TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 366, Number 7, July 2014, Pages 3535–3551
S 0002-9947(2014)05931-X
Article electronically published on February 26, 2014

SPLIT EMBEDDING PROBLEMS OVER THE OPEN ARITHMETIC DISC

ARNO FEHM AND ELAD PARAN

ABSTRACT. Let $\mathbb{Z}\{t\}$ be the ring of arithmetic power series that converge on the complex open unit disc. A classical result of Harbater asserts that every finite group occurs as a Galois group over the quotient field of $\mathbb{Z}\{t\}$. We strengthen this by showing that every finite split embedding problem over $\mathbb{Q}$ acquires a solution over this field. More generally, we solve all t-unramified finite split embedding problems over the quotient field of $\mathcal{O}_K\{t\}$, where $\mathcal{O}_K$ is the ring of integers of an arbitrary number field K.

1. INTRODUCTION

The inverse Galois problem (IGP) over a field K asks whether all finite groups occur as Galois groups over K. By Hilbert's irreducibility theorem, a positive answer to the classical IGP over the field of rational numbers $\mathbb{Q}$ would follow from a positive answer to the IGP over the rational function field $\mathbb{Q}(t)$.

In [Har84b], [Har84a] and [Har88], Harbater introduced and studied a family of fields which "approximate" the field $\mathbb{Q}(t)$: Given a positive number r, consider the ring $\mathbb{Z}_r[[t]]$ of continuous complex valued functions on the closed disc of radius r that are holomorphic on the interior and whose Taylor expansion has only integer coefficients. For each $r < 1$, $\mathbb{Z}_r[[t]]$ properly contains the ring $\mathbb{Z}[t]$ of polynomials over the integers, while for each $r \geq 1$, $\mathbb{Z}_r[[t]]$ coincides with $\mathbb{Z}[t]$. Intuitively, the bigger $r(< 1)$ is, the closer $\mathbb{Z}_r[[t]]$ is to $\mathbb{Z}[t]$, and hence the closer the quotient field $\mathrm{Quot}(\mathbb{Z}_r[[t]])$ is to $\mathbb{Q}(t)$. Harbater also considered a "final" object of this family, closest to $\mathbb{Z}[t]$ - the ring $\mathbb{Z}\{t\} = \bigcap_{r<1} \mathbb{Z}_r[[t]]$ of arithmetic power series which converge on the open unit disc. Harbater proved that the IGP has a positive solution over the quotient field of each of the rings $\mathbb{Z}_r[[t]], r < 1$, and $\mathbb{Z}\{t\}$.

In order to prove this result, Harbater introduced his "patching" method, which enables one to patch realizations of cyclic groups over these fields into a realization of a group generated by them. The patching of Galois groups has since become a central method in Galois theory, leading to several major results. For example, the solution of Abhyankar's conjecture by Harbater and Raynaud, and Pop's solution over $K(X)$ of all finite split embedding problems over K, for any *ample* (or *large*) field K; cf. [Pop96]. A *finite split embedding problem* (FSEP) $\Gamma \ltimes G \to \Gamma$ over K is given by a finite Galois extension L of K with Galois group Γ acting on a finite group G. A *solution* to this embedding problem over a regular extension E of K is a Galois extension F of E containing L, such that $\mathrm{Gal}(F/E) \cong \Gamma \ltimes G$, and the restriction of automorphisms from F to EL coincides with the projection onto Γ.

Received by the editors August 29, 2011 and, in revised form, August 2, 2012.
2010 *Mathematics Subject Classification.* Primary 12E30, 12F12, 13J05.
This research was supported by the DFG program "Initiation and Intensification of Bilateral Cooperation".

The solvability of split embedding problems is a much stronger Galois theoretic property than merely the realization of finite groups. This has been extensively studied in recent years, for example in [Pop96], [HS05], [Par09], [BSHH10], [Pop10]. In [FP11] it is shown that for each $r < 1$, the quotient field E_r of $\mathbb{Z}_r[[t]]$ is ample and hence every FSEP over E_r is solvable over $E_r(X)$, from which, using the fact that E_r is Hilbertian, one can deduce the solvability of every FSEP over E_r itself, thus extending Harbater's solution of the IGP over E_r. However, the field $E = \mathrm{Quot}(\mathbb{Z}\{t\})$, which is the most interesting within this family (being closest to $\mathbb{Q}(t)$), remained outside the scope of the results of [FP11]: It is unknown whether E is ample; see the discussion after Theorem 6.7. Nevertheless, in this work we show that every FSEP over the rational numbers $\mathbb{Q}$ is solvable over E. More generally, we prove the following result on the solvability of split embedding problems over E (which generalizes Harbater's solution of the IGP over E):

Main Theorem. *Let E'/E be a finite Galois extension with group Γ acting on a finite group G, and suppose the prime t of E is unramified in E'. Then the FSEP $\Gamma \ltimes G \to \Gamma$ has a solution.*

For the field E the methods of [FP11] fail altogether. Therefore, here we take a different path – we exploit the axiomatic approach to patching developed by Haran-Jarden-Völklein in [HV96], [HJ98a] and [HJ98b], where we replace the "analytic rings" constructed there by a new type of rings of power series with special properties, generalizing the rings used by Harbater in [Har84b]. In order to deal with the Galois action defined by a given FSEP, we work with rings of power series whose coefficients belong to the ring of integers of a certain number field. This Dedekind domain usually does not have the nice properties of $\mathbb{Z}$ (most notably, it need not be factorial), which leads to more delicate number theoretic constructions than in [Har84b], which, in particular, yield a stronger matrix factorization result.

In his recent work [Poi10], Poineau applies the patching of analytic Berkovich spaces in order to extend Harbater's solution of the IGP from E to the quotient field E_K of $\mathcal{O}_K\{t\}$, where K is an arbitrary number field with ring of integers $\mathcal{O}_K$. Using our constructions we are able to generalize that result as well, replacing the field E in our Main Theorem with E_K (Theorem 6.7). Moreover, we show that our solutions are regular over K.

2. Analytic fields

In this section we define the analytic rings needed for the patching machinery and prove some of their basic properties.

2.1. Rings of convergent power series.

We start by defining rings of convergent power series.

Definition 2.1. A **norm** on a ring R is a map $||\cdot|| : R \to \mathbb{R}_{\geq 0}$ such that $||\pm 1|| = 1$, $||x|| = 0$ iff $x = 0$, $||x + y|| \leq ||x|| + ||y||$, and $||xy|| \leq ||x|| \cdot ||y||$ for all $x, y \in R$. If moreover $||x + y|| \leq \max\{||x||, ||y||\}$, then $||\cdot||$ is called **ultrametric**. A norm is an **absolute value** if it satisfies $||xy|| = ||x|| \cdot ||y||$ for all $x, y \in R$. An absolute value that is not ultrametric is **archimedean**. □

Remark 2.2. Fix an algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$. The field of complex numbers $\mathbb{C}$ is complete with respect to the usual archimedean absolute value $|\cdot|$. The restriction

of this absolute value to $\mathbb{Q}$ extends to a norm on $\tilde{\mathbb{Q}}$ by

$$||x|| = \max_{\sigma \in \mathrm{Hom}(\tilde{\mathbb{Q}}, \mathbb{C})} |\sigma(x)|,$$

where $\mathrm{Hom}(\tilde{\mathbb{Q}}, \mathbb{C})$ denotes the set of all embeddings of $\tilde{\mathbb{Q}}$ into $\mathbb{C}$. Note that if K is a number field (that is, a finite extension of $\mathbb{Q}$), then

$$||x|| = \max_{\sigma \in \mathrm{Hom}(K, \mathbb{C})} |\sigma(x)|$$

for each $x \in K$, and $\mathrm{Hom}(K, \mathbb{C})$ is the finite set of embeddings of K into $\mathbb{C}$. □

Notation 2.3. For each $r > 0$, let $\mathbb{C}_r[[t]]$ be the ring of continuous complex functions on the closed disc of radius r around the origin which are holomorphic on the interior of the disc. Then $\mathbb{C}_r[[t]]$ is complete with respect to the uniform norm $|\cdot|_r$ on the closed disc of radius r. Note that

$$\mathbb{C}_{1^-}[[t]] := \bigcap_{r<1} \mathbb{C}_r[[t]] = \left\{ \sum_{n=0}^{\infty} a_n t^n \in \mathbb{C}[[t]] \ : \ \limsup_{n\to\infty} |a_n|^{1/n} \leq 1 \right\}$$

is the ring of holomorphic functions on the open unit disc. We will identify each $\sigma \in \mathrm{Hom}(\tilde{\mathbb{Q}}, \mathbb{C})$ with its extension $\sigma \in \mathrm{Hom}(\tilde{\mathbb{Q}}[[t]], \mathbb{C}[[t]])$ given by $\sigma(\sum_{n=0}^{\infty} a_n t^n) = \sum_{n=0}^{\infty} \sigma(a_n) t^n$. For $r > 0$ put

$$\begin{aligned} \tilde{\mathbb{Q}}_r[[t]] &:= \bigcap_{\sigma \in \mathrm{Hom}(\tilde{\mathbb{Q}}, \mathbb{C})} \sigma^{-1}(\mathbb{C}_r[[t]]) \\ &= \left\{ f \in \tilde{\mathbb{Q}}[[t]] \ : \ \sigma(f) \in \mathbb{C}_r[[t]] \text{ for all } \sigma \in \mathrm{Hom}(\tilde{\mathbb{Q}}, \mathbb{C}) \right\}. \end{aligned}$$

We also put

$$\tilde{\mathbb{Q}}\{t\} := \bigcap_{r<1} \tilde{\mathbb{Q}}_r[[t]].$$

For a subring R of $\tilde{\mathbb{Q}}$, put

$$R_r[[t]] := \tilde{\mathbb{Q}}_r[[t]] \cap R[[t]]$$

and

$$R\{t\} := \tilde{\mathbb{Q}}\{t\} \cap R[[t]].$$

□

Remark 2.4. If $R \subseteq \mathbb{Q}$, then

$$R\{t\} = R[[t]] \cap \mathbb{C}_{1^-}[[t]]$$

is the ring of power series in $R[[t]]$ that converges on the open unit disc, and thus coincides with the ring denoted by $R\{t\}$ in [Har84b]. □

Remark 2.5. If R is a subring of a number field K, then the fact that $\mathrm{Hom}(K, \mathbb{C})$ is finite implies that

$$R\{t\} = \left\{ \sum_{n=0}^{\infty} a_n t^n \in R[[t]] \ : \ \limsup_{n\to\infty} ||a_n||^{1/n} \leq 1 \right\}.$$

In particular, if $f = \sum_{n=0}^{\infty} a_n t^n \in R[[t]]$ satisfies $||a_n|| < C$ for all $n \geq 0$, for some constant C, then $f \in R\{t\}$. □

2.2. **A Weierstrass division theorem.** For the rest of this section, fix a number field K and let $R = \mathcal{O}_K$ be its ring of integers. We show that the rings of power series just defined satisfy a variant of the Weierstrass division theorem.

Lemma 2.6. *For each $0 \neq g \in R$ there exists a positive bound $C_g \in \mathbb{R}$ such that for each $f \in K$ there exists $h \in R$ satisfying $||f - gh|| < C_g$.*

Proof. Let $b_1, \dots, b_n \in R$ be an integral basis of K. In particular, $K = \sum_{i=1}^n b_i\mathbb{Q}$. Let $C_1 = \sum_i ||b_i||$. For $f_1 \in K$, write $f_1 = \sum_i \lambda_i b_i$ with $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$, take $\mu_1, \dots, \mu_n \in \mathbb{Z}$ such that $|\lambda_i - \mu_i| \leq \frac{1}{2}$ for each $1 \leq i \leq n$ and put $h = \sum_i \mu_i b_i \in R$. Then $||f_1 - h|| = ||\sum_i (\lambda_i - \mu_i)b_i|| \leq \sum_i |\lambda_i - \mu_i| \cdot ||b_i|| \leq \frac{1}{2} \cdot C_1 < C_1$.

Now let $C_g = C_1 \cdot ||g||$. Given $f \in K$, let $f_1 = \frac{f}{g} \in K$. By the previous paragraph there exists $h \in R$ such that $||f_1 - h|| < C_1$, hence $||f - gh|| \leq ||g|| \cdot ||f_1 - h|| < C_g$. □

In several places we will use the constant C_1, which is just C_g for $g = 1$.

Let $\mathcal{F}$ be the family of non-trivial valuations on K (corresponding to the maximal ideals of R, i.e. the non-archimedean primes of K). For each $a \in R$, let $\mathcal{F}_a$ be the finite subfamily of valuations which are positive on a. For each $v \in \mathcal{F}$, denote the valuation ring of v (in K) by R_v.

Lemma 2.7. *Let $0 \neq g \in R$ and let C_g be the bound given by Lemma 2.6. For $0 \neq a \in R$ and $f \in R[\frac{1}{a}]$ there exists $h \in R[\frac{1}{a}]$ such that $f - gh \in R$ and $||f - gh|| < C_g$.*

Proof. The strong approximation theorem [Cas86, Chapter 10, Theorem 4.1] gives an element $h \in K$ such that $v(h - \frac{f}{g}) \geq 0 \geq v(\frac{1}{g})$ for each $v \in \mathcal{F}_a$, and $v(h) \geq 0$ for each $v \in \mathcal{F} \setminus \mathcal{F}_a$. Since R is integrally closed, so is $R[\frac{1}{a}]$. It follows that $R[\frac{1}{a}] = \bigcap_{v \in \mathcal{F} \setminus \mathcal{F}_a} R_v$, hence $h \in R[\frac{1}{a}]$. Let $v \in \mathcal{F} \setminus \mathcal{F}_a$. Then $v(f) \geq 0$ (since $f \in R[\frac{1}{a}]$), hence $v(h - \frac{f}{g}) \geq \min(v(h), v(\frac{f}{g})) \geq v(\frac{1}{g})$. We conclude that $v(h - \frac{f}{g}) \geq v(\frac{1}{g})$ holds for all $v \in \mathcal{F}$, hence $f - gh \in \bigcap_{v \in \mathcal{F}} R_v = R$, as needed. By Lemma 2.6, we may subtract an element of R from h to assume that $||f - gh|| < C_g$. □

The following proposition can be viewed as a form of "Weierstrass division".

Proposition 2.8. *Let $0 \neq a \in R$ and let $A = R\{t\}[\frac{1}{a}]$. Let D be either $R[\frac{1}{a}]\{t\}$ or $R[\frac{1}{a}][[t]]$. Then for each $0 \neq g \in D$ we have*

$$D = A + g \cdot (1 + tD).$$

Proof. Write $g = \sum_{i=m}^\infty g_i t^i$ with $g_m \neq 0$. Let $f = \sum_{i=0}^\infty f_i t^i \in D$. It suffices to find $h \in D$ with constant term 1 and such that $f - gh \in A$. Put $\hat{f} = \sum_{i=m}^\infty f_i t^{i-m}$. Then $f - t^m \hat{f} \in R[\frac{1}{a}][t] \subseteq A$. Replace f with $\hat{f}$ and g with $t^{-m}g$ to assume that $m = 0$. Since $a \in R[\frac{1}{a}]^\times$, we may multiply g and f with a power of a to assume that $g_0 \in R$. We now recursively construct the coefficients of h as follows: Put $h_0 = 1$. Suppose we have constructed $h_0, \dots, h_{n-1} \in R[\frac{1}{a}]$. Let $b_n := f_n - \sum_{i+j=n, j \neq n} g_i h_j$. Apply Lemma 2.7 to find $h_n \in R[\frac{1}{a}]$ such that $b_n - g_0 h_n \in R$. If $D = R[\frac{1}{a}][[t]]$ we also assume (by Lemma 2.7) that $||b_n - g_0 h_n|| < C_{g_0}$. If $D = R[\frac{1}{a}]\{t\}$, we instead apply Lemma 2.6 and subtract an element of R from h_n to assume that $||h_n|| < C_1$, where C_1 is the constant defined there.

Write $h = \sum_{i=0}^\infty h_i t^i \in R[\frac{1}{a}][[t]]$. Then the n-th coefficient of $f - gh$ is $b_n - g_0 h_n \in R$, hence $f - gh \in R[[t]]$. If $D = R[\frac{1}{a}][[t]]$, then $h \in R[\frac{1}{a}][[t]] = D$ and the coefficients of $f - gh$ are bounded, hence $f - gh \in R\{t\} \subseteq A$ (by Remark 2.5). If $D = R[\frac{1}{a}]\{t\}$,

then the coefficients of h are bounded, hence $h \in R[\frac{1}{a}]\{t\} = D$. Since also $f, g \in D$, we conclude that $f - gh \in D \cap R[[t]] = R\{t\} \subseteq A$. □

Corollary 2.9. *Let $0 \neq a \in R$ and let D be either $R[\frac{1}{a}]\{t\}$ or $R[\frac{1}{a}][[t]]$. Let Q be the localization of D by the multiplicative subset $R\{t\} \setminus \{0\}$. Then Q is a field. Equivalently, for each $g \in D$ there exists $0 \neq h \in D$ such that $gh \in R\{t\}$.*

Proof. The equivalence of the two assertions is clear. Let $0 \neq g \in D$. By Proposition 2.8, there exists $h \in 1+tD, r \in R\{t\}[\frac{1}{a}]$ such that $0 = r+gh$. Then $0 \neq h \in D$ and $gh = -r \in R\{t\}[\frac{1}{a}]$. Replace h with ha^m for a sufficiently large $m \in \mathbb{N}$ to get $gh \in R\{t\}$. □

2.3. **Analytic rings.** We now construct the analytic rings and fields for the patching machinery. For the rest of this section we fix the following setup:

Setup 2.10. Let I be a finite index set. For each $i \in I$ let a_i be a non-invertible element of R such that a_i, a_j are co-prime (as elements of the Dedekind domain R) for distinct $i, j \in I$. For each $J \subseteq I$, set $a_J = \prod_{j \in J} a_j$ (for $J = \emptyset$ put $a_\emptyset = 1$) and let $R_J = R[\frac{1}{a_J}]$. For each $i \in I$, set $a_i' = a_{I\setminus\{i\}}, z_i = \frac{a_i'}{a_i}, R_i = R_{I\setminus\{i\}}$ and $R_i' = R_{\{i\}}$. □

Lemma 2.11. *For each $J \subseteq I$ the ring R_J equals $R[z_j : j \in J]$ (the subring of K generated over R by all z_j with $j \in J$).*

Proof. Since R is a Dedekind domain, so is its overring $R[z_j : j \in J]$ (see [FJ08, Proposition 2.4.7]), which therefore equals the intersection of the valuation rings R_v of K lying above it. Since the a_i are coprime, $R[z_j : j \in J] \subseteq R_v$ if and only if $v(a_j) = 0$ for each $j \in J$, equivalently, if and only if $v(a_J) = 0$. Thus $R[z_j : j \in J] = \bigcap_{v \in \mathcal{F}\setminus\mathcal{F}_{a_J}} R_v = R[\frac{1}{a_J}] = R_J$. □

Lemma 2.12. *The intersection $\bigcap_{i\in I} R_i$ equals R.*

Proof. Let $v \in \mathcal{F}$. If there exists $i \in I$ such that $v(a_i') > 0$, then $v(a_j) > 0$ for some $j \neq i$, hence (since a_k is co-prime to a_j for each $k \neq j$) we have $v(a_j') = 0$, which implies that $\bigcap_{k\in I} R_k \subseteq R_j = R[\frac{1}{a_j'}] \subseteq R_v$. If $v(a_i') = 0$ for all $i \in I$, then also $\bigcap_{k\in I} R_k \subseteq R_v$. Thus $\bigcap_{k\in I} R_k \subseteq \bigcap_{v\in\mathcal{F}} R_v = R$. □

Proposition 2.13. *For each $i \in I$ and $y \in R_I$ there exist $y_i \in R_i$ and $y_i' \in R_i'$ such that $y = y_i + y_i'$.*

Proof. Let $y \in R_I$. By Lemma 2.11 we have $R_I = R[z_j : j \in I], R_i = R[z_j : j \neq i]$ and $R_i' = R[z_i]$. Thus without loss of generality we may assume that y is a monomial of the form $b\prod_{j\in I} z_j^{e_j}$ with $b \in R$ and e_j a non-negative integer for each $j \in I$. We list the elements of I as $\{i_1, \ldots, i_n\}$ such that $i = i_1$ and $e_{i_2} \leq e_{i_3} \leq \ldots \leq e_{i_n}$. Note that for distinct $j, k \in I$ we have

$$z_j \cdot z_k = \frac{\prod_{l\in I} a_l}{a_j^2} \cdot \frac{\prod_{l\in I} a_l}{a_k^2} = \frac{\prod_{l\in I} a_l^2}{a_j^2 a_k^2} = \prod_{l\neq j,k} a_l^2 \in R.$$

Thus, we have

$$z_{i_2}^{e_{i_2}} \cdot z_{i_3}^{e_{i_3}} = (z_{i_2} \cdot z_{i_3})^{e_{i_2}} \cdot z_{i_3}^{e_{i_3}-e_{i_2}} = c \cdot z_{i_3}^{e_{i_3}-e_{i_2}}$$

for some $c \in R$. Replace b with $b \cdot c$ and e_{i_3} with $e_{i_3} - e_{i_2}$ to assume that $e_{i_2} = 0$. Proceeding by induction we may assume that $e_{i_2} = e_{i_3} = \ldots = e_{i_{n-1}} = 0$. So

$y = b \cdot z_{i_1}^{e_{i_1}} \cdot z_{i_n}^{e_{i_n}}$. If $e_{i_n} \geq e_{i_1}$, then $y \in R[z_{i_n}] \subseteq R[z_j : j \neq i_1] = R[z_j : j \neq i] = R_i$, and if $e_{i_n} < e_{i_1}$, then $y \in R[z_{i_1}] = R[z_i] = R_i'$, as needed. □

For the rest of this section, set $D = R\{t\}$ and $E = \mathrm{Quot}(D)$. We wish to construct "analytic fields" over E.

Construction 2.14. Suppose the index set I contains 1 (as a symbol) and let $J \subseteq I$. If $1 \notin J$, put $D_J = R_J\{t\}$, and if $1 \in J$, put $D_J = R_J[[t]]$. For each $i \in I$, let $D_i = D_{I\setminus\{i\}}$ and $D_i' = D_{\{i\}}$. We view all these rings as contained in the common ring $D_I = R_I[[t]]$. Note that

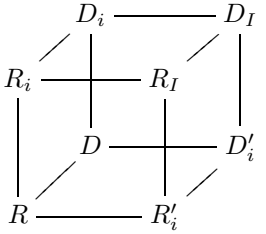
$$D_\emptyset = R\{t\} = D,$$

$$D_1 = D_{I\setminus\{1\}} = R_1\{t\}, \quad D_1' = D_{\{1\}} = R_1'[[t]]$$

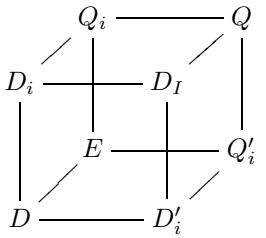
and

$$D_i = D_{I\setminus\{i\}} = R_i[[t]], \quad D_i' = D_{\{i\}} = R_i'\{t\}$$

for each $i \neq 1$.



Let $Q_J = \mathrm{Quot}(D_J)$, and note that $Q_\emptyset = \mathrm{Quot}(R\{t\}) = E$. Let $Q = \mathrm{Quot}(D_I)$, and for each $i \in I$ put $Q_i = Q_{I\setminus\{i\}} = \mathrm{Quot}(D_i)$, $Q_i' = \bigcap_{j\neq i} Q_j$. Note that $E, D_i' \subseteq Q_i'$ for each $i \in I$, since $D_i' \subseteq D_j$ for each $i \neq j \in I$.



□

For the rest of this section we fix the notation of Construction 2.14.

Proposition 2.15. *The intersection $\bigcap_{i\in I} Q_i$ equals E.*

Proof. Let $y \in \bigcap_{i\in I} Q_i$. For each $i \in I$, by Corollary 2.9 there exists $p_i \in R\{t\}$ such that $p_i y \in D_i$. Put $p = \prod_{i\in I} p_i$. Then $py \in \bigcap_{i\in I} R_i[[t]]$ and $py \in D_1 \subseteq K\{t\}$. It follows from Lemma 2.12 that $py \in R\{t\}$, hence $y = \frac{py}{p} \in \mathrm{Quot}(R\{t\}) = E$. □

For any domain R we denote the t-adic absolute value on $R[[t]]$ by $|\cdot|_t$. That is, we let $|f|_t = e^{-v_t(f)}$, where v_t is the (normalized) t-adic valuation on $R[[t]]$. Recall that C_1 is the constant C_g from Lemma 2.6 for $g = 1$.

Proposition 2.16. *For each $f \in D_I$ and $i \in I$ there exist $g = \sum_{n=0}^\infty g_n t^n \in D_i', h = \sum_{n=0}^\infty h_n t^n \in D_i$ such that $f = g + h$ and $|g|_t \leq |f|_t$ and $|h|_t \leq |f|_t$. Moreover, if $i = 1$, then $||h_n|| < C_1$, and if $i \neq 1$, then $||g_n|| < C_1$, for all $n \geq 0$.*

Proof. Let $f = \sum_{n=m}^{\infty} f_n t^n \in D_I$ with $f_m \neq 0$. For each $n \geq m$, Proposition 2.13 gives $g_n \in R_i', h_n \in R_i$ such that $f_n = g_n + h_n$. By Lemma 2.6 we may add an element of R to g_n and subtract it from h_n to assume that: If $i = 1$, then $||h_n|| < C_1$, and if $i \neq 1$, then $||g_n|| < C_1$. Then $g = \sum_{n=m}^{\infty} g_n t^n \in R_i'[[t]], h = \sum_{n=m}^{\infty} h_n \in R_i[[t]]$ satisfy $f = g + h$. Moreover, if $i = 1$, then $h \in R_i\{t\} = D_i$, $g \in R_i'[[t]] = D_i'$, and if $i \neq 1$, then $g \in R_i'\{t\} = D_i'$, $h \in R_i[[t]] = D_i$. Clearly, $|g|_t \leq |f|_t$, $|h|_t \leq |f|_t$. □

Construction 2.17. Consider the case where K is a finite Galois extension of a subfield K_0 with $a_1, a_I \in K_0^{\times}$, and suppose there is an action of $\Gamma = \mathrm{Gal}(K/K_0)$ on the set I, such that $a_i^{\gamma} = a_{i^{\gamma}}$ for all $i \in I, \gamma \in \Gamma$. Since R is the ring of integers of K, Γ acts on R. Since $a_I \in K_0$ we have $a_I^{\gamma} = a_I$ for all $\gamma \in \Gamma$, hence Γ acts on $R_I = R[\frac{1}{a_I}]$. For each $J \subseteq I$ and $\gamma \in \Gamma$ we have $R_J^{\gamma} = R[\frac{1}{a_J^{\gamma}}] = R[\frac{1}{a_{J^{\gamma}}}] = R_{J^{\gamma}}$.

The action of Γ on R_I extends to an action of Γ on $R_I[[t]]$ (coefficient-wise). Let J be a subset of I and let $\gamma \in \Gamma$. If $1 \in J$, then also $1 = 1^{\gamma} \in J^{\gamma}$, hence $D_J^{\gamma} = R_J[[t]]^{\gamma} = (R_J)^{\gamma}[[t]] = R_{J^{\gamma}}[[t]] = D_{J^{\gamma}}$. Suppose $1 \notin J$. Then $1 = 1^{\gamma} \notin J^{\gamma}$. If $f \in D_J$, then $\sigma(f) \in \mathbb{C}_{1^-}[[t]]$ for all $\sigma \in \mathrm{Hom}(K, \mathbb{C})$. Since $\sigma(f^{\gamma}) = (\sigma \circ \gamma)(f)$ and $\sigma \circ \gamma \in \mathrm{Hom}(K, \mathbb{C})$, $f^{\gamma} \in R_{J^{\gamma}}[[t]]$ also satisfies $\sigma(f^{\gamma}) \in \mathbb{C}_{1^-}[[t]]$ for all $\sigma \in \mathrm{Hom}(K, \mathbb{C})$. Thus in this case as well we have $D_J^{\gamma} = D_{J^{\gamma}}$.

Thus the action of Γ extends to $Q = \mathrm{Quot}(D_I)$ (by $(\frac{f}{g})^{\gamma} = \frac{f^{\gamma}}{g^{\gamma}}$), satisfying $Q_i^{\gamma} = Q_{i^{\gamma}}, (Q_i')^{\gamma} = Q_{i^{\gamma}}'$ for all $i \in I, \gamma \in \Gamma$. Note also that $E^{\gamma} = E$ for each $\gamma \in \Gamma$, since $R^{\gamma} = R$. □

3. Matrix factorization

We now combine the additive decomposition $D_I = D_i + D_i'$ of Proposition 2.16 with the "Weierstrass division" of Proposition 2.8 and some completeness arguments to get a matrix factorization result for the quotient fields of our analytic rings (Corollary 3.6).

Remark 3.1. Let D be a domain, equipped with a norm $|\cdot|$. For each $n \geq 1$, $|\cdot|$ extends to a metric on the ring of $n \times n$-matrices $\mathrm{Mat}_n(D)$ by $|(a_{ij})_{1 \leq i,j \leq n}| = \max_{i,j} |a_{ij}|$, satisfying $|a + b| \leq |a| + |b|$ and $|ab| \leq n|a||b|$ (and if $|\cdot|$ is ultrametric, then $|a + b| \leq \max\{|a|, |b|\}, |ab| \leq |a||b|$). Clearly, D is complete w.r.t. $|\cdot|$ if and only if $\mathrm{Mat}_n(D)$ is complete for each $n \geq 1$. □

Proposition 3.2. *Let A be a domain equipped with an ultrametric absolute value $|\cdot|$ and let A_0 be a dense subring, such that $A = A_0 + gA$ for each $0 \neq g \in A_0$. Put $E = \mathrm{Quot}(A), E_0 = \mathrm{Quot}(A_0)$ and let E_1, E_2 be subfields of E such that $E_0 \subseteq E_2$. Let $n \in \mathbb{N}$ and suppose that:*

(i) *The localization $(A_0 \setminus \{0\})^{-1}A$ equals E.*
(ii) *For for each $b \in \mathrm{Mat}_n(A)$ with $|b - \mathbb{1}| < 1$ (where $\mathbb{1}$ is the identity matrix of rank n), there exist $b_1 \in \mathrm{GL}_n(E_1), b_2 \in \mathrm{GL}_n(E_2)$ such that $b = b_1 b_2$.*

Then $\mathrm{GL}_n(E) = \mathrm{GL}_n(E_1) \cdot \mathrm{GL}_n(E_2)$.

Proof. Let $b \in \mathrm{GL}_n(E)$. By (i) there exists $0 \neq h \in A_0$ such that $hb \in \mathrm{Mat}_n(A)$. If $hb = b_1 b_2'$ with $b_1 \in \mathrm{GL}_n(E_1)$, $b_2' \in \mathrm{GL}_n(E_2)$, then $b = b_1 b_2$, where $b_2 = \frac{1}{h} b_2' \in \mathrm{GL}_n(E_2)$. So we may assume that $b \in \mathrm{Mat}_n(A)$. Let $0 \neq d = \det(b) \in A$. Let $b'' \in \mathrm{Mat}_n(A)$ be the adjugate matrix of b, so that $bb'' = d\mathbb{1}$. By (i) again, there

exists $0 \neq f \in A, 0 \neq g \in A_0$ such that $\frac{1}{d} = \frac{f}{g}$. Set $b' = fb''$. Then $b' \in \mathrm{Mat}_n(A)$ and $bb' = g\mathbb{1}$. Put

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

Then V is an additive subgroup of $\mathrm{Mat}_n(A)$ and $g\mathrm{Mat}_n(A) \leq V$. Since $A = A_0 + gA$, we also have $\mathrm{Mat}_n(A) = \mathrm{Mat}_n(A_0) + g\mathrm{Mat}_n(A)$, hence $V = V_0 + g\mathrm{Mat}_n(A)$. Since A_0 is dense in A, $\mathrm{Mat}_n(A_0)$ is dense in $\mathrm{Mat}_n(A)$, hence $g\mathrm{Mat}_n(A_0)$ is dense in $g\mathrm{Mat}_n(A)$. It follows that $V_0 = V_0 + g\mathrm{Mat}_n(A_0)$ is dense in $V = V_0 + g\mathrm{Mat}_n(A)$. Since $b' \in V$, there exists $a_0 \in V_0$ with $|b' - a_0| < \frac{|g|}{|b|}$. In particular, $a_0 \in \mathrm{Mat}_n(A_0)$ and $ba_0 \in g\mathrm{Mat}_n(A)$.

Put $a = \frac{1}{g}a_0 \in \mathrm{Mat}_n(E_0)$. Then $ba = \frac{1}{g}ba_0 \in \mathrm{Mat}_n(A)$ and $|\mathbb{1} - ba| = |\frac{1}{g}b(b' - a_0)| \leq \frac{1}{|g|}|b||b' - a_0| < 1$. By (ii), there exist $b_1 \in \mathrm{GL}_n(E_1)$, $b_2' \in \mathrm{GL}_n(E_2)$ such that $ba = b_1b_2'$. In particular, $\det(a) \neq 0$, hence $a \in \mathrm{GL}_n(E_0)$. Thus $b = b_1b_2$ for $b_2 = b_2'a^{-1} \in \mathrm{GL}_n(E_2)\mathrm{GL}_n(E_0) = \mathrm{GL}_n(E_2)$. □

Lemma 3.3. *Let D be a domain complete with respect to a norm $|\cdot|$. Let $(a_k)_{k=1}^{\infty}$ be a sequence of matrices in $\mathrm{Mat}_n(D)$ such that $\sum_{k=1}^{\infty} |a_k| < \infty$. Then the infinite products $\ldots \cdot (\mathbb{1} + a_2) \cdot (\mathbb{1} + a_1)$ and $(\mathbb{1} + a_1) \cdot (\mathbb{1} + a_2) \cdot \ldots$ both converge in $\mathrm{Mat}_n(D)$. Moreover, if each $\mathbb{1} + a_k$ is invertible, so is each of the products.*

Proof. The proof is verbally the same as the proof of [Har84b, Lemma 2.2] (where the lemma is proven for specific complete normed domains). □

Remark 3.4. If $(f_k)_{k\in\mathbb{N}}$ is a sequence in $\mathbb{C}_r[[t]]$ that converges both with respect to $|\cdot|_t$ in $\mathbb{C}[[t]]$ and with respect to $|\cdot|_r$ in $\mathbb{C}_r[[t]]$, then the two limits coincide. Indeed, if $g \in \mathbb{C}_r[[t]]$ with $||g - f_k||_r \to 0$, then, writing $f_k = \sum_{n=0}^{\infty} f_{kn}t^n$ and $g = \sum_{n=0}^{\infty} g_n t^n$, the Cauchy integral formula implies that $|g_n - f_{kn}| \leq ||g - f_k||_r r^{-n} \to 0$ as $k \to \infty$. Since f_k also converges t-adically, the sequence $(f_{kn})_{n\in\mathbb{N}}$ is eventually constant for every k, and therefore eventually equal to g_k. Hence, g is also the limit of $(f_k)_{k\in\mathbb{N}}$ with respect to $|\cdot|_t$. □

For the rest of this section we use the notation of Construction 2.14.

Proposition 3.5. *Let $n \in \mathbb{N}$ and let $b \in \mathrm{Mat}_n(D_I)$ satisfy $|b - \mathbb{1}|_t < 1$. Then for each $i \in I$ there exist $b_i' \in \mathrm{GL}_n(Q_i')$ and $b_i \in \mathrm{GL}_n(Q_i)$ such that $b = b_i'b_i$.*

Proof. Let C_1 be given by Lemma 2.6. By Proposition 2.16, for each $y \in \mathrm{Mat}_n(D_I)$ there exist $y^+ \in \mathrm{Mat}_n(D_i')$ and $y^- \in \mathrm{Mat}_n(D_i)$ such that $y = y^+ + y^-$ and $|y^+|_t \leq |y|_t$, $|y^-|_t \leq |y|_t$. Moreover, if $i = 1$ and λ is a coefficient of one of the entries of y^-, then $||\lambda|| < C_1$. Similarly, if $i \neq 1$ and λ is a coefficient of an entry of y^+, then $||\lambda|| < C_1$.

Write $y_1 = b - \mathbb{1}$ and $c = |y_1|_t < 1$. We recursively define a sequence of matrices $(y_j)_{j=1}^{\infty} \subseteq \mathrm{Mat}_n(D_I)$ by setting

$$y_{j+1} = y_j^+y_j^- - y_j^+y_j - y_jy_j^- + y_j^+y_jy_j^-. \tag{3.5.1}$$

Since $|\cdot|_t$ is ultrametric it follows by induction that $|y_{j+1}|_t \leq |y_j|_t^2$ and $|y_j^+|_t \leq |y_j|_t \leq c^{2^{j-1}} < 1$ for each $j \geq 1$. Thus $\det(\mathbb{1} - y_j^+) \equiv \det(\mathbb{1}) = 1 \mod (t)$, hence $\mathbb{1} - y_j^+$ is invertible in the ring $\mathrm{Mat}_n(R_i'[[t]])$ (which is complete with respect to $|\cdot|_t$) for all j. Moreover, $\sum_j |y_j^+|_t < \infty$. By Lemma 3.3, $\ldots \cdot (\mathbb{1} - y_2^+) \cdot (\mathbb{1} - y_1^+)$ converges

to a matrix $p_i' \in \mathrm{GL}_n(R_i'[[t]])$. Similarly, $(\mathbb{1} - y_1^-) \cdot (\mathbb{1} - y_2^-) \cdot \ldots$ converges to a matrix $p_i \in \mathrm{GL}_n(R_i[[t]])$. In particular, $\det(p_i), \det(p_i') \neq 0$. By (3.5.1) we have

$$\mathbb{1} + y_{j+1} = (\mathbb{1} - y_j^+)(\mathbb{1} + y_j)(\mathbb{1} - y_j^-),$$

hence

$$\mathbb{1} + y_{j+1} = (\mathbb{1} - y_j^+) \cdot \ldots \cdot (\mathbb{1} - y_1^+) \cdot b \cdot (\mathbb{1} - y_1^-) \cdot \ldots \cdot (\mathbb{1} - y_j^-)$$

for all j. Taking the t-adic limit, we get $\mathbb{1} = p_i' \cdot b \cdot p_i$.

Suppose $i \neq 1$. Since $|y_j^+|_t \leq c^{2^{j-1}} \leq c^j$ for all j, it follows that each of the entries of y_j^+ is divisible by t^j. Let $0 < r < 1$ and suppose $f \in D_i'$ is one of the entries of y_j^+. Then we may write $f = t^j(\sum_{m=0}^{\infty} f_m t^m)$, hence for each $\sigma \in \mathrm{Hom}(K, \mathbb{C})$ we have $|\sigma(f)|_r \leq r^j(\sum_{m=0}^{\infty} C_1 r^m) = r^j \cdot \frac{C_1}{1-r}$. It follows that $|\sigma(y_j^+)|_r \leq r^j \cdot \frac{C_1}{1-r}$ (where $\sigma(y_j^+)$ is the matrix obtained by applying σ to all of the entries). Thus, $\sum_{j=1}^{\infty} |\sigma(y_j^+)|_r \leq \sum_{j=1}^{\infty} r^j \cdot \frac{C_1}{1-r} = r \cdot \frac{C_1}{(1-r)^2} < \infty$. By Lemma 3.3, $\ldots \cdot (\mathbb{1} - \sigma(y_2^+)) \cdot (\mathbb{1} - \sigma(y_1^+))$ converges w.r.t. $|\cdot|_r$ to an element of $\mathrm{Mat}_n(\mathbb{C}_r[[t]])$, which by Remark 3.4 must equal $\sigma(p_i')$. We conclude that $p_i' \in \mathrm{Mat}_n(D_i')$. Note that since $i \neq 1$, $p_i \in \mathrm{GL}_n(R_i[[t]]) = \mathrm{GL}_n(D_i)$.

Similarly, if $i = 1$ we get that $p_i \in \mathrm{Mat}_n(D_i), p_i' \in \mathrm{GL}_n(D_i')$. Thus in both cases, $p_i \in \mathrm{Mat}_n(Q_i), p_i' \in \mathrm{Mat}_n(Q_i')$, and since $\det(p_i) \neq 0, \det(p_i') \neq 0$ we conclude that $p_i \in \mathrm{GL}_n(Q_i), p_i' \in \mathrm{GL}_n(Q_i')$. Write $b_i = p_i^{-1}, b_i' = (p_i')^{-1}$. Then $b = b_i' \cdot b_i$. □

Corollary 3.6. *For each $i \in I$ and $n \in \mathbb{N}$ we have*

$$\mathrm{GL}_n(Q) = \mathrm{GL}_n(Q_i') \cdot \mathrm{GL}_n(Q_i) = \mathrm{GL}_n(Q_i) \cdot \mathrm{GL}_n(Q_i').$$

Proof. Let $i \in I$ and put $A = D_I$, $A_0 = R\{t\} \cdot R_I$, $E = Q$, $E_1 = Q_i'$, $E_2 = Q_i$. Then A is complete with respect to the ultrametric absolute value $|\cdot|_t$, and A_0 is $|\cdot|_t$-dense in A, since A_0 contains the ring $R_I[t]$. By Proposition 2.8, $A = A_0 + gA$ for each $0 \neq g \in A$. Clearly, $E_0 = \mathrm{Quot}(A_0) \subseteq E_2$. Condition (i) of Proposition 3.2 holds by Corollary 2.9 and condition (ii) holds by Proposition 3.5, thus $\mathrm{GL}_n(Q) = \mathrm{GL}_n(Q_i') \cdot \mathrm{GL}_n(Q_i)$. Consequently, $\mathrm{GL}_n(Q) = \mathrm{GL}_n(Q)^{-1} = \mathrm{GL}_n(Q_i)^{-1}\mathrm{GL}_n(Q_i')^{-1} = \mathrm{GL}_n(Q_i)\mathrm{GL}_n(Q_i')$. □

Remark 3.7. It is unknown to the authors whether the above matrix factorization results hold for the base rings. That is, whether $\mathrm{GL}_n(D_I) = \mathrm{GL}_n(D_i)\mathrm{GL}_n(D_i')$ for $i \in I$. In the case where $K = \mathbb{Q}$, the answer is positive, and a proof is given in [Har84b, Proposition 2.3]. However, that proof does not generalize to arbitrary number fields (the critical point is that for $\mathbb{Z}$, the bound C_1 given by Lemma 2.6 is 1, which ensures invertibility of certain convergent power series on the open unit disc). However, for our constructions to work, matrix factorization over the quotient fields is precisely the needed result. □

4. Cyclic extensions

As before, let K be a number field with ring of integers $R = \mathcal{O}_K$, and let $n = [K : \mathbb{Q}]$. In this section we construct cyclic Galois extensions of $E = \mathrm{Quot}(R\{t\})$ and embed them into the quotient fields of our analytic rings.

Remark 4.1. We associate to K its **Minkowski space** $K_{\mathbb{R}}$, defined as follows. Let $\rho_1, \ldots, \rho_r \in \mathrm{Hom}(K, \mathbb{R})$ denote the real, and $\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s \in \mathrm{Hom}(K, \mathbb{C})$ the

complex embeddings of K into $\mathbb{C}$. Then $K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$, and we have an embedding $\iota\colon K \to K_{\mathbb{R}}$ given by

$$\iota(x) = (\rho_1(x), \dots, \rho_r(x), \sigma_1(x), \dots, \sigma_s(x))$$

for each $x \in K$. Note that $n = r + 2s$. We identify $K_{\mathbb{R}}$ with $\mathbb{R}^n$ via the standard isomorphism $\mathbb{C} \to \mathbb{R}^2$.

For any $\mathbb{R}$-basis $B = (b_1, \dots, b_n)$ of $\mathbb{R}^n$, the norm on $\mathbb{R}^n$ defined by

$$\left\| \sum_i x_i b_i \right\|_B = \max_i |x_i|, \quad x_1, \dots, x_n \in \mathbb{R},$$

is equivalent to the Euclidean norm $|\cdot|_{\mathbb{R}^n}$. In particular, $|\cdot|_{\mathbb{R}^n}$ is equivalent to $||\cdot||_e$, where e is the standard basis of $\mathbb{R}^n$, so the norms $||\cdot||$ (see Remark 2.2) and $|\cdot|_{\mathbb{R}^n} \circ \iota$ are equivalent on K.

Lemma 4.2. *If $a \neq 0$ is a non-invertible element of R, then there exists $0 \neq b \in \mathbb{Z}[\frac{1}{a}]$ with $||b|| < 1$.*

Proof. Since a^{-1} is not integral over $\mathbb{Z}$, $\mathbb{Z}[a^{-1}]$ is not finitely generated as a $\mathbb{Z}$-module. Thus (in the notation of Remark 4.1) $\iota(\mathbb{Z}[a^{-1}])$ is a subgroup but not a lattice of $\mathbb{R}^n$, i.e. a non-discrete subgroup [Neu99, Proposition I.4.2]. Since the norm induced on K by $|\cdot|_{\mathbb{R}^n}$ is equivalent to $||\cdot||$, the claim follows. □

Proposition 4.3. *Let K be a number field with ring of integers $R = \mathcal{O}_K$. Let $k \in \mathbb{N}$ and suppose that K contains a root of unity of order k. Let $a \in R \setminus R^\times$ and $A = R[\frac{1}{a}]$. Put $B = A\{t\}$, $E = \mathrm{Quot}(R\{t\})$, and $L = \mathrm{Quot}(B)$. Then there exists a Galois extension F of E contained in L, with $\mathrm{Gal}(F/E) \cong \mathbb{Z}/k\mathbb{Z}$.*

Proof. Consider the polynomial $p(X) = X^k - (1 - k^2 t)$. We first claim it has a root in $\mathbb{Z}[[t]]$. Indeed, $p'(1) = k, p(1) = k^2 t \in p'(1)^2 t\mathbb{Z}[[t]]$. By the general Hensel's Lemma [Eis95, Theorem 7.3] (for the t-adically complete domain $\mathbb{Z}[[t]]$), there exists $f(t) \in \mathbb{Z}[[t]]$ with $p(f(t)) = 0$. Now view $f(t)$ as a formal power series in $\mathbb{C}[[t]]$, algebraic over $\mathbb{C}[t]$. By [Art68, Theorem 2.14], the field of formal power series in $\mathbb{C}((t))$ which converge at some non-zero point is algebraically closed in $\mathbb{C}((t))$, in particular $f(t)$ converges at some non-zero point. Thus, there exists $r > 0$ such that $f(t)$ converges on the open disc of radius r around the origin.

By Lemma 4.2 there exists $0 \neq b \in A$ with $||b|| < 1$, hence also $|\mathrm{norm}_{K/\mathbb{Q}}(b)| < 1$, which implies that $b \notin R$ (otherwise $\mathrm{norm}_{K/\mathbb{Q}}(b) \in \mathbb{Z}$). Thus there exists a non-archimedean prime $\mathfrak{p}$ of R such that $v_{\mathfrak{p}}(b) < 0$ (where $v_{\mathfrak{p}}$ is the corresponding discrete valuation on K). Let $m \in \mathbb{N}$ be a sufficiently large integer such that $||b^m|| < r$ and $v_{\mathfrak{p}}(b^m) < -v_{\mathfrak{p}}(k^2)$. Put $g(t) = f(tb^m) \in A[[t]]$. Then for each $\lambda \in \mathbb{C}$ with $|\lambda| < 1$ we have $|\lambda \cdot \sigma(b^m)| < r$, hence $\sigma(g)(\lambda) = f(\lambda \cdot \sigma(b^m))$ converges. It follows that $g(t) \in B$. Moreover, $g(t)$ is a root of the polynomial $q(X) = X^k - (1 - (k^2 \cdot b^m)t) \in E[X]$.

We next claim that $q(X)$ is irreducible over E. Let O be the completion of the localization $R_{\mathfrak{p}}$. By our assumptions, $\frac{1}{b^m \cdot k^2} \in \mathfrak{p}R_{\mathfrak{p}}$, hence by [Bou72, Ch. VII, §3, Prop. 8, p. 511] and [Bou72, Ch. VII, §3, Cor. to Prop. 7, p. 510] the element $s = \frac{1}{b^m \cdot k^2} - t$ is a prime element of the ring $O[[t]]$, hence defines an s-adic valuation w_s on $\Omega = \mathrm{Quot}(O[[t]])$. Then $w_s(s) = 1$ and $w_s(c) = 0$ for each constant $c \in K^\times$. By the generalized Eisenstein Criterion [Cas86, Section 6, Theorem 2.1], the polynomial $r(X) = \frac{1}{b^m k^2} \cdot q(X) = \frac{1}{b^m k^2} \cdot X^k - (\frac{1}{b^m k^2} - t) \in O[[t]][X]$ is irreducible over Ω, hence $q(X)$ is irreducible over Ω and hence irreducible over the subfield E.

Let F be the splitting field of $q(X)$ over E. Since $K \subseteq E$ contains a primitive k-th root of unity, F/E is a Kummer extension with Galois group $\mathbb{Z}/k\mathbb{Z}$. Since $q(X)$ has a root $g(t) \in L$, we have $F \subseteq L$. □

5. Algebraic extensions of rings of power series

Let R be an integral domain with quotient field K. Let $R[[t]]$ be the ring of formal power series over R, viewed as a subring of

$$B := \bigcup_{0 \neq a \in R} R[[\frac{t}{a}]]$$

(the union taken inside $K((t))$). Put $F = \mathrm{Quot}(B)$. The goal of this section is to show that F is separably closed in $K((t))$. This result may be viewed as an arithmetic version of the theorem of Artin [Art68, Theorem 2.14] concerning convergent power series (with respect to an absolute value). Our proof is an adaptation of the proof of [Par08, Proposition 3.10].

Lemma 5.1. *Let $h(Y) = p_d Y^d + \ldots + p_1 Y + p_0 \in K[[t]][Y]$ be a polynomial over $K[[t]]$. Suppose that for each $0 \leq k \leq d$ we have $p_k = \sum_{n=0}^{\infty} b_{k,n} t^n$, where $\{b_{k,n}\} \subseteq K$ satisfy $b_{0,0} = 0, b_{1,0} = 1, b_{2,0} = \cdots = b_{d,0} = 0$. Suppose $y = \sum_{n=0}^{\infty} a_n t^n \in K[[t]]$ is a root of h. Then for each $n \geq 1$, a_n is a sum of products of the form $\pm b_{k,j_0} a_{j_1} a_{j_2} \cdots a_{j_k}$, with $0 \leq k \leq d$, $0 \leq j_0 \leq n$, $0 < j_1, \ldots, j_k < n$ such that $j_0 + j_1 + \ldots + j_k = n$.*

Proof. The proof is the same as the proof of [Par08, Lemma 3.9], with F there replaced by K here. Note that the assumption in [Par08, Lemma 3.9] that almost all of the coefficients are zero is not used in the proof. □

Remark 5.2. Let $y(t) = \sum_{n=0}^{\infty} a_n t^n \in K[[t]]$. If $y(at) \in B$ for some $0 \neq a \in R$, then $y(t) \in B$. Indeed, $y(at) \in B$ implies the existence of $b \in R$ such that $y(at) \in R[[\frac{t}{b}]]$, which implies that $y(t) \in R[[\frac{t}{ab}]] \subseteq B$. □

Proposition 5.3. *The field F is separably closed in $K((t))$.*

Proof. Let $y = \sum_{n=l}^{\infty} a_n t^n \in K((t))$ be separably algebraic over F.

Part A. A shift of y. Let $y_1, y_2, \ldots, y_d$ with $y_1 = y$ be the distinct conjugates of y over F. Then $y \in F$ if and only if $d = 1$, so suppose $d \geq 2$. Let v be the t-adic valuation on $K((t))$. Extend v to the algebraic closure of $K((t))$ and let $r = \max\{v(y - y_i) : i = 2, \ldots, d\}$ $(\neq \infty)$, $s = r + 1$. Let $y_i' = t^{-s}(y_i - \sum_{n=l}^{s} a_n t^n)$ for each $1 \leq i \leq d$. Then $y_1', \ldots, y_d'$ are the distinct conjugates of y_1' over F. Moreover, $v(y_1') \geq 1$, hence for each $2 \leq i \leq d$ we have $v(y_1' - y_i') = v(y_1 - y_i) - s \leq r - s = -1$, hence $v(y_i') \leq -1$.

Since $K(t) \subseteq F$ we may replace each y_i with y_i' to assume that $v(y) \geq 1$ and $v(y_i) \leq -1$ for each $2 \leq i \leq d$. In particular, $y = \sum_{n=0}^{\infty} a_n t^n$ with $a_0 = 0$ and $y_1, \ldots, y_d$ are the roots of an irreducible polynomial $h(Y) = p_d Y^d + \ldots + p_1 Y + p_0 \in F[Y]$.

Part B. The values of the coefficients. Multiplying by the common denominator, we may assume that $p_i \in B$ for all i. Thus for each $0 \leq i \leq d$ there exists $0 \neq \alpha_i \in R$ such that $p_i \in R[[\frac{t}{\alpha_i}]]$. Without loss of generality $a = \alpha_i$ is independent of i. By Remark 5.2, if $y(at) \in B$, then so is $y(t)$. Thus we may replace each $p_i(t)$ with $p_i(at)$ to assume that $p_i(t) \in R[[t]]$.

By [Par08, Lemma 3.8] we have $e := v(p_1) < v(p_i)$ for each $i \neq 1$. Divide the p_i by t^e to assume that $v(p_1) = 0 < v(p_i)$ for each $i \neq 1$. Therefore for each $0 \leq k \leq d$ we have $p_k = \sum_{n=0}^{\infty} b_{k,n} t^n$, where $b_{k,n} \in R$, $b_{1,0} \neq 0$, and for each $k \neq 1$ we have $b_{k,0} = 0$. Put $\beta = b_{1,0}$.

By Remark 5.2 it suffices to show that $\tilde{y}(t) = y(\beta t) \in B$. The substitution $t \mapsto \beta t$ defines an automorphism of $K((t))$, hence the following equality follows from $h(y) = 0$:

$$\frac{p_d(\beta t)}{\beta}\tilde{y}^d + \ldots + \frac{p_1(\beta t)}{\beta}\tilde{y} + \frac{p_0(\beta t)}{\beta} = 0.$$

The coefficients in this equality are all in $R[[t]]$, in particular

$$\frac{p_1(\beta t)}{\beta} = \frac{\beta + b_{1,1}\beta t + \ldots}{\beta} = 1 + b_{1,1}t + \ldots,$$

hence without loss of generality we may assume that $\beta = 1$.

Part C. The coefficients a_n. By Lemma 5.1, for each n, a_n is a sum of products of the form $\pm b_{k,j_0} a_{j_1} a_{j_2} \cdots a_{j_k}$, with $0 \leq k \leq d, 0 \leq j_0 \leq n, 0 < j_1, \ldots, j_k < n$ such that $j_0 + j_1 + \ldots + j_k = n$.

We now claim that $a_n \in R$ for all $n \geq 0$. Indeed, $a_0 = 0 \in R$. Assume that $a_m \in R$ for each $0 \leq m \leq n-1$. Then, each summand in a_n belongs to R, hence $a_n \in R$. Thus $y(t) \in R[[t]] \subseteq B \subseteq F$. □

Corollary 5.4. *Suppose K_0 is a number field and K is a finite Galois extension of K_0. Let R_0 be the ring of integers of K_0, and let R be the ring of integers of K. Put $E = \mathrm{Quot}(R\{t\})$ and let F be a finite Galois extension of E. Suppose ϕ is a K-rational place of F extending the place $t \mapsto 0$ of E, and that ϕ is unramified in F/E. Then there exists an E-embedding of F into $\mathrm{Quot}(R[\frac{1}{a}][[t]])$, for some $0 \neq a \in R_0$.*

Proof. Since ϕ is K-rational and unramified in $F/K(t)$, the completion of F at ϕ is isomorphic to $K((t))$, and therefore we can assume that $E \subseteq F \subseteq K((t))$. Since $E = \mathrm{Quot}(R\{t\}) \subseteq \mathrm{Quot}(R[[t]])$, Proposition 5.3 implies that $F \subseteq \mathrm{Quot}(R[[\frac{t}{b}]])$ for some $0 \neq b \in R$. Let $0 \neq a = \mathrm{norm}_{K/K_0}(b) \in R_0$. Then $R[[\frac{t}{b}]] \subseteq R[[\frac{t}{a}]]$, hence $F \subseteq \mathrm{Quot}(R[[\frac{t}{a}]]) \subseteq \mathrm{Quot}(R[\frac{1}{a}][[t]])$. □

6. Solution of split embedding problems

In this section we finally prove our Main Theorem. We start by recalling a few definitions:

Definition 6.1. Let E_0/K_0 be a regular field extension. A **finite split embedding problem** (FSEP) over E_0 is an epimorphism $\Gamma_1 \ltimes H \to \Gamma_1$, where $\Gamma_1 = \mathrm{Gal}(F_1/E_0)$ for some finite Galois extension F_1 of E_0, and Γ_1 acts on the finite group H. A **solution** to the FSEP $\Gamma_1 \ltimes H \to \Gamma_1$ is a finite Galois extension F of E_0 that contains F_1, such that $\mathrm{Gal}(F/E_0) \cong \Gamma_1 \ltimes H$ and the restriction of automorphisms from F to F_1 coincides with the projection from $\Gamma_1 \ltimes H$ onto Γ_1. Let K be the algebraic closure of E_0 in F_1. The solution F is **K_0-regular** if K is algebraically closed in F.

Note that any FSEP $\mathrm{Gal}(L_0/K_0) \ltimes H \to \mathrm{Gal}(L_0/K_0)$ over K_0 gives rise to an FSEP $\mathrm{Gal}(E_0L_0/E_0) \ltimes H \to \mathrm{Gal}(E_0L_0/E_0)$ over E_0, and $\mathrm{Gal}(E_0L_0/E_0) \cong \mathrm{Gal}(L_0/K_0)$. A **solution over** E_0 to an embedding problem over K_0 is a solution to the induced embedding problem over E_0. □

Lemma 6.2. *Suppose E_0/K_0 is regular, E/E_0 is a finite Galois extension, and $\mathrm{Gal}(E/E_0)$ acts on a finite group G. Let E' be a finite Galois extension of E_0 that contains E, let $\mathrm{res}\colon \mathrm{Gal}(E'/E_0) \to \mathrm{Gal}(E/E_0)$ be the restriction map, and let $h\colon G' \to G$ be an epimorphism of groups. Suppose $\mathrm{Gal}(E'/E_0)$ acts on G' such that $h(\sigma^\gamma) = h(\sigma)^{\mathrm{res}(\gamma)}$ for all $\gamma \in \mathrm{Gal}(E'/E_0), \sigma \in G'$. If the FSEP*

$$\mathrm{Gal}(E'/E_0) \ltimes G' \to \mathrm{Gal}(E'/E_0)$$

has a K_0-regular solution, then so does

$$\mathrm{Gal}(E/E_0) \ltimes G \to \mathrm{Gal}(E/E_0).$$

Proof. The proof is verbally the same as the proof of [HJ98b, Lemma 1.1] (where the lemma is proven for rational function fields, but the proof works for arbitrary regular extensions). □

Proposition 6.3. *Let K be a number field and let $R = \mathcal{O}_K$ be its ring of integers. Then $R\{t\}$ is the compositum of $\mathbb{Z}\{t\}$ and R.*

Proof. Let $f = \sum_{i=0}^{\infty} f_i t^i \in R\{t\}$ and let $z = (z_1, \ldots, z_n) \in R^n$ be an integral basis of K. Let $\iota : K \to K_{\mathbb{R}}$ be the embedding of K into its Minkowski space (Remark 4.1). By [Neu99, Proposition I.5.2], $\iota(z) = (\iota(z_1), \ldots, \iota(z_n))$ is an $\mathbb{R}$-basis of $K_{\mathbb{R}}$. By Remark 4.1, $||\cdot|| = ||\cdot||_e \circ \iota$ and $||\cdot||_{\iota(z)} \circ \iota$ are equivalent on K, hence there exists $c \in \mathbb{R}$ such that $||\iota(x)||_{\iota(z)} \leq c \cdot ||x||$ for each $x \in K$.

For each i, let $f_i = \sum_{k=1}^{n} f_{ik} z_k$, $f_{ik} \in \mathbb{Z}$. Then $|f_{ik}| \leq ||\iota(f_k)||_{\iota(z)} \leq c \cdot ||f_i||$. Thus, $\limsup_i |f_{ik}|^{1/i} \leq \limsup_i ||f_i||^{1/i} \leq 1$, so $g_k := \sum_i f_{ij} t^i \in \mathbb{Z}\{t\}$ for $k = 1, \ldots, n$, hence $f = \sum_k g_k z_k \in \mathbb{Z}\{t\} \cdot R$. □

We shall need the following technical lemmas:

Lemma 6.4. *Let K_0 be a number field, let K be a finite Galois extension of K, let $R = \mathcal{O}_K$ be the ring of integers of K, and let $0 \neq b \in R$. There exists a primitive element $z \in R \setminus R^\times$ of K/K_0 such that all of its conjugates over K_0 are pairwise co-prime. Moreover, each of the conjugates of z is co-prime to b.*

Proof. Set $n = [K : K_0]$, let $R = \mathcal{O}_{K_0}$ be the ring of integers of K_0 and let $\mathcal{F}_b$ be the family of primes ideals of R which contain b. By [FJ08, Lemma 13.3.1] there exist infinitely many prime ideals of R_0 which are totally split in K/K_0. Choose such a prime $\mathfrak{p}$ of R_0, with the additional property that all of the primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ of R which lie over $\mathfrak{p}$ do not belong to the (finite) family $\mathcal{F}_b$. Since the ideal class group of a number field is finite, there exists an integer h such that $\mathfrak{q}_1^h$ is a principal ideal of R, and we denote a generator of this ideal by z. It follows that z has n distinct conjugates and that all of the conjugates are pairwise co-prime. In particular, z is a primitive element of K/K_0, and since z generated a proper ideal, $z \in R \setminus R^\times$. Since $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are not in $\mathcal{F}_b$, each of the conjugates of z is co-prime to b. □

Lemma 6.5. *Let K_0 be a number field and K a finite Galois extension of K_0. Let R be the ring of integers of K and let $0 \neq a_1 \in R$. Let J be a finite index set with $1 \notin J$. Then for each $j \in J$ there exists a primitive element $a_j \in R \setminus R^\times$ of K/K_0 such that the sequence $\{a_1\} \cup \{a_j^\gamma\}_{j \in J, \gamma \in \mathrm{Gal}(K/K_0)}$ consists of pairwise co-prime elements.*

Proof. Let $J = \{j_1, \ldots, j_m\}$. Suppose we constructed $a_{j_1}, \ldots, a_{j_{k-1}}$ (for $1 \leq k \leq m$). Then write $b = a_1 \cdot \prod_{1 \leq l \leq k-1, \gamma \in \mathrm{Gal}(K/K_0)} a_{j_l}^\gamma$ and apply Lemma 6.4 to produce

the primitive element a_{j_k}. By induction, the elements $\{a_j^\gamma\}_{j\in J,\gamma\in\mathrm{Gal}(K/K_0)}$ are pairwise co-prime and also co-prime to a_1. □

We are now ready to formulate and prove our Main Theorem:

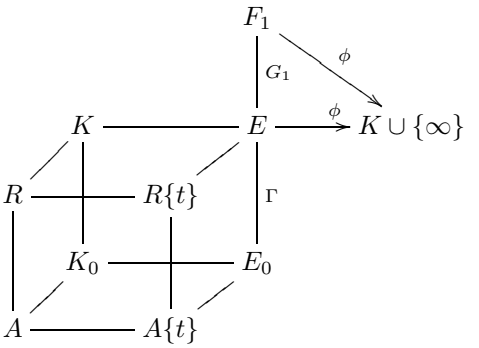
Definition 6.6. Let K_0 be a field, and E_0 an extension of K_0 contained in $K_0((t))$. An FSEP $\mathrm{Gal}(F_1/E_0)\ltimes H\to\mathrm{Gal}(F_1/E_0)$ is **t-unramified** if the t-adic valuation is unramified in F_1/E_0. □

Theorem 6.7. *Let A be the ring of integers of a number field K_0 and let $E_0=\mathrm{Quot}(A\{t\})$. Then every t-unramified finite split embedding problem over E_0 has a K_0-regular solution.*

Proof. Let F_1/E_0 be a finite Galois extension, such that the place $\phi: t\to 0$ of E_0 is unramified in F_1/E_0, and assume that $\mathrm{Gal}(F_1/E_0)$ acts on a non-trivial group H. Let K be the algebraic closure of K_0 in F_1. We wish to solve the problem $\mathrm{Gal}(F_1/E_0)\ltimes H\to\mathrm{Gal}(F_1/E_0)$ regularly over K_0.

Let $R=\mathcal{O}_K$ be the ring of integers of K, and let $E=\mathrm{Quot}(R\{t\})$. First observe that $E\subseteq F_1$. Indeed, by Proposition 6.3 we have $R\{t\}=\mathbb{Z}\{t\}\cdot R\subseteq E_0\cdot K\subseteq F_1$. Moreover, this shows that $E=E_0\cdot K$. Since $R\{t\}\subseteq K[[t]]$ we have $E\subseteq K((t))$, hence E/K is a regular extension. Similarly, E_0/K_0 is a regular extension.

Part A. Enlarging K. This part is the proof of [HJ98b, Proposition 4.2]. Extend ϕ to F_1, and let $\bar{F}_1$ be the corresponding residue field. Then $\bar{F}_1$ is a finite Galois extension of K_0 that contains K. Let $K'=\bar{F}_1(\zeta_k)$, where $k=|H|$ and ζ_k is a primitive k-th root of unity. Let $F_1'=F_1K', E'=EK'$. Then ϕ extends to a K'-rational place ϕ' of F_1', unramified over E'. Moreover, F_1'/E_0 is a Galois extension and its Galois group acts on H via the restriction $\mathrm{Gal}(F_1'/E_0)\to\mathrm{Gal}(F_1/E_0)$. By Lemma 6.2 and Proposition 6.3 we may replace F_1,E,K with F_1',E',K' to assume that ϕ is a K-rational place of F_1, unramified over E, and that $\zeta_k\in K$. Put $\Gamma=\mathrm{Gal}(K/K_0)$. Since E_0/K_0 is regular, E_0 and K are linearly disjoint over K_0, thus $\mathrm{Gal}(E/E_0)$ is isomorphic to Γ by restriction of automorphisms. Put $G_1=\mathrm{Gal}(F_1/E)$.



Part B. Patching data. By Corollary 5.4 we may assume that $F_1\subseteq\mathrm{Quot}(R[\frac{1}{a_1}][[t]])$, for some $0\neq a_1\in A$. We extend (E,F_1) to a patching data $\mathcal{E}=(E,F_i,Q_i,Q;G_i,G)_{i\in I}$ in the sense of [HJ98b, Definition 3.1], as follows: Write H as

$$H=\{\tau_j: j\in J\}, \tag{6.7.1}$$

with the index set J of cardinality as of H such that 1 (as a symbol) does not belong to J. Set $I_2=J\times\Gamma$ and let Γ act on I_2 by $(j,\gamma')^\gamma=(j,\gamma'\gamma)$. Identify

$(j,1) \in I_2$ with j, for each $j \in J$. Then every $i \in I_2$ can be uniquely written as

$$i = j^\gamma, \text{ with } j \in J \text{ and } \gamma \in \Gamma. \tag{6.7.2}$$

Let $I = \{1\} \cup I_2$ and extend the action of Γ on I_2 to I by $1^\gamma = 1$ for each $\gamma \in \Gamma$.

By Lemma 6.5, for each $j \in J$ we find a primitive element $c_j \in R \setminus R^\times$ of K/K_0, such that the elements $\{c_j^\gamma\}_{j\in J,\gamma\in\Gamma}$ are pairwise co-prime and also co-prime to a_1. For each $i \in I \setminus \{1\}$, we define an element $a_i \in R$ by writing $i = j^\gamma$ for some $j \in J, \gamma \in \Gamma$ and letting $a_i = c_j^\gamma$. Then $a_i^\gamma = a_{i^\gamma}$ for each $i \in I, \gamma \in \Gamma$ (note that this also includes the case of $i = 1$). We now use the analytic rings given by Setup 2.10 and Construction 2.14. Note that (using the notation of Setup 2.10) $a_I = \prod_{i\in I} a_i = a_1 \cdot \prod_{j\in J} \operatorname{norm}_{K/K_0}(a_j) \in K_0^\times$. Extend the action of Γ to Q by Construction 2.17. Then $Q_i^\gamma = Q_{i^\gamma}$ and $(Q_i')^\gamma = Q_{i^\gamma}'$ for all $i \in I$ and $\gamma \in \Gamma$.

Part C. Groups. This part repeats Part D of the proof of [HJ98b, Proposition 4.1].

Since $F_1 \subseteq Q$ is a Galois extension of E_0, it is Γ-invariant. The action of Γ on K is faithful, hence it is faithful on each of the fields $E \subseteq F_1 \subseteq Q$. Thus we may identify Γ with its image in $\operatorname{Gal}(F_1/E_0)$. Then $\operatorname{Gal}(F_1/E_0) = \Gamma \ltimes G_1$, where Γ acts on G_1 by conjugation in $\operatorname{Gal}(F_1/E_0)$. Thus

$$(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma} \text{ for all } a \in F_1,\ \tau \in G_1, \text{ and } \gamma \in \Gamma. \tag{6.7.3}$$

The given action of $\operatorname{Gal}(F_1/E_0)$ on H restricts to actions of its subgroups G_1 and Γ on H. Let $G = G_1 \ltimes H$ with respect to this action, and let Γ act on G componentwise by its action on G_1 and H. Then

$$\operatorname{Gal}(F_1/E_0) \ltimes H = (\Gamma \ltimes G_1) \ltimes H = \Gamma \ltimes (G_1 \ltimes H) = \Gamma \ltimes G.$$

Let $i \in I_2$. Use (6.7.2) to write $i = j^{\gamma'}$ with unique $j \in J$ and $\gamma' \in \Gamma$. Then define $\tau_i = \tau_j^{\gamma'} \in H$ and observe that

$$\tau_i^\gamma = \tau_{i^\gamma} \text{ for all } i \in I_2 \text{ and } \gamma \in \Gamma. \tag{6.7.4}$$

By (6.7.1),

$$H = \langle \tau_i : i \in I_2 \rangle. \tag{6.7.5}$$

For each $i \in I_2$ let $G_i = \langle \tau_i \rangle \leq H$. Then,

$$G = \langle G_i : i \in I \rangle \text{ and } H = \langle G_i : i \in I_2 \rangle; \tag{6.7.6}$$

$$G_i^\gamma = G_{i^\gamma} \text{ for all } i \in I \text{ and } \gamma \in \Gamma; \tag{6.7.7}$$

$$|I| \geq 2. \tag{6.7.8}$$

Part D. Solution of $\operatorname{Gal}(F_1/E_0) \ltimes H \to \operatorname{Gal}(F_1/E_0)$. Let $j \in J$. Since by the reductions made in Part A, K contains a primitive k-th root of unity, and $|G_j|$ divides $k = |H|$, Proposition 4.3 gives a cyclic extension F_j/E with group $G_j = \langle \tau_j \rangle$, such that $F_j \subseteq \operatorname{Quot}(R_j'\{t\}) = \operatorname{Quot}(D_j') \subseteq Q_j' \subseteq Q$.

For an arbitrary $i \in I_2$ there exist unique $j \in J$ and $\gamma \in \Gamma$ such that $i = j^\gamma$ (by (6.7.2)). Let $F_i = F_j^\gamma$. Since 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 $\operatorname{Gal}(F_j/E) \cong \operatorname{Gal}(F_i/E)$ which maps each $\tau \in \operatorname{Gal}(F_j/E)$ onto $\gamma \circ \tau \circ \gamma^{-1} \in \operatorname{Gal}(F_i/E)$. In particular, it maps τ_j onto $\gamma \circ \tau_j \circ \gamma^{-1}$. We may therefore identify G_i with $\operatorname{Gal}(F_i/E)$ such that τ_i coincides with $\gamma \circ \tau_j \circ \gamma^{-1}$. This means that $(y^\tau)^\gamma = (y^\gamma)^{\tau^\gamma}$ for all $y \in F_j$ and $\tau \in G_j$.

By Proposition 2.15 we have $\bigcap_{i\in I} Q_i = E$, and by Corollary 3.6 for $n = |G|$ we have $\mathrm{GL}_n(Q) = \mathrm{GL}_n(Q_i)\cdot \mathrm{GL}_n(Q_i')$ for each $i \in I$. By (6.7.6) we have $G = \langle G_i : i \in I\rangle$. Thus $\mathcal{E} = (E, F_i, Q_i, Q; G_i, G)_{i\in I}$ is a patching data in the sense of [HJ98b, Definition 3.1].

Since F_1 is invariant under Γ, 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 $\tau \in G_i$. This generalizes (6.7.3).

We have shown that Γ acts properly on $\mathcal{E}$, in the sense of [HJ98b, Definition 3.1]. By [HJ98b, Corollary 3.4(e)] the "compound" $F \subseteq Q$ of $\mathcal{E}$ is a solution for the split embedding problem $\mathrm{Gal}(F_1/E_0) \ltimes H \to \mathrm{Gal}(F_1/E_0)$. Since $K \subseteq F \subseteq Q \subseteq K((t))$ and $K((t))/K$ is regular, so is F/K. □

The field $E = \mathrm{Quot}(\mathbb{Z}\{t\})$ is Hilbertian by [FP12, Proposition 4.3]. In [DD99] it is conjectured that every FSEP over a Hilbertian field is solvable. This has been proven for function fields over ample fields in [Pop96, HJ98b]. The field E above can be viewed as an analogue of the (non-ample) field $K((x))(t)$ of rational functions over the complete (and hence ample) field $K((x))$ (where K is some field); see the discussion in [Har88, p. 855]. However, it is unclear from this analogy how to prove the non-ampleness of E. Moreover, unlike the function field case where all geometric primes play an equivalent role, in E the prime $t \mapsto 0$ is distinguished, which leads to the ramification constraint of Theorem 6.7. More precisely, in the function field case, if $t \mapsto 0$ is ramified, then one chooses a non-ramified point $a \in K$ and applies the automorphism $t \mapsto t + a$ of $K[t]$ to assume that $t \mapsto 0$ is unramified (see [HJ98b, Proof of Proposition 4.2(a)]). In contrast, the map $t \mapsto t + a$ does not extend to an automorphism of $\mathbb{Z}\{t\}$ (and not even to a $\mathbb{C}$-automorphism of $\mathbb{C}_{1^-}[[t]]$) for any $a \neq 0$. Nevertheless, Theorem 6.7 gives our main objective:

Corollary 6.8. *If K is a number field with ring of integers $\mathcal{O}_K$, then every finite split embedding problem over K has a K-regular solution over* $\mathrm{Quot}(\mathcal{O}_K\{t\})$.

Proof. Let $E = \mathrm{Quot}(\mathcal{O}_K\{t\})$ and let $\mathrm{Gal}(L/K) \ltimes H \to \mathrm{Gal}(L/K)$ be an FSEP over K. Since E/K is regular and L/K is algebraic, the t-adic valuation is totally inert in EL/E, so that the induced embedding problem $\mathrm{Gal}(EL/E) \ltimes H \to \mathrm{Gal}(EL/E)$ over E is t-unramified. Thus the claim follows from Theorem 6.7. □

Acknowledgement

We thank the referee for a careful reading and many helpful suggestions.

References

[Art68] Emil Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach Science Publishers, New York, 1967. MR0237460 (38 #5742)

[BSHH10] Lior Bary-Soroker, Dan Haran, and David Harbater, *Permanence criteria for semi-free profinite groups*, Math. Ann. **348** (2010), no. 3, 539–563, DOI 10.1007/s00208-010-0484-8. MR2677893 (2012b:20068)

[Bou72] N. Bourbaki, *Commutative Algebra*, Hermann, 1972. MR0360549

[Cas86] J. W. S. Cassels, *Local fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986. MR861410 (87i:11172)

[DD99] Pierre Dèbes and Bruno Deschamps, *The regular inverse Galois problem over large fields*, Geometric Galois actions, 2, London Math. Soc. Lecture Note Ser., vol. 243, Cambridge Univ. Press, Cambridge, 1997, pp. 119–138, DOI 10.1017/CBO9780511666124.007. MR1653011 (99j:12002)

[Eis95] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. With a view toward algebraic geometry. MR1322960 (97a:13001)

[FJ08] Michael D. Fried and Moshe Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008. Revised by Jarden. MR2445111 (2009j:12007)

[FP11] Arno Fehm and Elad Paran, *Galois theory over rings of arithmetic power series*, Adv. Math. **226** (2011), no. 5, 4183–4197, DOI 10.1016/j.aim.2010.11.010. MR2770445 (2012b:12004)

[FP12] Arno Fehm and Elad Paran. Klein approximation and Hilbertian fields. J. Reine Angew. Math. **676** (2013), 213–225. MR3028759

[Har84a] David Harbater, *Algebraic rings of arithmetic power series*, J. Algebra **91** (1984), no. 2, 294–319, DOI 10.1016/0021-8693(84)90104-2. MR769575 (86i:13007)

[Har84b] David Harbater, *Convergent arithmetic power series*, Amer. J. Math. **106** (1984), no. 4, 801–846, DOI 10.2307/2374325. MR749258 (85j:13036)

[Har88] David Harbater, *Galois covers of an arithmetic surface*, Amer. J. Math. **110** (1988), no. 5, 849–885, DOI 10.2307/2374696. MR961498 (90e:14013)

[HJ98a] Dan Haran and Moshe Jarden, *Regular split embedding problems over complete valued fields*, Forum Math. **10** (1998), no. 3, 329–351, DOI 10.1515/form.10.3.329. MR1619723 (99e:12007)

[HJ98b] Dan Haran and Moshe Jarden, *Regular split embedding problems over function fields of one variable over ample fields*, J. Algebra **208** (1998), no. 1, 147–164, DOI 10.1006/jabr.1998.7454. MR1643991 (99h:12005)

[HS05] David Harbater and Katherine F. Stevenson, *Local Galois theory in dimension two*, Adv. Math. **198** (2005), no. 2, 623–653, DOI 10.1016/j.aim.2005.06.011. MR2183390 (2007e:12002)

[HV96] Dan Haran and Helmut Völklein, *Galois groups over complete valued fields*, Israel J. Math. **93** (1996), 9–27, DOI 10.1007/BF02761092. MR1380632 (97c:12002)

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; with a foreword by G. Harder. MR1697859 (2000m:11104)

[Par08] Elad Paran, *Algebraic patching over complete domains*, Israel J. Math. **166** (2008), 185–219, DOI 10.1007/s11856-008-1027-9. MR2430432 (2009e:12006)

[Par09] Elad Paran, *Split embedding problems over complete domains*, Ann. of Math. (2) **170** (2009), no. 2, 899–914, DOI 10.4007/annals.2009.170.899. MR2552112 (2010m:12005)

[Poi10] Jérôme Poineau, *Raccord sur les espaces de Berkovich* (French, with English and French summaries), Algebra Number Theory **4** (2010), no. 3, 297–334, DOI 10.2140/ant.2010.4.297. MR2602668 (2011g:12009)

[Pop96] Florian Pop, *Embedding problems over large fields*, Ann. of Math. (2) **144** (1996), no. 1, 1–34, DOI 10.2307/2118581. MR1405941 (97h:12013)

[Pop10] Florian Pop, *Henselian implies large*, Ann. of Math. (2) **172** (2010), no. 3, 2183–2195, DOI 10.4007/annals.2010.172.2183. MR2726108 (2011j:12012)

Department of Mathematics and Statistics, University of Konstanz, 78457 Konstanz, Germany

Department of Mathematics and Computer Science, Open University of Israel, 43107 Raanana, Israel