJ, Lemma 20.35]. The kernel of $\varphi$ is contained in the Frattini subgroup of $\hat{F}_\omega$ which is trivial [FrJ, Cor. 24.8]. Hence, $\hat{F}_\omega \cong \bar{G}$ and therefore there exists an epimorphism $\alpha\colon G \to \hat{F}_\omega$. But for each $i$, $\alpha(G_i)$ is a finite subgroup of $\hat{F}_\omega$. Since $\hat{F}_\omega$ is torsion free, $\alpha(G_i) = 1$. Since the $G_i$ generate $G$, we obtain that $\hat{F}_\omega = \alpha(G) = 1$. This contradiction proves that $\hat{F}_\omega$ is not realizable over $K$.

Note that as $K$ is PAC, the latter conclusion implies, in view of a result of Fried and Völklein [FV2, Thm. A], that $K$ is not Hilbertian. So, our argement strengthen the one given in [Fv2, Sect. , Example]. ∎

Proposition 3.6 (W.-D. Geyer): *If $K$ is an algebraically closed field of characteristic 0 and $r \geq 2$, then $\hat{F}_\omega$ is realizable over $K((X_1, \ldots, X_r))$.*

*Proof:* Observe that $K\left(\frac{X_1}{X_2}\right) \subseteq K((X_1, \ldots, X_r))$. As $t = \frac{X_1}{X_2}$ is transcendental over $K$, the absolute Galois group of $K(t)$ is free of rank which is equal to the cardinality of $K$ [Rib, p. 70]. In particular $\hat{F}_\omega$ is a quotient of $G(K(t))$.* It follows from the next claim tht $\hat{F}_\omega$ is realizable over $K((X_1, \ldots, X_r))$.

Claim: *$K(t)$ is algebraically closed in $K((X_1, \ldots, X_r))$.* Indeed, consider an algebraic element $f \in K((X_1, \ldots, X_r))$ over $K(t)$. We prove that each prime divisor of $K(t)$ is unramified in $K(t, f)$. It will follow that $f \in K(t)$, [FrJ, Prop. 2.15], as desired.

To this end consider $c \in K$ and let $u = t - c$. Then $X_1 = X_2(u + c)$ and therefore

$$\begin{aligned} K(u) = K(t) \subseteq K((X_1, X_2, \ldots, X_r)) &\subseteq K((u, X_2, \ldots, X_r)) \\ &\subseteq K((u))((X_2, \ldots, X_r)) = F. \end{aligned}$$

The map $X_i \mapsto 0$, $i = 2, \ldots, r$, extends to a $K((u))$-place $\varphi\colon F \to K((u)) \cup \{\infty\}$ which extends further to a place $\varphi\colon \tilde{F} \to \widetilde{K((u))} \cup \{\infty\}$ which fixes each element of $\widetilde{K((u))}$. In particular, as $f \in \widetilde{K(u)} \cap F$, we have $f = \varphi(f) \in K((u))$. But $K((u))/K(t)$ is

* Florian Pop has recently announced a '$\frac{1}{2}$ Riemann existence theorem' from which the same result follows also if $\mathrm{char}(K) \neq 0$. If we use Pop's theorem, then Proposition 3.6 will hold for an arbitrary algebraically closed field.

unramified at the zero $(t-c)_0$ of $t-c$. So, $(t-c)_0$ is unramified in $K(t,f)$. Finally, replace $t$ by $\frac{X_2}{X_1}$ to conclude that also $(t)_\infty$ is unramified in $K(t,f)$, as desired. ∎

Example 3.5 and Proposition 3.6 naturally raise the following question:

PROBLEM 3.7: *Let $K$ be an arbitrary field and let $r \geq 2$. Is $\hat{F}_\omega$ realizable over $K((X_1,\ldots,X_r))$?*

*Remark 3.8:* Harbater [Ha2, Prop. 2.3] proves that if $O$ is the ring of integers of a number field $K$ and $F$ is the quotient field of $O[[X]]$, then every finite group $G$ is realizable over $F$. Moreover, $F$ has a Galois extension $\hat{F}$ which is regular over $K$ such that $\mathcal{G}(\hat{F}/F) \cong G$. Note that as $O$ is a Dedekind domain, $O[[X]]$ is a Krull domain of dimension at least 2. Hence, by Proposition 3.1, $F$ is Hilbertian. ∎

In view of Theorem A and Remarks 3.3 and 3.8 we may ask:

PROBLEM 3.8: *Let $O$ be a domain of characteristic* 0 *which is not a field. Denote the quotient field of $O[[X]]$ by $F$. Is every finite group realizable over $F$?* ∎

## References


[Bou] N. Bourbaki, *Elements of Mathematics, Commutative Algebra, Chapters 1–7,* Springer, Berlin, 1989.

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

[FV1] M. D. Fried and Helmut Völklein, *The inverse Galois problem and rational points on moduli spaces,* Mathemtische Annalen **209** (1991), 771–800.

[FV2] M. D. Fried and Helmut Völklein, The embedding problem over a Hilbertian PAC-field Annals of Mathemtics **135** (1992), 469–481.

[GrD] A. Grothendieck and J. Dieudonne, *Éléments de Géométrie Algébrique III,* Publications Mathématiques, IHES **11** (1961),

[Ha1] D. Harbater, *Galois coverings of the arithmetic line,* In Chundnovsky, D.V. et al. eds: Number Theory, New York 1984–1985, Springer, Berlin, 1987.

[Ha2] D. Harbater, *Mock covers and Galois extensions* Journal of Algebra **91** (1984), 281–293.

[Hil] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten,* Journal für die reine und angewandte Mathematik **110** (1892), 104–129.

[JaR] M. Jarden and Peter Roquette, *The Nullstellensatz over p-adically closed fields,* Journal of the Mathematical Society Japan **32** (1980), 425–460.

[Jar] M. Jarden, *Intersection of local algebraic extensions of a Hilbertian field (edited by Barlotti and all.),* NATO ASI Series C **333** 343–405, Kluwer, Dordrecht, 1991

[Kul] F.-V. Kuhlmann, *Henselian Function Fields and Tame Fields,* Manuscript, Heidelberg, 1990.

[La1] S. Lang, *Introduction to algebraic geometry,* Interscience Publishers, New York, 1958.

[La2] S. Lang, *Algebra,* Addison-Wesley, Reading, 1970.

[Liu] Q. Liu, *Tout groupe fini est un groupe de Galois sur $\mathbb{Q}_p(T)$,* manuscript, 1991.

[Mat] B. H. Matzat, *Der Kenntnisstand in der Konstruktiven Galoisschen Theorie,* manuscript, Heidelberg, 1990.

[Rei] H. Reichardt, *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung,* Journal für die reine und angewandte Mathematik **177** (1937), 1–5.

[Rbn] P. Ribenboim, *Théorie des valuations,* Les Presses de l'Université de Montréal, Montréal, 1964.

[Rib] L. Ribes, *Introduction to profinite groups and Galois Cohomology,* Queen's papers in pure and applied Mathematics **24**, Queen's University, Kingston, 1970.

[Se1] J.-P. Serre, *Topics in Galois Theory,* Jones and Barlett, Boston 1992

[Se2] J.-P. Serre, *Corps Locaux,* Hermann, Paris 1962.

[Sha] I.R. Shafarevich, *The imbedding problem for splitting extensions,* Dokl. Akad. Nauk SSSR **120** (1958), 1217–1219.

[Slz] Arnold Scholz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I.,* Mathematische Zeitschrift **42** (1936), 161–188.

[Voe] H. Völklein, *Moduli spaces for covers of the Riemann sphere,* Israel Journal of Mathematics