REGULAR SPLIT EMBEDDING PROBLEMS OVER COMPLETE VALUED FIELDS*

by

Dan Haran and Moshe Jarden**

School of Mathematical Sciences, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

e-mail: jarden@math.tau.ac.il and haran@math.tau.ac.il

Abstract

We give an elementary self-contained proof of the following result, which Pop proved with methods of rigid geometry.

THEOREM: *Let L_0/K_0 be a finite Galois extension of complete discrete valued fields. Let t be a transcendental element over K_0, let $K = K_0(t)$ and $L = L_0(t)$. Then each finite split embedding problem $G \to \mathcal{G}(L/K)$ over K has a solution field F which is regular over L_0.*

This gives a new proof of the theorem of Fried-Pop-Völklein:

THEOREM: *The absolute Galois group of a countable separably Hilbertian PAC field K is the free profinite group on countably many generators.*

Forum Mathematicum **10** (1998), 329–351

* This research was supported by The Israel Science Foundation administered by The Israel Academy of Sciences and Humanities.

** The second author wishes to express his gratitude to IWR and in particular to Heinrich Matzat for their kind hospitality while working on the paper.

Introduction

The main goal of this work is to give a new proof to the following result:

THEOREM A: *Every separably Hilbertian PAC field K is ω-free.*

Recall that K is **separably Hilbertian** if it satisfies the Hilbert irreducibility theorem with respect to irreducible polynomials $f(T, X)$ which are separable in X [FrJ, p. 147]. It is **PAC** if every nonvoid absolutely irreducible variety defined over K has a K-rational point. Finally, K is ω-**free** if each finite embedding problem over K is solvable. That is, given a finite Galois extension L/K and an epimorphism $\pi\colon G \to \mathcal{G}(L/K)$ from a finite group G, there exists a Galois extension N of K which contains L and there exists an isomorphism $\psi\colon \mathcal{G}(N/K) \to G$ such that $\pi \circ \psi = \mathrm{res}_L$.

Theorem A was stated as Open Problem 24.41 in [FrJ]. The problem was first solved for $\mathrm{char}(K) = 0$ by Fried and Völklein [FrV, p. 474], and then by Pop [Po1, Thm. 1] in the general case. Both Fried-Völklein and Pop use heavy analytical machinery in their proofs. Fried-Völklein use complex analytical methods, while Pop uses rigid analytical geometry.

Following [HaV], we propose here an elementary algebraic proof, which, together with [HaV], is self-contained and easy to access. The only rudiments from analysis we use are simple properties of fields of convergent power series over complete discrete valued fields, which we develop ad hoc.

To prove Theorem A, one first observes that K, as a PAC field, is existentially closed in the field $K((t))$ of formal power series in the variable t. The latter is complete with respect to a nontrivial ultrametric absolute value $|\ |$ having t as a prime element and K as a residue field. This reduces Theorem A to the following result (see also Lemma 6.2):

PROPOSITION B: *Let K_0 be a field complete with respect to a nontrivial ultrametric absolute value. Let x be transcendental over K_0. Then each* **finite constant split embedding problem** *over $K_0(x)$ has a* **rational solution**.

That is, let K be a finite Galois extension of K_0, with Galois group Γ. Suppose that Γ acts on a finite group G, and let pr$\colon G \rtimes \Gamma \to \Gamma$ *be the projection on Γ. Then $K_0(x)$ has*

a Galois extension F which contains K, there is an isomorphism $\psi\colon \mathcal{G}(F/K_0(x)) \to G \rtimes \Gamma$ such that $\mathrm{pr} \circ \psi = \mathrm{res}_K$, and F has a K-rational place.

For technical reasons the proof of Proposition B requires that the residue field of K_0 is infinite and K/K_0 is an unramified extension. However, the same reduction step from Proposition B to Theorem A removes these conditions and even leads to a quite general result:

THEOREM C: *Let K_0 be an ample field. Then each finite constant split embedding problem over $K_0(x)$ has a rational solution.*

We refer to §6 for a definition of 'ample field' and note here only that PAC fields, PRC fields, PpC fields, and Henselian fields are all ample.

Finally we note that Pop proves more than Proposition B: Let E be a function field of one variable over K_0. Then every finite split embedding problem over E has a regular solution [Po2, Thm. 2.7]*. That is, if F/E is a finite Galois extension, K is the algebraic closure of K_0 in F, and $\Gamma = \mathcal{G}(F/E)$ acts on a finite group G, then E has a Galois extension $\hat{F}$ which contains F, is regular over K, and there is an isomorphism $\theta\colon \mathcal{G}(\hat{F}/E) \to G \rtimes \Gamma$ such that $\mathrm{pr} \circ \theta = \mathrm{res}_F$. This stronger result is however not needed for the proof of Theorems A and C.

Theorem C and Pop's result are affirmative instances of the following general conjecture:

CONJECTURE D (Dèbes - Deschamps [DeD]): *Let E be a function field of one variable over an arbitrary field K_0. Then every finite split embedding problem over E has a regular solution.*

Note that Conjecture D gives a positive answer to the Inverse Galois Problem: Is every finite group realizable over $\mathbb{Q}$?

---

* This result does not appear in the later version [Po3].

1. Split embedding problems

A **finite split embedding problem** over a field E_0 is an epimorphism

$$\pi\colon G \rtimes \Gamma \to \Gamma \tag{1}$$

of finite groups, where $\Gamma = \mathcal{G}(E/E_0)$ is the Galois group of a Galois extension E/E_0, G is a finite group on which Γ acts, $G \rtimes \Gamma$ is the corresponding semidirect product, and π is the projection on Γ. A **solution** of (1) is a Galois extension F of E_0 which contains E and an isomorphism $\gamma\colon \mathcal{G}(F/E_0) \to G$ such that $\pi \circ \gamma = \mathrm{res}_E$. We propose a general setting in which the embedding problem is solvable.

The first step is to **realize** G over E. That is, to construct a Galois extension F of E with $\mathcal{G}(F/E) = G$. Assuming that we have already realized a set of subgroups of G (usually cyclic groups) which generate G, we 'patch' the realizations of these subgroups into a realization of G, as in [HaV].

Definition 1.1: Patching data. Let I be a finite set with $|I| \geq 2$. A **patching data**

$$\mathcal{E} = (E, F_i, Q_i, Q; G_i, G)_{i\in I}$$

consists of fields $E \subseteq F_i, Q_i \subseteq Q$ and finite groups $G_i \leq G$, $i \in I$, such that

(2a) F_i/E is a Galois extension with group G_i, $i \in I$;

(2b) $F_i \subseteq Q_i'$, where $Q_i' = \bigcap_{j\neq i} Q_j$, $i \in I$;

(2c) $\bigcap_{i\in I} Q_i = E$; and

(2d) $G = \langle G_i \mid i \in I\rangle$.

(2e) (Decomposition) Let $n = |G|$. 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 $B = B_1B_2$. ∎

We extend $\mathcal{E}$ by more fields and algebras. For each $i \in I$ let $P_i = F_iQ_i$ be the compositum of F_i and Q_i in Q. Conditions (2b) and (2c) imply that $F_i \cap Q_i = E$. Hence P_i/Q_i is a Galois extension with Galois group isomorphic (via the restriction of automorphisms) to $G_i = \mathcal{G}(F_i/E)$. Identify $\mathcal{G}(P_i/Q_i)$ with G_i via this isomorphism.

Consider the algebra

$$N = \mathrm{Ind}_1^G Q = \Big\{ \sum_{\theta\in G} a_\theta\theta \mid a_\theta \in Q\Big\}$$

of dimension $|G|$ over Q. Addition and multiplication are defined in N component-wise, Q is embedded diagonally in N, and G acts on N from the right:

$$\Big(\sum_{\theta\in G} a_\theta\theta\Big)^\sigma = \sum_{\theta\in G} a_\theta\sigma^{-1}\theta = \sum_{\theta\in G} a_{\sigma\theta}\theta, \qquad \sigma\in G. \tag{3}$$

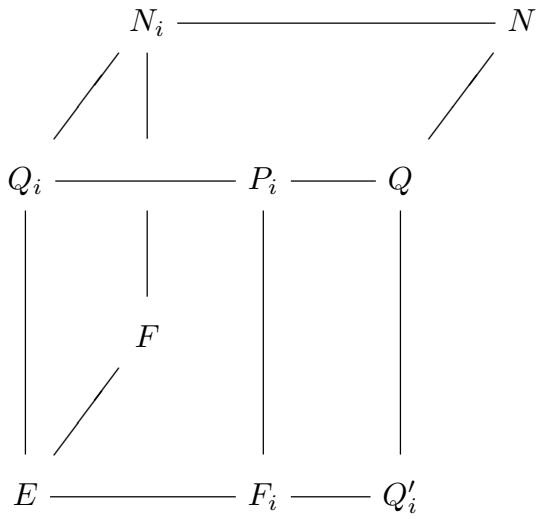
The action of G commutes with the addition and the multiplication in N.

For each $i\in I$ consider the following Q_i-subalgebra of N:

$$N_i = \mathrm{Ind}_{G_i}^G P_i = \Big\{ \sum_{\theta\in G} a_\theta\theta \in N \mid \ a_\theta\in P_i,\ a_\theta^\tau = a_{\theta\tau} \text{ for all } \theta\in G,\ \tau\in G_i\Big\}. \tag{4}$$

Then N_i is G-invariant, $N_i^G = Q_i$, and $\dim_{Q_i} N_i = \dim_Q N$ [HaV, Lemma 3.1]. It follows that $F = \bigcap_{i\in I} N_i$ is an E-algebra which is G-invariant. We call F the **co-compound** of the patching data $\mathcal{E}$, and consider the **patching diagram** associated with $\mathcal{E}$:

(5)



LEMMA 1.2: *There exists a basis of N over Q which is also a basis for N_i over Q_i, for each $i\in I$.*

Proof: For each subset J of I we find, by induction on $|J|$, a basis $\mathcal{V}_J$ of N over Q that is also a basis of N_i over Q_i, for each $i\in J$. For $J=I$ this will prove our assertion.

For $J=\emptyset$ there is nothing to be proved. Suppose that $|J|\geq 1$, choose $k\in J$, and let $J' = J\smallsetminus\{k\}$. By assumption there is a basis $\mathcal{V}_{J'}$ of N over Q that is also a basis of N_i over Q_i, for each $i\in J'$.

Remark 3.2 of [HaV] constructs a basis $\mathcal{V}_k$ of N over Q that is also a basis of N_k over Q_k. Hence there is a matrix $B \in \mathrm{GL}_n(Q)$ such that $\mathcal{V}_k B = \mathcal{V}_{J'}$. Condition (2e) gives $A \in \mathrm{GL}_n(Q_k)$ and $M \in \mathrm{GL}_n(Q'_k) \subseteq \mathrm{GL}_n(Q_i)$, for $i \in J'$, such that $B = AM$. Let $\mathcal{V}_J = \mathcal{V}_{J'} M^{-1}$. Then $\mathcal{V}_J$ is a basis of N over Q which is also a basis of N_i over Q_i, for each $i \in J'$. Moreover, $\mathcal{V}_J$ is also a basis of N_k over Q_k, because $\mathcal{V}_J = \mathcal{V}_k B M^{-1} = \mathcal{V}_k A$. So, the induction is complete. ∎

Lemma 1.2 asserts condition (COM) of [HaV]. Hence, the following consequence of [HaV, Prop. 3.4] is true:

Lemma 1.3:

(a) *F is a Galois field extension of E with Galois group G (via restriction from N);*

(b) *there is an E-embedding of F into Q.*

To solve the finite split embedding problem (1) we need a 'proper' action of Γ on the patching data.

Definition 1.4: Let E/E_0 be a finite Galois extension with Galois group Γ. Let $\mathcal{E}$ be a patching data (Definition 1.1). A **proper action** of Γ on $\mathcal{E}$ is a triple that consists of an action of Γ on the group G, an action of Γ on the field Q, and an action of Γ on the set I such that the following conditions hold:

(6a) The action of Γ on Q extends the action of Γ on E;

(6b) $F_i^\gamma = F_{i^\gamma}$, $Q_i^\gamma = Q_{i^\gamma}$, and $G_i^\gamma = G_{i^\gamma}$, for all $i \in I$ and $\gamma \in \Gamma$;

(6c) $(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma}$ for all $a \in F_i$, $\tau \in G_i$, $i \in I$, and $\gamma \in \Gamma$.

The action of Γ on G defines a semidirect product $G \rtimes \Gamma$ such that $\tau^\gamma = \gamma^{-1}\tau\gamma$ for all $\tau \in G$ and $\gamma \in \Gamma$. Let $\pi\colon G \rtimes \Gamma \to \Gamma$ be the canonical projection. ∎

Proposition 1.5: *Suppose that $\Gamma = \mathcal{G}(E/E_0)$ properly acts on the patching data $\mathcal{E}$. Then F/E_0 is Galois and there is an isomorphism $\psi\colon G \rtimes \Gamma \to \mathcal{G}(F/E_0)$ such that $\mathrm{res}_E \circ \psi = \pi$.*

Proof: We break the proof of the proposition into three parts.

PART A: *The action of* Γ *on* F. The actions of Γ on Q and on G combine to an action of Γ on the Q-algebra N:

$$\Big(\sum_{\theta\in G} a_\theta\theta\Big)^\gamma = \sum_{\theta\in G} a_\theta^\gamma\theta^\gamma \qquad a_\theta\in Q,\ \gamma\in\Gamma. \tag{7}$$

Let $i\in I$ and $\gamma\in\Gamma$. Then $P_i = Q_iF_i$, and hence, by (6b), $P_i^\gamma = P_{i^\gamma}$. Moreover, we have identified $\mathcal{G}(P_i/Q_i)$ with $G_i = \mathcal{G}(F_i/E)$ via restriction. Hence, by (6b), for all $a\in Q_i$ and $\tau\in G_i$, we have $(a^\tau)^\gamma = a^\gamma = (a^\gamma)^{\tau^\gamma}$. This, together with (6c), gives

$$(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma} \quad \text{for all } a\in P_i \text{ and } \tau\in G_i. \tag{8}$$

Next, we claim that $N_i^\gamma = N_{i^\gamma}$. Indeed, if $a = \sum_{\theta\in G} a_\theta\theta \in N_i$, then $a_\theta\in P_i$ and $a_\theta^\tau = a_{\theta\tau}$ for all $\theta\in G$ and $\tau\in G_i$. By (7), $a^\gamma = \sum_{\theta\in G} b_\theta\theta$ where $b_\theta = a^\gamma_{\theta^{\gamma^{-1}}}\in P_{i^\gamma}$. For each $\sigma\in G_{i^\gamma}$ there exists $\tau\in G_i$ such that $\sigma = \tau^\gamma$. Hence, by (8),

$$b_\theta^\sigma = \big(a^\gamma_{\theta^{\gamma^{-1}}}\big)^{\tau^\gamma} = \big(a^\tau_{\theta^{\gamma^{-1}}}\big)^\gamma = a^\gamma_{\theta^{\gamma^{-1}}\tau} = a^\gamma_{(\theta\tau^\gamma)^{\gamma^{-1}}} = b_{\theta\sigma},$$

and therefore $a^\gamma\in N_{i^\gamma}$. This proves that $N_i^\gamma\subseteq N_{i^\gamma}$. Applying this rule to i^γ and γ^{-1} instead of to i and γ, we get $N_{i^\gamma}^{\gamma^{-1}}\subseteq N_i$. Hence $N_{i^\gamma}\subseteq N_i^\gamma$. So, $N_i^\gamma = N_{i^\gamma}$, as asserted.

Thus, γ permutes the N_i's and therefore $F^\gamma = F$. It follows that (7) gives an action of Γ on F.

PART B: *The action of* $G\rtimes\Gamma$ *on* F. Let $a = \sum_{\theta\in G} a_\theta\theta\in N$, let $\gamma\in\Gamma$, and let $\sigma\in G$. Then, by (7) and (3),

$$\Big(\big(a^{\gamma^{-1}}\big)^\sigma\Big)^\gamma = \Big(\big(\sum_{\theta\in G} a_\theta^{\gamma^{-1}}\theta^{\gamma^{-1}}\big)^\sigma\Big)^\gamma = \Big(\sum_{\theta\in G} a_\theta^{\gamma^{-1}}\sigma^{-1}\theta^{\gamma^{-1}}\Big)^\gamma = \sum_{\theta\in G} a_\theta(\sigma^\gamma)^{-1}\theta = a^{\sigma^\gamma}.$$

It follows that the actions of Γ and G on N combine to an action of $G\rtimes\Gamma$ on N. As both Γ and G leave F invariant, $G\rtimes\Gamma$ acts on F.

PART C: *Conclusion of the proof.* As $F^G = E$ and $E^\Gamma = E_0$, we have $F^{G\rtimes\Gamma} = E_0$. Furthermore $[F:E_0] = [F:E]\cdot[E:E_0] = |G|\cdot|\Gamma| = |G\rtimes\Gamma|$. By Galois theory, $\mathcal{G}(F/E_0) = G\rtimes\Gamma$ and the restriction res: $\mathcal{G}(F/E_0)\to\mathcal{G}(E/E_0)$ coincides with the canonical map $\pi\colon G\rtimes\Gamma\to\Gamma$. ∎

2. Ultrametric valued rings

We will construct patching data over fields $K(x)$, where K is a complete ultrametric valued field. The 'analytic' fields Q_i will be the quotient fields of certain rings of convergent power series in several variables over K. At a certain point in a proof by induction we will consider a ring of convergent power series in one variable over a complete ultrametric valued ring. So, we start by recalling the definition and properties of the latter rings.

Let A be a commutative ring with unity equipped with a **nontrivial ultrametric absolute value** $|\ |$. That is, $a \mapsto |a|$ is a map $A \to \mathbb{R}$ satisfying:

(1a) $|a| \geq 0$, and $|a| = 0$ if and only if $a = 0$;

(1b) there is $a \in A$ with $0 < |a| < 1$;

(1c) $|ab| = |a| \cdot |b|$; and

(1d) $|a + b| \leq \max(|a|, |b|)$.

By (1a) and (1c), A is an integral domain. By (1c), the absolute value of A extends to an absolute value on the quotient field of A (by $|\frac{a}{b}| = \frac{|a|}{|b|}$). It also follows that $|-a| = |a|$, and

(1d′) if $|a| < |b|$, then $|a + b| = |b|$.

Assume, furthermore, that

(1e) A is **complete with respect to** $|\ |$, i.e., every Cauchy sequence in A converges.

It then follows from (1d) that a series $\sum_{n=0}^{\infty} a_n$ of elements of A converges if and only if $a_n \to 0$. Also, if $a_n \to a$ and $a \neq 0$, then $|a_n| = |a|$ for large n.

Let $A[[x]]$ the ring of formal power series in the variable x over A. Consider the following subring of $A[[x]]$:

$$A\{x\} = \Big\{ \sum_{n=0}^{\infty} a_n x^n \| a_n \in A, \quad \lim_{n\to\infty} a_n = 0 \Big\}. \tag{2}$$

Definition 2.1: For $f = \sum_{n=0}^{\infty} a_n x^n \in A\{x\}$ let $|f| = \max |a_n|$. If $f \neq 0$, we define the **pseudodegree** of f to be the integer $d = \max\{n \geq 0 \,|\ |a_n| = |f|\}$. If a_d is invertible in A, we call f **regular**. In particular, if A is a field, then each $0 \neq f \in A\{x\}$ is regular. ∎

By [HaV, Lemma 1.3], $(A\{x\}, |\ |)$ is a complete ultrametric valued ring. Using an analog of Weierstraß' division theorem, [HaV] proves the following result, which, among others, implies that if A is a field, then $A\{x\}$ is a principal ideal domain.

LEMMA 2.2 ([HaV, Cor. 1.7]): *Let $f \in A\{x\}$ be regular of pseudodegree d. Then $f = qg$, where q is a unit of $A\{x\}$ and $g \in A[x]$ is a monic polynomial of degree d with $|g| = 1$.*

3. Rings of convergent power series of several variables

Let $E = K(x)$ be the field of rational functions in the variable x over a field K. Let I be a nonempty finite set. For each $i \in I$ let c_i be an element of K. Assume that $c_i \neq c_j$ if $i \neq j$. For each $i \in I$ let $w_i = \frac{1}{x-c_i} \in K(x)$.

LEMMA 3.1:

(a) *For all $i \neq j$ in I and for each nonnegative integer m*

$$w_i w_j^m = \frac{w_i}{(c_i - c_j)^m} - \sum_{k=1}^{m} \frac{w_j^k}{(c_i - c_j)^{m+1-k}}. \tag{1}$$

(b) *Given nonnegative integers m_i, $i \in I$, not all zero, there exist $a_{ik} \in K$ such that*

$$\prod_{i \in I} w_i^{m_i} = \sum_{i \in I} \sum_{k=1}^{m_i} a_{ik} w_i^k. \tag{2}$$

(c) *Every $f \in K[w_i \mid i \in I]$ can be uniquely written as*

$$f = a_0 + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in} w_i^n \tag{3}$$

where $a_0, a_{in} \in K$ and almost all of them are zero.

Proof of (a) and (b): Starting with the identity

$$w_i w_j = \frac{w_i}{c_i - c_j} + \frac{w_j}{c_j - c_i} \tag{4}$$

one proves (1) by induction on m. Then one proceeds by induction on $|I|$ and $\max_{i \in I} m_i$ to prove (2).

Proof of (c): The existence of the presentation (3) follows from (b). To prove the uniqueness we assume that $f = 0$ in (3) but $a_{jk} \neq 0$ for some $j \in I$ and $k \in \mathbb{N}$. Then, $\sum_{n=1}^{\infty} a_{jn} w_j^n = -a_0 - \sum_{i \neq j} \sum_{n=1}^{\infty} a_{in} w_i^n$. The left hand side has a pole at c_j while the right hand side has not. This is a contradiction. ∎

From now on we assume that K is complete with respect to a nontrivial ultrametric absolute value $|\ |$, as in §2. Furthermore assume that

$$|c_i| \leq |c_i - c_j| = 1 \text{ for all } i, j \in I,\ i \neq j. \tag{5}$$

Let $E = K(x)$ be the field of rational functions over K in the variable x. Then $|\sum a_n x^n| = \max_n |a_n|$, $a_n \in K$, extends $|\ |$ to an ultrametric absolute value of $K[x]$, which further extends to E. Let $\hat{E}$ be the completion of E with respect to $|\ |$ [CaF, p. 47].

We proceed to define rings of convergent power series of several variables over E. In the language of rigid geometry, these are the rings of holomorphic functions on the complements in the projective line $\mathbb{P}^1(K)$ of finitely many open discs. Quotient fields of these rings will be our 'analytic' fields Q_i in a patching data over E that we start to assemble.

Remark 3.2: (a) $|x| = |w_i| = 1$ for each $i \in I$.

(b) Let $\bar{K} \subseteq \bar{E}$ be the residue fields of $K \subseteq E$ with respect to $|\ |$. Denote the image in $\bar{E}$ of an element $g \in K(x)$ with $|g| \leq 1$ by $\bar{g}$. Then $\bar{x}$ is transcendental over $\bar{K}$. Indeed, let h be a monic polynomial over $\bar{K}$. Lift it to a monic polynomial p with coefficients in the valuation ring of K such that $\bar{p} = h$. As $|p(x)| = 1$, we have $\bar{p}(\bar{x}) \neq 0$. It follows that $\bar{E} = \bar{K}(\bar{x})$ is the field of rational functions over $\bar{K}$ in the variable $\bar{x}$.

(c) If $|\ |'$ is an extension of the absolute value $|\ |$ of K to E such that the residue x' of x with respect to $|\ |'$ is transcendental over $\bar{K}$, then $|\ |'$ coincides with $|\ |$.

Indeed, let $p(x) = \sum a_n x^n$ be a nonzero polynomial in $K[x]$. Let $|a_d| = \max |a_n|$. Then $(a_d^{-1} p(x))' = \sum (a_d^{-1} a_n)'(x')^n \neq 0$ (the prime indicates the residue with respect to $|\ |'$) and therefore $|a_d^{-1} p(x)|' = 1$. So, $|p(x)|' = |a_d| = |p(x)|$.

(d) It follows from (c) that if γ is an automorphism of E that leaves K invariant, preserves the absolute value of K, and $\overline{x^\gamma}$ is transcendental over $\bar{K}$, then γ preserves the absolute value of E.

(e) In particular, suppose that K is a finite Galois extension of a complete field K_0 with respect to $|\ |$. Let $\gamma \in \mathcal{G}(K/K_0)$ and extend γ in the unique possible way to an element $\gamma \in \mathcal{G}(E/K_0(x))$. Then γ preserves $|\ |$ on K [CaF, p. 56] and $x^\gamma = x$. By (d), γ preserves $|\ |$ also on E.

(f) Now suppose that $y = \frac{ax+b}{cx+d}$ with $a, b, c, d \in K$ such that $|a|, |b|, |c|, |d| \leq 1$ and $\bar{a}\bar{d} - \bar{b}\bar{c} \neq 0$. Then $\bar{a}\bar{x} + \bar{b}$ and $\bar{c}\bar{x} + \bar{d}$ are nonzero elements of $\bar{K}(\bar{x})$ and therefore

$\bar{y} = \frac{\bar{a}\bar{x}+\bar{b}}{\bar{c}\bar{x}+\bar{d}} \in \bar{K}(\bar{x})$. Moreover, $\bar{K}(\bar{x}) = \bar{K}(\bar{y})$ and therefore $\bar{y}$ is transcendental over $\bar{K}$. Conclude from (c) that the unique K-automorphism of $K(x)$ given by $x \mapsto y$ preserves the absolute value.

(g) For f as in (3) we have $|f| = \max_{i,n}\{|a_0|, |a_{in}|\}$. Indeed, we may assume that $f \neq 0$. Divide f by the coefficient with the maximal absolute value, if necessary, to assume that $\max_{i,n}\{|a_0|, |a_{in}|\} = 1$. By (a), $|f| \leq 1$. Thus

$$\bar{f} = \bar{a}_0 + \sum_{i\in I}\sum_{n=1}^{\infty} \bar{a}_{in}\bar{w}_i^n.$$

with $\bar{a}_0, \bar{a}_{in} \in \bar{K}$ almost all, but not all, zero. Note that $\bar{w}_i = \frac{1}{\bar{x}-\bar{c}_i}$ for $i \in I$, and $\bar{c}_i \neq \bar{c}_j$ (by (5)), if $i \neq j$. By (b), $\bar{x}$ is transcendental over $\bar{K}$. By Lemma 3.1, applied to $\bar{K}$ and $\bar{x}$ instead of to K and x, we have $\bar{f} \neq 0$. Therefore $|f| = 1$.

(h) Multiply $w_j^{-1} - w_i^{-1} = c_i - c_j$ by w_i to get that

$$\frac{w_i}{w_j} = 1 + (c_i - c_j)w_i$$

is in $K[w_i]$. Similarly, $\frac{w_j}{w_i} \in K[w_j]$. Hence $\frac{w_i}{w_j}$ is invertible in $K[w_i, w_j]$. ∎

Let $R = K\{w_i \mid i \in I\}$ be the closure of $K[w_i \mid i \in I]$ in $\hat{E}$. Our first result gives a Mittag-Leffler decomposition of each $f \in R$ (cf. [FrP, p. 7] for K algebraically closed).

LEMMA 3.3: *The ring R is the completion of $K[w_i \mid i \in I]$ with respect to the absolute value. In particular, $|\ |$ is a nontrivial complete ultrametric absolute value on R. Each element f of R has a unique presentation as a multiple power series:*

$$f = a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in}w_i^n, \tag{6}$$

where $a_0, a_{in} \in K$, and $|a_{in}| \to 0$ as $n \to \infty$. Moreover, $|f| = \max_{i,n}\{|a_0|, |a_{in}|\}$.

Proof: Each f as in (6) is a well defined element of $\hat{E}$. The partial sums $f_d = a_0 + \sum_{i\in I}\sum_{n=1}^{d} a_{in}w_i^n$ belong to $K[w_i \mid i \in I]$ and converge to f. Hence $f \in R$. By Remark 3.2(g), $|f_d| = \max_{i,n}\{|a_0|, |a_{in}|\}$ for each sufficiently large d. Hence, $|f| = \max_{i,n}\{|a_0|, |a_{in}|\}$.

Therefore, if $g_k = a_{k,0} + \sum_{i\in I}\sum_{n=1}^{\infty} a_{k,in}w_i^n$, $k = 1,2,3,\ldots$, form a Cauchy sequence in R, then, each of the sequences $\{a_{k,0} \mid k = 1,2,3,\ldots\}$ and $\{a_{k,in} \mid k = 1,2,3,\ldots\}$ is Cauchy. Since K is complete, $a_{k,0} \to a_0$ and $a_{k,in} \to a_{in}$ for some $a_0, a_{in} \in K$. Let f be as in (6). Then, $|a_{in}| \to 0$ and $g_k \to f$.

The uniqueness of the presentation (6) is a consequence of Remark 3.2(g). ∎

Remark 3.4: Let $K\{x\}$ be the closure of $K[x]$ in the completion $\hat{E}$ of E. By [HaV, §1], $K\{x\}$ consists of all convergent power series $f = \sum_{n=0}^{\infty} a_n x^n$, with $a_n \in K$, $a_n \to 0$ as $n \to \infty$, and $|f| = \max\{|a_n|\}_{n\geq 0}$.

Let $i \in I$. By Remark 3.2(f), the map $x \mapsto w_i$ extends to a K-automorphism α of $K(x)$ which preserves $|\ |$. As α maps $K[x]$ onto $K[w_i]$, its restriction to $K[x]$ extends to an isomorphism of the completions $K\{x\} \to K\{w_i\}$. Extend this isomorphism to an isomorphism of the quotient fields. The latter isomorphism extends α. ∎

Call the partial sum in (6), $\sum_{n=1}^{\infty} a_{in}w_i^n$, the ***i*-component** of f.

Remark 3.5: Each $c \in K$ with $|c| > 1$ defines an **evaluation homomorphism** $R \to K$ given by

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

Indeed, $|\frac{1}{c-c_i}| = \frac{1}{|c|} < 1$. ∎

LEMMA 3.6 (Degree shifting): *Let $f \in R$ be given by (6). Fix $i \neq j$ in I. Let $\sum_{n=1}^{\infty} a'_{in}w_i^n$ be the i-component of $\frac{w_j}{w_i}f \in R$. Then*

$$a'_{in} = -\sum_{r=n+1}^{\infty} \frac{a_{ir}}{(c_j - c_i)^{r-n}} \qquad n = 1,2,3,\ldots \tag{7}$$

Furthermore, let $m \geq 1$ be an integer, and let $\sum_{n=1}^{\infty} b_{in}w_i^n$ be the i-component of $(\frac{w_j}{w_i})^m f$. Let $\epsilon \geq 0$ be a real number and let d be a positive integer.

(a) *If $|a_{in}| \leq \epsilon$ for each $n \geq d+1$, then $|b_{in}| \leq \epsilon$ for each $n \geq d+1-m$.*

(b) *Let $d > m$. If $|a_{in}| < \epsilon$ for each $n \geq d+1$ and $|a_{id}| = \epsilon$, then $|b_{in}| < \epsilon$ for each $n \geq d+1-m$ and $|b_{i,d-m}| = \epsilon$.*

(c) $\sum_{n=1}^{\infty} a_{in} w_i^n$ *is a polynomial in* w_i *if and only if* $\sum_{n=1}^{\infty} b_{in} w_i^n$ *is.*

Proof: By Remark 3.2(h), $\frac{w_j}{w_i} f \in R$. So, the above statements make sense.

PROOF OF (7): We may assume that $a_0 = a_{i1} = 0$ and $a_{kr} = 0$ for each $k \neq i$ and each r. Indeed, $\frac{w_j}{w_i} = 1 + (c_j - c_i) w_j \in K\{w_j\}$. Hence, by (1), $\frac{w_j}{w_i} \cdot w_k^r \in K\{w_l \mid l \neq i\}$. Furthermore, $\frac{w_j}{w_i} \cdot w_i = w_j \in K\{w_l \mid l \neq i\}$. Hence a_0, a_{i1} and the a_{kr} do not contribute to the i-component of $\frac{w_j}{w_i} f$.

Thus $f = \sum_{r=2}^{\infty} a_{ir} w_i^r$. Hence, by (1),

$$\begin{aligned} \frac{w_j}{w_i} f &= \sum_{r=2}^{\infty} a_{ir} w_j w_i^{r-1} = \sum_{r=2}^{\infty} a_{ir} \big[\frac{w_j}{(c_j - c_i)^{r-1}} - \sum_{n=1}^{r-1} \frac{w_i^n}{(c_j - c_i)^{r-n}} \big] \\ &= \sum_{r=2}^{\infty} \frac{a_{ir}}{(c_j - c_i)^{r-1}} w_j - \sum_{n=1}^{\infty} \sum_{r=n+1}^{\infty} \frac{a_{ir}}{(c_j - c_i)^{r-n}} w_i^n \end{aligned},$$

from which (7) follows.

PROOF OF (a) AND (b): By induction on m it suffices to assume that $m = 1$. In this case we have to prove: (a) If $|a_{in}| \leq \varepsilon$ for each $n \geq d+1$, then $|a'_{in}| \leq \varepsilon$ for each $n \geq d$; (b) assuming $d \geq 2$, if $|a_{in}| < \varepsilon$ for each $n \geq d+1$ and $|a_{id}| = \varepsilon$, then $|a'_{in}| < \varepsilon$ for each $n \geq d$ and $|a'_{i,d-1}| = \varepsilon$. By (5), $|c_i - c_j| = 1$. Hence, (a) follows from (7) with $n = d, d+1, d+2, \ldots$ and (b) follows from (7) with $n = d-1, d, d+1, \ldots$.

PROOF OF (c): Again, it suffices to prove that $\sum_{n=1}^{\infty} a_{in} w_i^n$ is a polynomial if and only if $\sum_{n=1}^{\infty} a'_{in} w_i^n$ is a polynomial.

If $\sum_{n=1}^{\infty} a_{in} w_i^n$ is a polynomial, then $|a_{in}| = 0$ for all large n. It follows from (a), with $\varepsilon = 0$, that $|a'_{i,n-1}| = 0$ for all large n. Hence, $\sum_{n=1}^{\infty} a'_{in} w_i^n$ is a polynomial.

If $\sum_{n=1}^{\infty} a_{in} w_i^n$ is not a polynomial, then for each d_0 there exists $d > d_0$ such that $a_{id} \neq 0$. Increasing d, if necessary, we may assume that $|a_{in}| < |a_{id}|$ for each $n \geq d+1$. By (b), $|a'_{i,d-1}| = |a_{id}|$ and therefore $a'_{i,d-1} \neq 0$. Conclude that $\sum_{n=1}^{\infty} a'_{in} w_i^n$ is not a polynomial. ∎

LEMMA 3.7 (cf. [FrP, Thm. I.2.2]): *Let* $j \in I$. *Then each* $f \in R$ *can be written as* $f = pu$ *with* $p \in K[w_j]$ *and* $u \in R^{\times}$.

Proof: Assume that $f \neq 0$. If $|I| = 1$, then f is regular (Definition 2.1) and the claim follows from Lemma 2.2. Suppose therefore that $|I| \geq 2$ and continue by induction.

Write f in the form (6). Take $d' \geq 1$ such that $|a_{jn}| \leq |f|/2$ for all $n \geq d' + 1$. By Lemma 3.6(a) we may assume that $|a_{jn}| < |f|$ for all $n \geq 1$, otherwise choose $i \in I$, $i \neq j$, and multiply f by $(\frac{w_i}{w_j})^{d'}$. (As $|\frac{w_i}{w_j}| = 1$, this does not change $|f|$.) Thus we are either in Case I or Case II below:

CASE I: *$|a_0| = |f| > |a_{in}|$ for all i and n.* Multiply f by a_0^{-1} to assume that $a_0 = 1$. Hence $|1 - f| < 1$. By [HaV, Remark 1.1], $f \in R^\times$, and we are done.

CASE II: *There exist $i \in I \smallsetminus \{j\}$ and $d \geq 1$ such that $|a_{id}| = |f|$.* Increase d, if necessary, to assume that $|a_{in}| < |a_{id}| = |f|$ for all $n \geq d+1$. By Lemma 3.6(b) we may assume that $d = 1$, otherwise multiply f by $(\frac{w_j}{w_i})^{d-1}$.

Introduce a new variable w, and consider the ring $A\{w\}$ of convergent power series in w over the subring $A = K\{w_k \mid k \neq i\}$ of R. Since $a_{i1} \in K^\times$, the element

$$\hat{f} = (a_0 + \sum_{k \neq i} \sum_{n=1}^{\infty} a_{kn} w_k^n) + \sum_{n=1}^{\infty} a_{in} w^n$$

of $A\{w\}$ is regular of pseudodegree 1. By Lemma 2.2 (with w instead of x) we have $\hat{f} = \hat{p}\hat{u}$, where $\hat{u}$ is a unit of $A\{w\}$ and $\hat{p} = h + w$ for some $h \in A$.

We have $|w_i| = 1$. The homomorphism θ: $A\{w\} \to R$ defined by $\sum c_n w^n \mapsto \sum c_n w_i^n$, with $c_n \in A$, maps $\hat{u}$ onto a unit u' of R. Thus $f = \theta(\hat{f}) = \theta(\hat{p})\theta(\hat{u}) = (h + w_i)u' = g \cdot \frac{w_i}{w_j} u'$, where

$$g = (h + w_i)\frac{w_j}{w_i} = h(1 + (c_j - c_i)w_j) + w_j \in A$$

and $\frac{w_i}{w_j} u' \in R^\times$ (Remark 3.2(h)). Apply the induction hypothesis on g to conclude the proof. ∎

COROLLARY 3.8: *Let $0 \neq g \in R$. Then $K[w_i \mid i \in I] + gR = R$.*

Proof: As $R = \sum_{i \in I} K\{w_i\}$ and $K[w_i \mid i \in I] = \sum_{i \in I} K[w_i]$, it suffices to show for each $i \in I$ and for every $f \in K\{w_i\}$ that there is $r \in K[w_i]$ such that $f - r \in gR$. By Lemma 3.7 we may assume that $g \in K[w_i]$. By Remark 3.4 there is a K-isomorphism

$K\{x\} \to K\{w_i\}$ that maps $K[x]$ onto $K[w_i]$. Therefore the assertion follows from Weierstraß' division theorem [HaV, Theorem 1.6] for the ring $K\{x\}$. ∎

The next result appears in [FrP, p. 67] for K algebraically closed.

PROPOSITION 3.9: *The ring $R = K\{w_i \mid i \in I\}$ is a principal ideal domain. For each $i \in I$, each ideal of R is generated by an element of $K[w_i]$.*

Proof: By Lemma 3.7, each ideal $\mathfrak{a}$ of R is generated by the ideal $\mathfrak{a} \cap K[w_i]$ of $K[w_i]$. Since $K[w_i]$ is a principal ideal domain, $\mathfrak{a} \cap K[w_i] = pK[w_i]$ for some $p \in K[w_i]$. Conclude that $\mathfrak{a} = pR$ is a principal ideal. ∎

Denote the quotient field of R by Q. For a nonempty subset J of I consider $R_J = K\{w_i \| i \in J\}$ as an absolute valued subring of $R = R_I$. Let $Q_J = \mathrm{Quot}(R_J) \subseteq Q$ be the quotient field of R_J.

PROPOSITION 3.10: *If $J \cap J' \neq \emptyset$, then $Q_J \cap Q_{J'} = Q_{J \cap J'}$. If $J \cap J' = \emptyset$, then $Q_J \cap Q_{J'} = K(x)$.*

Proof: Let $j \in J$. Then $K[w_j] \subseteq R_J$, and hence $K(x) = K(w_j) \subseteq Q_J$. Similarly $K(x) \subseteq Q_{J'}$. Hence $K(x) \subseteq Q_J \cap Q_{J'}$. If $J \cap J' \neq \emptyset$, then, by the unique representation (6) for the elements of R, we have $R_{J \cap J'} = R_J \cap R_{J'}$, and therefore $Q_{J \cap J'} \subseteq Q_J \cap Q_{J'}$.

For the converse inclusion, let $0 \neq f \in Q_J \cap Q_{J'}$. Fix $j \in J$ and $j' \in J'$; if $J \cap J' \neq \emptyset$, take $j, j' \in J \cap J'$. Write f as f_1/g_1 with $f_1, g_1 \in R_J$. By Lemma 3.7, $g_1 = p_1 u_1$, where $0 \neq p_1 \in K[w_j]$ and $u_1 \in R_J^\times$. Replace f_1 by $f_1 u_1^{-1}$ to assume that $g_1 \in K[w_j]$. Similarly $f = f_2/g_2$ with $f_2 \in R_{J'}$ and $g_2 \in K[w_{j'}]$.

If $J \cap J' \neq \emptyset$, then $g_1, g_2 \in R_J \cap R_{J'}$. Thus $g_2 f_1 = g_1 f_2 \in R_J \cap R_{J'} = R_{J \cap J'} \subseteq Q_{J \cap J'}$, and hence $f = \frac{f_1 g_2}{g_1 g_2} \in Q_{J \cap J'}$.

Assume that $J \cap J' = \emptyset$. Write g_1 as $\sum_{n=0}^{d_1} b_n w_j^n$, with $b_n \in K$. Put $h_1 = (\frac{w_{j'}}{w_j})^{d_1} g_1$. As $\frac{w_{j'}}{w_j} \in K[w_{j'}]$, we have $h_1 = \sum_{n=0}^{d_1} b_n (\frac{w_{j'}}{w_j})^{d_1 - n} w_{j'}^n \in K[w_{j'}]$. Similarly there is $d_2 \geq 0$ such that $h_2 = (\frac{w_j}{w_{j'}})^{d_2} g_2 \in K[w_j]$. Let $d = d_1 + d_2$. Then, for each $k \in J$

$$f_1 h_2 \cdot \left(\frac{w_{j'}}{w_k}\right)^d = f_2 h_1 \cdot \left(\frac{w_j}{w_k}\right)^d. \tag{8}$$

Note that $f_1h_2 \in R_J$ while $f_2h_1 \in R_{J'}$. In particular, the kth component of f_2h_1 is zero. By Lemma 3.6(c), the kth component of $f_2h_1 \cdot \left(\frac{w_j}{w_k}\right)^d$ is a polynomial in w_k. By (8), the kth component of $f_1h_2 \cdot \left(\frac{w_{j'}}{w_k}\right)^d$ is a polynomial in w_k. Hence, again by Lemma 3.6(c), the kth component of f_1h_2 is a polynomial in w_k.

Conclude that $f_1h_2 \in K[w_k \mid k \in J]$ and therefore that $f = \frac{f_1h_2}{g_1h_2} \in K(x)$. ∎

Proposition 3.10 essentially says that the pre-sheaf of meromorphic functions on an affinoid in $\mathbb{P}^1(K)$ is a sheaf (cf. [FrP, Thm. III.7.4]).

4. Factorization of matrices over complete rings

We show in this section how to decompose a matrix over a complete ring into a product of matrices over certain complete subrings. This will establish condition (2e) of §1 in our setup. of §1 in our setup.

Lemma 4.2 below appears as Lemma 11.14 in [Voe]. Its proof is almost identical with that of [HaV, Lemma 2.2] and with that of [FrP, III.6.3].

Definition 4.1: Normed ring. Let M be an associative ring with 1. A **norm** on M is a function $||\cdot||: M \to \mathbb{R}$ that satisfies the following conditions for all $a, b \in M$:

(a) $||a|| \geq 0$, and $||a|| = 0$ if and only if $a = 0$; further $||1|| = ||-1|| = 1$;

(b) $||a + b|| \leq \max(||a||, ||b||)$;

(c) $||ab|| \leq ||a|| \cdot ||b||$.

We say that M is **complete** if every Cauchy sequence in M converges. Note that in this case, if $||1 - a|| < 1$, then $a \in M^\times$. Indeed, $a^{-1} = \sum_{n=0}^{\infty}(1-a)^n$. ∎

Lemma 4.2 (Cartan's Lemma): *Let M be a complete normed ring. Let M_1 and M_2 be complete subrings of M. Suppose that*

(d) *for each $a \in M$ there are $a^+ \in M_1$ and $a^- \in M_2$ with $||a^+||, ||a^-|| \leq ||a||$ such that $a = a^+ + a^-$.*

Then for each $b \in M$ with $||b - 1|| < 1$ there exist $b_1 \in M_1^\times$ and $b_2 \in M_2^\times$ such that $b = b_1 b_2$.

For the rest of this section let A be a commutative ring with a nontrivial ultrametric absolute value $|\ |$.

Example 4.3: Let n be a positive integer and let M be the ring $\mathrm{M}_n(A)$ of $n \times n$ matrices over A. We define the **norm** of a matrix $a = (a_{ij}) \in M$ by $||a|| = \max_{ij} |a_{ij}|$. It satisfies conditions (a), (b), and (c). If A is complete, then so is M. In this case suppose that A_1 and A_2 are complete subrings of A. Then $M_1 = \mathrm{M}_n(A_1)$ and $M_2 = \mathrm{M}_n(A_2)$ are complete subrings of M. If A satisfies conditions (d′) below, then M satisfies condition (d) above.

(d′) For each $a \in A$ there are $a^+ \in A_1$ and $a^- \in A_2$ with $|a^+|, |a^-| \leq |a|$ such that $a = a^+ + a^-$. ∎

COROLLARY 4.4: *In the notation of Example 4.3, suppose that A, A_1, and A_2 are complete and satisfy Condition (d′). Let A_0 be a dense subring of A that satisfies*
(e′) *$A = A_0 + gA$ for each nonzero $g \in A_0$; and*
(f′) *for every $f \in A$ there are $p \in A_0$ and $u \in A^\times$ such that $f = pu$.*
Let $E_i = \mathrm{Quot}(A_i)$, for $i = 0, 1, 2$, and let $E = \mathrm{Quot}(A)$. Assume that $E_0 \subseteq E_2$. Then, for each $b \in \mathrm{GL}_n(E)$ there are $b_1 \in \mathrm{GL}_n(E_1)$ and $b_2 \in \mathrm{GL}_n(E_2)$ such that $b = b_1 b_2$.

Proof: By Condition (f′) each element of E is of the form $\frac{1}{h}f$, where $f \in A$ and $h \in A_0$. So there is $h \in A_0$ such that $hb \in \mathrm{M}_n(A)$. If $hb = b_1 b_2'$, where $b_1 \in \mathrm{GL}_n(E_1)$ and $b_2' \in \mathrm{GL}_n(E_2)$, then $b = b_1 b_2$ with $b_2 = \frac{1}{h} b_2' \in GL_n(E_2)$. So we may assume that $b \in \mathrm{M}_n(A)$.

Let $d \in A$ be the determinant of b. By Condition (f′) there are $g \in A_0$ and $u \in A^\times$ such that $d = gu$. Let $b'' \in \mathrm{M}_n(A)$ be the adjoint matrix of b, so that $bb'' = d1$. Let $b' = u^{-1}b''$. Then $b' \in \mathrm{M}_n(A)$ and $bb' = g1$.

Put

$$V = \{a' \in \mathrm{M}_n(A) \mid ba' \in g\mathrm{M}_n(A)\} \qquad \text{and} \qquad V_0 = V \cap \mathrm{M}_n(A_0).$$

Then V is an additive subgroup of $\mathrm{M}_n(A)$ and $g\mathrm{M}_n(A) \leq V$. By (e′), $\mathrm{M}_n(A) = \mathrm{M}_n(A_0) + g\mathrm{M}_n(A)$. Hence $V = V_0 + g\mathrm{M}_n(A)$. Since $\mathrm{M}_n(A_0)$ is dense in $\mathrm{M}_n(A)$, and therefore $g\mathrm{M}_n(A_0)$ is dense in $g\mathrm{M}_n(A)$, it follows that $V_0 = V_0 + g\mathrm{M}_n(A_0)$ is dense in $V = V_0 + g\mathrm{M}_n(A)$. As $b' \in V$, there is $a_0 \in V_0$ such that $||b' - a_0|| < \frac{|g|}{||b||}$. In particular, $a_0 \in \mathrm{M}_n(A_0)$ and $ba_0 \in g\mathrm{M}_n(A)$.

Put $a = \frac{1}{g}a_0 \in \mathrm{M}_n(E_0)$. Then $ba \in \mathrm{M}_n(A)$ and $||1 - ba|| = ||\frac{1}{g}b(b' - a_0)|| \leq \frac{1}{|g|}||b|| \cdot ||b' - a_0|| < 1$. It follows that $ba \in \mathrm{GL}_n(A)$. In particular $\det(a) \neq 0$ and therefore $a \in \mathrm{GL}_n(E_0)$. By Lemma 4.2 there are $b_1 \in \mathrm{GL}_n(A_1)$ and $b_2' \in \mathrm{GL}_n(A_2)$ such that $ba = b_1 b_2'$. Thus $b = b_1 b_2$, where $b_1 \in \mathrm{GL}_n(A_1) \subseteq \mathrm{GL}_n(E_1)$ and $b_2 = b_2' a^{-1} \in \mathrm{GL}_n(E_2)$.
∎

We apply Corollary 4.4 to the rings and fields of §3.

COROLLARY 4.5: *Suppose that $I = J \cup J'$ is a partition of I into nonempty sets J and J'. Let n be a positive integer. Then, for each $b \in \mathrm{GL}_n(Q)$ there are $b_1 \in GL_n(Q_J)$*

and $b_2 \in \mathrm{GL}_n(Q_{J'})$ *such that* $b = b_1 b_2$. *The special case* $J = \{i\}$ *and* $J' = I \smallsetminus \{i\}$ *establishes condition (2e) of §1.*

Proof: By Lemma 3.3, R, R_J, and $R_{J'}$ are complete rings. Given $f \in R$, say, $f = a_0 + \sum_{i\in I} \sum_{k=1}^{\infty} a_{ik} w_i^k$, we let $f_1 = a_0 + \sum_{i\in J} \sum_{k=1}^{\infty} a_{ik} w_i^k$ and $f_2 = \sum_{i\in J'} \sum_{k=1}^{\infty} a_{ik} w_i^k$. Then $|f_i| \leq |f|$, $i = 1, 2$ and $f = f_1 + f_2$. This proves condition (d′). Next note that $R_0 = K[w_i \mid i \in I]$ is dense in R and its quotient field $K(x)$ is contained in both Q_J and $Q_{J'}$. Conditions (e′) and (f′) are Corollary 3.8 and Lemma 3.7, respectively. Corollary 4.5 is therefore a special case of Corollary 4.4. ∎

5. Solution of embedding problems

We solve here finite constant split embedding problems over complete fields with a couple of extra conditions. The first step of our solution is the construction of cyclic extensions with some extra conditions as required by Condition (2b) of §1.

PROPOSITION 5.1: *In the notation of §3, let $i \in I$, and let A be a finite abelian group. Then there exists a finite Galois extension F/E with $\mathcal{G}(F/E) \cong A$ such that $F \subseteq Q_{\{i\}}$. Moreover, F/K has a prime divisor of degree 1 which is unramified over E.*

Proof: By [FrJ, Lemma 24.46], E has a Galois extension F with Galois group A such that F is regular over K. By [HaV, Lemma 4.5], we may assume that F/K has a prime divisor of degree 1 which is unramified over E. By [HaV, Lemma 4.2(a)], we may assume that $F \subseteq K((x))$. Let z be a primitive element for F/E. By [HaV, Lemma 4.2(b)], we may assume that $z \in \mathrm{Quot}(K\{x\})$. By Remark 3.4 there is an isomorphism $\mathrm{Quot}(K\{x\}) \to Q_{\{i\}} = \mathrm{Quot}(K\{w_i\})$ that maps E onto itself. Hence we may assume that $z \in Q_{\{i\}}$. ∎

PROPOSITION 5.2: *Let K_0 be a field complete with respect to a non-trivial discrete ultrametric absolute value, with infinite residue field. Let K/K_0 be a finite unramified Galois extension with Galois group Γ. Let x be a transcendental element over K, and put $E_0 = K_0(x)$ and $E = K(x)$. Suppose that Γ acts (from the right) on a finite group G. Let $G \rtimes \Gamma$ be the corresponding semidirect product. Let $\pi\colon G \rtimes \Gamma \to \Gamma$ be the canonical projection. Then the* **constant split embedding problem** *$\pi\colon G \rtimes \Gamma \to \Gamma = \mathcal{G}(E/E_0)$ has a* **rational** *(and hence* **regular***)* **solution***: That is, there exists an extension F of E such that*

(1a) *F/E_0 is Galois;*

(1b) *there is an isomorphism $\psi\colon \mathcal{G}(F/E_0) \to G \rtimes \Gamma$ such that $\pi \circ \psi = \mathrm{res}_E$; and*

(1c) *F has a K-rational place $\mathfrak{p}$ (and hence F/K is regular).*

Proof: Our strategy is to attach a patching data $\mathcal{E}$ to the embedding problem and to define a proper action of Γ on $\mathcal{E}$. Then we apply Proposition 1.5 to conclude that the co-compound F of $\mathcal{E}$ gives a solution to the embedding problem.

Fix a finite set I on which Γ acts from the right and a system of generators $T = \{\tau_i \mid i \in I\}$ of G such that for each $i \in I$

(2a) $\{\gamma \in \Gamma \mid i^\gamma = i\} = \{1\}$;

(2b) $\tau_i^\gamma = \tau_{i^\gamma}$, for every $\gamma \in \Gamma$; and

(2c) $|I| \geq 2$.

(E.g., assuming $G \neq 1$, let $I = G \times \Gamma$, let Γ act on I by $(\sigma, \gamma)^\delta = (\sigma, \gamma\delta)$, and let $\tau_{(\sigma,\gamma)} = \sigma^\gamma$.)

Let G_i be the cyclic subgroup generated by τ_i. Then $G_i^\gamma = G_{i^\gamma}$ for each $\gamma \in \Gamma$ and $G = \langle G_i \mid i \in I\rangle$. Choose a system of representatives J for the Γ-orbits of I. Then every $i \in I$ can be uniquely written as $i = j^\gamma$ with $j \in J$ and $\gamma \in \Gamma$.

Claim A: *There exists a subset $\{c_i \mid i \in I\} \subseteq K$ such that $c_i^\gamma = c_{i^\gamma}$ and $|c_i| = |c_i - c_j| = 1$ for all distinct $i, j \in I$ and all $\gamma \in \Gamma$.*

Indeed, let $U = \{a \in K \mid |a| = 1\}$. It suffices to find $\{c_j \| j \in J\} \subseteq U$ (and then define c_i, for $i = j^\gamma \in I$, as c_j^γ) such that $c_j^\delta - c_j^\varepsilon \in U$ for all $(j, \delta), (k, \varepsilon) \in J \times \Gamma$ with $(j, \delta) \neq (k, \varepsilon)$.

Let $\bar{K}/\bar{K}_0$ be the residue fields extension of K/K_0. The residue map $a \mapsto \bar{a}$ maps U onto $\bar{K}^\times$. As K/K_0 is unramified, $\bar{K}/\bar{K}_0$ is a Galois extension and there is an isomorphism $\gamma \mapsto \bar{\gamma}$ from $\mathcal{G}(K/K_0)$ onto $\mathcal{G}(\bar{K}/\bar{K}_0)$ such that $\overline{a^\gamma} = \bar{a}^{\bar{\gamma}}$ for each $a \in U$. Thus it suffices to find $\{\bar{c}_j \mid j \in J\} \subseteq \bar{K}^\times$ such that $\bar{c}_j^{\bar{\delta}} \neq \bar{c}_j^{\bar{\varepsilon}}$ for all $j \in J$ and all distinct $\bar{\delta}, \bar{\varepsilon} \in \mathcal{G}(\bar{K}/\bar{K}_0)$, and $\bar{c}_j^{\bar{\delta}} \neq \bar{c}_k^{\bar{\varepsilon}}$ for all distinct $j, k \in J$ and all $\bar{\delta}, \bar{\varepsilon} \in \mathcal{G}(\bar{K}/\bar{K}_0)$.

The first condition says that $\bar{c}_j$ is a primitive element for $\bar{K}/\bar{K}_0$; the second condition says that $\bar{c}_j, \bar{c}_k$ are not conjugate over $\bar{K}_0$. Thus it suffices to show that there are infinitely many primitive elements for $\bar{K}/\bar{K}_0$. But if $\bar{c} \in \bar{K}^\times$ is primitive, then so is $\bar{c} + \bar{a}$, for each $\bar{a} \in \bar{K}_0$. As $\bar{K}_0$ is infinite, our Claim follows.

Construction B: *A patching data.*

For each $i \in I$ put $w_i = \frac{1}{x - c_i} \in K(x)$. As in §3, consider the ring $R = K\{w_i \| i \in I\}$ and let Q be its quotient field. For each $i \in I$ let

$$Q_i = Q_{I \smallsetminus \{i\}} = \mathrm{Quot}(K\{w_j \mid j \neq i\}) \qquad \text{and} \qquad Q_i' = Q_{\{i\}} = \mathrm{Quot}(K\{w_i\})$$

(we use the notation of §3). By Proposition 3.10, $Q_i' = \bigcap_{j \neq i} Q_j$ and $E = K(x) = \bigcap_i Q_i$.

The group $\Gamma = \mathcal{G}(K/K_0)$ lifts isomorphically to $\mathcal{G}(E/E_0)$. By Remark 3.2(e), each $\gamma \in \Gamma$ preserves the absolute value on E. Moreover, $w_i^\gamma = w_{i^\gamma}$, $i \in I$. Hence, γ leaves $K[w_i \mid i \in I]$ invariant. It follows that Γ lifts to a group of continuous automorphisms of R and therefore also of $Q = \mathrm{Quot}(R)$. Clearly $Q_i^\gamma = Q_{i^\gamma}$ and $(Q_i')^\gamma = Q_{i^\gamma}'$.

For each $j \in J$, Proposition 5.1 gives a cyclic extension F_j/E with group $G_j = \langle \tau_j \rangle$ such that $F_j \subseteq Q_j'$.

For an arbitrary $i \in I$ there exist unique $j \in J$ and $\gamma \in \Gamma$ such that $i = j^\gamma$ (by (2a)). Let $F_i = F_j^\gamma$. As γ acts on Q and leaves E invariant, F_i is a Galois extension of E and $F_i \subseteq Q_i'$.

The isomorphism $\gamma\colon F_j \to F_i$ gives an isomorphism $\mathcal{G}(F_j/E) \cong \mathcal{G}(F_i/E)$ which maps each $\tau \in \mathcal{G}(F_j/E)$ onto $\gamma^{-1} \circ \tau \circ \gamma \in \mathcal{G}(F_i/E)$ (notice that the elements of the Galois groups act from the right). In particular, it maps τ_j onto $\gamma^{-1} \circ \tau_j \circ \gamma$. We can therefore identify G_i with $\mathcal{G}(F_i/E)$ such that τ_i coincides with $\gamma^{-1} \circ \tau_j \circ \gamma$. This means that $(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma}$ for all $a \in F_j$ and $\tau \in G_j$.

It follows that for all $i \in I$ and $\gamma \in \Gamma$ we have $F_i^\gamma = F_{i^\gamma}$. Moreover, $(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma}$ for all $a \in F_i$ and $\tau \in G_i$.

By Corollary 4.5, $\mathrm{GL}_n(Q) = \mathrm{GL}_n(Q_i)\mathrm{GL}_n(Q_i')$ for each $i \in I$. Thus $\mathcal{E} = (E, F_i, Q_i, Q; G_i, G)_{i \in I}$ is a patching data (Definition 1.1) and Γ acts properly on $\mathcal{E}$ (Definition 1.4).

Let P_i, N_i, N, and F be as in Diagram (5) of §1. By Proposition 1.5, the compound F of $\mathcal{E}$ satisfies (1a) and (1b). We now verify (1c).

Claim C: *F/K has a set of prime divisors of degree 1 with cardinality* $\mathrm{Card}(K)$.

Lemma 1.3(b) gives an E-embedding $\lambda\colon F \to Q$. Each $b \in K$ with $|b| > 1$ induces the evaluation homomorphism $x \mapsto b$ from R to K which maps w_i onto $\frac{1}{b - c_i}$ (Remark 3.5). As R is a principal ideal domain (Proposition 3.9), this homomorphism extends to a K-rational place $\varphi_b\colon Q \to K \cup \{\infty\}$. Thus $\varphi_b \circ \lambda$ is a K-rational place of F, and so it corresponds to a prime divisor of F/K of degree 1. The cardinality of $\{b \in K \mid |b| > 1\}$ is equal to the cardinality of K. Since $\varphi_b \circ \lambda(w_i) = \frac{1}{b - c_i}$, distinct b give distinct $\varphi_b \circ \lambda$. This establishes Condition (1c) and concludes the proof of the Proposition. ∎

6. Ample fields

In this section K/K_0 is an arbitrary finite Galois extension with Galois group Γ, x is transcendental over K, $E_0 = K_0(x)$, $E = K(x)$, and we identify $\mathcal{G}(E/E_0)$ with Γ via restriction. Suppose that Γ acts on a finite group G. We look for a rational solution of the constant split embedding problem over E_0:

$$\pi\colon G \rtimes \Gamma \longrightarrow\!\!\!\!\!\rightarrow \mathcal{G}(E/E_0), \tag{1}$$

where π is the projection on Γ. Under quite general conditions this problem reduces to the special case we have just solved in §5.

Let $\hat{K}_0$ be a field extension of K_0 and let $\hat{K} = K\hat{K}_0$. Recall that K_0 is **existentially closed** in $\hat{K}_0$ if each algebraic subset A of $\mathbb{A}^n$ which has a $\hat{K}_0$-rational point also has a K_0-rational point. This implies that $\hat{K}_0/K_0$ is regular. Assume that K_0 is existentially closed in $\hat{K}_0$ and, in addition, that x is transcendental over $\hat{K}_0$. Then $\hat{K}(x)$ is a regular extension of E and res: $\mathcal{G}(\hat{K}(x)/\hat{K}_0(x)) \to \mathcal{G}(E/E_0)$ is an isomorphism. We identify the two groups and obtain a constant split embedding problem over $\hat{K}_0(x)$:

$$\pi\colon G \rtimes \Gamma \longrightarrow\!\!\!\!\!\rightarrow \mathcal{G}(\hat{K}(x)/\hat{K}_0(x)), \tag{2}$$

Let F/K be a finitely generated regular extension of transcendence degree 1. A **model** of F/K is an absolutely irreducible algebraic curve C which is defined over K and whose function field over K is F. Choose a generic point $\mathbf{x} = (x_1, \ldots, x_n)$ of an affine part of C over K such that $F = K(\mathbf{x})$. If $\varphi\colon F \to \tilde{K} \cup \{\infty\}$ is a K-place of F (in particular $\varphi(a) = a$ for each $a \in K$) and $\varphi(x_1), \ldots, \varphi(x_n) \neq \infty$, then $\mathbf{p} = \varphi(\mathbf{x})$ is a point of $C(\tilde{K})$ which is called the **center** of φ at C.

LEMMA 6.1: *Let F/K be a finitely generated separable extension of transcendence degree* 1.

(a) *Let $\varphi\colon F \to K \cup \{\infty\}$ be a K-rational place. Denote the valuation ring of φ by O. Then F/K has an affine model C such that the center of φ at C is a simple K-rational point $\mathbf{a}$ of C whose local ring coincides with O.*

(b) *Conversely, suppose that C is a model for F/K. Then, for each point $\mathbf{p} \in C_{\mathrm{simp}}(K)$ there exists a unique K-rational place $\varphi\colon F \to K \cup \{\infty\}$ whose center at C is $\mathbf{p}$.*

(c) *Let C be an absolutely irreducible curve over an infinite field K which has a K-rational simple point $\mathbf{p}$. Then there is a birational correspondence θ between C and an affine plane curve given by an absolutely irreducible equation $f(X,Y)=0$ over K such that $\theta(\mathbf{p})=(a,b)$, $f(a,b)=0$, and $\frac{\partial f}{\partial Y}(a,b)\neq 0$.*

Proof of (a): Let t be a separating transcendence element for F/K. Replace t by t^{-1}, if necessary, to assume that $\varphi(t)\in K$. Let $R=K[t]$ and let S be the integral closure of R in F. Then S is a finitely generated K-algebra, say $S=K[x_1,\ldots,x_n]$, and φ is finite at $x_1,\ldots,x_n$. The existence of a K-rational place for F/K implies that F/K is regular. Hence, the curve $C=\mathrm{Spec}(S)$ generated by $\mathbf{x}$ over K is absolutely irreducible and $\mathbf{a}=\varphi(\mathbf{x})\in C(K)$.

Let $\mathfrak{M}$ be the maximal ideal of O and put $\mathfrak{p}=R\cap\mathfrak{M}$ and $\mathfrak{q}=S\cap\mathfrak{M}$. Let $R_{\mathfrak{p}}$ and $S_{\mathfrak{p}}$ be the localizations of R and S, respectively, with respect to $R\setminus\mathfrak{p}$. Then $R_{\mathfrak{p}}$ is a discrete valuation ring and $S_{\mathfrak{p}}$ is the integral closure of $R_{\mathfrak{p}}$ in F. As $R\subseteq O$, we have $S\subseteq S_{\mathfrak{p}}\subseteq O$. By [Lan, p. 18, Thm. 4], $O_{C,\mathbf{a}}=S_{\mathfrak{q}}=(S_{\mathfrak{p}})_{\mathfrak{q}S_{\mathfrak{p}}}=O$. Finally, as a discrete valuation ring, O is a regular ring. Conclude that $\mathbf{a}$ is a simple point of C [Lan, p. 204].

Proof of (b): The local ring $O=O_{C,\mathbf{p}}$ is, by assumption, regular and therefore integrally closed [Mts, p. 157]. Hence, it is a valuation ring [Lan, p. 151]. The corresponding place is the desired one.

Proof of (c): Assume without loss that C is a projective curve in $\mathbb{P}^n$ and that $n\geq 2$. If $n=2$, apply a linear automorphism of $\mathbb{P}^2$ over K to assume that $\mathbf{p}=(a,b)$ is a finite point of C. Then take f as the polynomial that defines the affine part of C which contains $\mathbf{p}$. Exchange the coordinates X and Y, if necessary, to obtain the condition $\frac{\partial f}{\partial Y}(a,b)\neq 0$.

Assume therefore that $n\geq 3$. Then, there is a nonempty Zariski open subset U of $\mathbb{P}^n$ such that for each point $\mathbf{o}\in U(\tilde{K})$, the projection $\pi\colon \mathbb{P}^n\to\mathbb{P}^{n-1}$ from $\mathbf{o}$ maps C onto an absolutely irreducible curve C' such that $\pi|_C$ is a birational map and $\pi(\mathbf{p})$ is simple on C' [GJ1, Lemma 9.4]. Since K is infinite, we may choose $\mathbf{o}\in U(K)$. Then π and C' are defined over K and $\pi(\mathbf{p})\in C'(K)$. Now apply induction on n. ∎

LEMMA 6.2: *Let $\hat{K}_0/K_0$ be a field extension such that K_0 is existentially closed in $\hat{K}_0$. Suppose that embedding problem (2) has a rational (resp., regular) solution. Then embedding problem (1) also has a rational (resp., regular) solution.*

Proof: We prove only that a rational solution of (2) gives a rational solution of (1). The 'regular' case is analogous [Po1, Lemma 1.4].

So, $\hat{K}_0(x)$ has a Galois extension $\hat{F}$ which contains $\hat{K}(x)$, there exists an isomorphism θ: $\mathcal{G}(\hat{F}/\hat{K}_0(x)) \to G \rtimes \Gamma$ such that $\pi \circ \theta = \mathrm{res}_{\hat{K}(x)}$, and $\hat{F}$ has a $\hat{K}$-rational place. In particular, $\hat{F}/\hat{K}$ is regular.

By Lemma 6.1(c), there exist polynomials $f \in \hat{K}_0[X,Z]$, $g \in \hat{K}[X,Z]$, and $h \in \hat{K}[T,Y]$, elements $z,t,y \in \hat{F}$, and elements $a,b \in \hat{K}$ such that the following conditions hold:

(3a) $\hat{F} = \hat{K}_0(x,z)$, $f(x,Z) = \mathrm{irr}(z, \hat{K}_0(x))$; we may therefore identify $\mathcal{G}(f(x,Z), \hat{K}_0(x))$ with $\mathcal{G}(\hat{F}/\hat{K}_0(x))$;

(3b) $g(x,Z) = \mathrm{irr}(z, \hat{K}(x))$; therefore $g(X,Z)$ is absolutely irreducible;

(3c) $\hat{K}(t,y) = \hat{F}$, $h(t,y) = 0$, $h(T,Y)$ is absolutely irreducible, $h(a,b) = 0$, and $\frac{\partial h}{\partial Y}(a,b) \neq 0$.

All of these objects depend on only finitely many parameters from $\hat{K}_0$. So, let $u_1, \ldots, u_n$ be elements of $\hat{K}_0$ such that the following conditions hold:

(4a) $F = K_0(\mathbf{u}, x, z)$ is a Galois extension of $K_0(\mathbf{u}, x)$, the coefficients of $f(X,Z)$ lie in $K_0[\mathbf{u}]$, $f(x,Z) = \mathrm{irr}(z, K_0(\mathbf{u},x))$, and $\mathcal{G}(f(x,Z), K_0(\mathbf{u},x)) = \mathcal{G}(f(x,Z), \hat{K}_0(x))$;

(4b) the coefficients of g lie in $K[\mathbf{u}]$; hence $g(x,Z) = \mathrm{irr}(z, K(\mathbf{u},x))$;

(4c) $K(\mathbf{u},t,y) = F$, and the coefficients of h and a,b belong to $K[\mathbf{u}]$.

Since K_0 is existentially closed in $\hat{K}_0$, the field $\hat{K}_0$ and therefore also $K_0(\mathbf{u})$ are regular extensions of K_0. Thus, $\mathbf{u}$ generates an absolutely irreducible variety $U = \mathrm{Spec}(K_0[\mathbf{u}])$ over K_0. The variety U has a nonempty Zariski open subset U' such that for each $\mathbf{u}' \in U'$ the K_0-specialization $\mathbf{u} \to \mathbf{u}'$ extends to a K-homomorphism $'$: $K[\mathbf{u}, x, z, t, y] \to K[\mathbf{u}', x, z', t', y']$ such that the following conditions hold:

(5a) $f'(x,z') = 0$, the discriminant of $f'(x,Z)$ is not zero, and $F' = K_0(\mathbf{u}', x, z')$ is the splitting field of $f'(x,Z)$ over $K_0(\mathbf{u}', x)$; in particular $F'/K_0(\mathbf{u}', x)$ is Galois;

(5b) $g'(X,Z)$ is absolutely irreducible and $g'(x,z') = 0$; so $g'(x,Z) = \mathrm{irr}(z, K(\mathbf{u}', x))$;

(5c) $h'(T,Y)$ is absolutely irreducible, $K(\mathbf{u}',t',y') = F'$, $a', b' \in K[\mathbf{u}']$, $h'(a',b') = 0$, and $\frac{\partial h'}{\partial Y}(a',b') \neq 0$.

To achieve the absolute irreducibility of g' and h' we have used the Bertini-Noether theorem [FrJ, Prop. 8.8]. Since K_0 is existentially closed in $\hat{K}_0$ and since $\mathbf{u} \in U'(\hat{K}_0)$, we can choose $\mathbf{u}' \in U'(K_0)$. By (5a), the homomorphism $'$ induces an embedding

$$\varphi^*\colon \mathcal{G}(f'(x,Z), K_0(x)) \to \mathcal{G}(f(x,Z), K_0(\mathbf{u},x))$$

which commutes with the restriction to $\mathcal{G}(K(x)/K_0(x))$ [Lan, p. 248]. Observe that $K(x)$ is linearly disjoint from $K_0(\mathbf{u})$ over K_0. Hence, by (5b),

$$\begin{aligned} |\mathcal{G}(f'(x,Z), K_0(x))| &= [F' : K_0(x)] = \deg(g'(x,Z))[K(x) : K_0(x)] \\ &= \deg(g(x,Z))[K(\mathbf{u},x) : K_0(\mathbf{u},x)] \\ &= [F : K_0(\mathbf{u},x)] = |\mathcal{G}(f(x,Z), K_0(\mathbf{u},x))|. \end{aligned}$$

It follows that φ^* is an isomorphism. Hence $\theta \circ \varphi^*$ solves embedding problem (1). By (5c) and Lemma 6.1(b), F' has a K-rational place. ∎

Definition 6.3: Let K be a field. We say that K is **ample*** if every absolutely irreducible variety V over K with a simple K-rational point has infinitely many K-rational points. Equivalently [Po1, Prop. 1.1], K is existentially closed in $K((t))$.

For example, Henselian fields, PAC fields and more generally, PSC fields [JaR, Remark 8.3] are ample. Fields which are finitely generated over their prime fields are not ample (use the general Mordell Conjecture [Ja1, Prop. 5.2]). It is unknown whether $\mathbb{Q}_{\mathrm{ab}}$ or $\mathbb{Q}_{\mathrm{sol}}$ are ample fields. ∎

THEOREM 6.4: *Let K_0 be an ample field. Then each finite constant split embedding problem over $K_0(x)$ has a rational solution.*

Proof: Consider a finite constant split embedding problem (1) over $K_0(x)$. Let $\hat{K}_0 = K_0((t))$. Then $\hat{K}_0$ has a complete non-trivial discrete ultrametric absolute value with

* Pop [Po1] uses 'large' instead of 'ample'. Unfortunately, the adjective 'large' in the naive sense has been attached to algebraic extensions of Hilbertian fields in several papers (e.g., [Ja1], [Ja2], [FyJ], [GJ2], [Ja3], [Ja4], [Ja5]). Thus, in order not to confuse the readers, we replace 'large' by 'ample'.

t as a prime element and with the infinite residue field K_0. Also, $\hat{K} = K\hat{K}_0$ is an unramified extension of $\hat{K}_0$. Hence, by Proposition 5.2, (2) has a rational solution. By Definition 6.3, K_0 is existentially closed in $\hat{K}_0$. Hence, by Lemma 6.2, (1) also has a rational solution. ∎

THEOREM 6.5: *Let K be an ample field.*

(a) *If K is separably Hilbertian, then each finite split embedding problem over K is solvable.*

(b) *If, in addition, $G(K)$ is projective, then each finite embedding problem is solvable.*

(c) *If, in addition, $G(K)$ has countably many generators, and, in particular, if K is countable, then $G(K)$ is isomorphic to the free profinite group $\hat{F}_\omega$ or rank $\aleph_0$.*

Proof of (a): Every finite split embedding problem over K defines a finite constant split embedding problem over $K(x)$. The latter is solvable by Theorem 6.4. Now use the Hilbertianity and specialize to get a solution of the original embedding problem over K.

Proof of (b): Every finite embedding problem for a projective group can be reduced to a finite split embedding problem [Mat, p. 231]. By (a), the latter is solvable for $G(K)$. Hence, each finite embedding problem over K is solvable.

Proof of (c): Use (b) and Iwasawa's criterion [FrJ, Cor. 24.2]. ∎

The following special case of Theorem 6.5 is a solution to [FrJ, Prob. 24.41]. Here we say that a field K is ω-**free** if each finite embedding problem over K is solvable.

THEOREM 6.6: *Let K be a PAC field. Then K is ω-free if and only if K is separably Hilbertian.*

Proof: That 'K is ω-free' implies 'K is separably Hilbertian' is a result of Roquette [FrJ, Cor. 24.38]. Conversely, if K is PAC, then $G(K)$ is projective [FrJ, Thm. 10.17]. Hence, if K is separably Hilbertian, then by Theorem 6.5(b), K is ω-free. ∎

References

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

[DeD] P. Dèbes and B. Deschamps, *The Regular Inverse Galois Problem over Large Fields,* Preprint, Lille, 1996.

[FrP] J. Fresnel and M. v.d. Put, *Géométrie Analytique Rigide et Applications,* Progress in Mathematics **18**, Birkhäuser, Boston, 1981.

[FyJ] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields,* Proceedings of the London Mathematical Society **28** (1974), 112–128.

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

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

[GJ1] W.-D. Geyer and M. Jarden, *On stable fields in positive characteristic,* geometria dedicata **29** (1989), 335–375.

[GJ2] W.-D. Geyer and M. Jarden, *Torsion points of elliptic curves over large algebraic extensions of finitely generated fields,* Israel Journal of Mathematics **31** (1978), 157–197.

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

[Ja1] M. Jarden, *Elementary statements over large algebraic fields,* Transactions of AMS **164** (1972), 67–91.

[Ja2] M. Jarden, *Roots of unity over large algebraic fields,* Mathematische Annalen **213** (1975), 109–127.

[Ja3] M. Jarden, *Torsion in linear groups over large algebraic fields,* Archiv der Mathematik **32** (1979), 445–451.

[Ja4] M. Jarden, *The elementary theory of large e-fold ordered fields,* Acta mathematica **149** (1982), 239–260.

[Ja5] M. Jarden, *Large normal extensions of Hilbertian fields,* Mathematische Zeitschrift, to appear.

[JaR] M. Jarden and A. Razon, *Rumely local global principle for algebraic PSC fields over rings,* Transactions of AMS, to appear.

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

[Mat] B. H. Matzat, *Konstruktive Galoistheorie,* Lecture Notes in Mathematics **1284**, Springer, Berlin, 1987.

[Mts] H. Matsumura, *Commutative ring theory,* Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, Cambridge 1994.

[Po1] F. Pop, *Embedding problems over large fields,* Annals of Mathematics **144** (1996) 1–34.

[Po2] F. Pop, *The geometric case of a conjecture of Shafarevich,* preprint, Heidelberg, 1993.

[Po3] F. Pop, *Étale Galois covers of affine smooth curves,* Inventiones mathematicae **120** (1995), 555–578.

[Voe] H. Völklein, *Groups as Galois groups – an Introduction,* Cambridge Studies in Advanced Mathematics **53**, Cambridge University Press 1996.