ISRAEL JOURNAL OF MATHEMATICS **166** (2008), 185–219
DOI: 10.1007/s11856-008-1027-9

ALGEBRAIC PATCHING OVER COMPLETE DOMAINS*

BY

ELAD PARAN

School of Mathematical Sciences, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: paranela@post.tau.ac.il

ABSTRACT

We extend the method of algebraic patching due to Haran-Jarden-Völklein from complete absolute valued fields to complete domains. We apply the extended method to reprove a result of Lefcourt obtained by formal patching – every finite group is regularly realizable over the quotient field of a complete domain.

Introduction

Consider a field K and let $E = K(x)$ be the field of rational functions over K. If K is the quotient field of an integral domain D complete at a maximal ideal and $K \neq D$, then every finite group occurs as a Galois group over E. This was first proved by Harbater in [Ha]. Harbater's proof is phrased in the language of formal geometry. Serre [Se, Theorem 8.4.6] and Liu [Li] translated that proof to the language of rigid analytic geometry in the case where K is complete under a nonarchimedean absolute value. That case was treated again by Haran and Völklein [HV] who gave a simple self-contained algebraic proof using "algebraic patching".

* This research stems from the author's M.Sc. thesis in Tel-Aviv university, written under the supervision of Prof. Dan Haran. The research was supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation.
Received December 15, 2006

Building on Serre-Liu, Pop proved that if K is an ample field (in particular, if K is a complete valued field), then every constant finite split embedding problem over K is regularly solvable (in particular, every finite group can be realized over $K(x)$). Extending the method of algebraic patching, Haran and Jarden [HJ] gave a self contained algebraic proof of Pop's theorem.

Lefcourt generalized the result of [Ha] in another direction. Starting from an integral domain D complete at a prime ideal $\mathfrak{p}$, she used formal algebraic geometry to prove that every finite group occurs as a Galois group over $K(x)$. Note that if K is ample, then this result follows from [Po] or [HJ]. However, it is unknown whether all of the fields $\mathrm{Quot}(D)$ with D as above are ample, and one suspects that they are not.

The goal of this work is to generalize "algebraic patching" from complete fields to complete domains. As an application, we present a simple algebraic proof of Lefcourt's result. Another application will be given elsewhere.

The basic idea is as follows. Suppose we wish to realize a finite group G as a Galois group over a field E assuming we already know how to realize generating subgroups $G_1, \dots, G_k$ of G (e.g. cyclic groups) by Galois extensions $F_1, \dots, F_k$. In the case where K is complete under a nontrivial absolute value, Haran–Jarden–Völklein choose field extensions $Q_1, \dots, Q_k$ of $F_1, \dots, F_k$ satisfying "patching conditions", induce them to algebras $N_1, \dots, N_k$ and prove that $F = \bigcap_{i=1}^k N_i$ is a Galois extension of E with $\mathrm{Gal}(F/E) \cong G$. Each of the fields Q_i is the quotient field of a ring of convergent power series in several variables. In our more general case, $Q_1, \dots, Q_k$ are the localizations of rings of convergent power series in several variables over D. The proof that the rings $Q_1, \dots, Q_k$ satisfy appropriate "patching conditions" becomes more difficult and uses several more tricks on top of those that were used in the former case. This leads to our main result.

Main Theorem: *Let D be a complete domain with respect to a non-trivial absolute value. Then every finite group occurs as a Galois group over* $\mathrm{Quot}(D[x])$.

Technical reasons force us to assume extra conditions on D. Fortunately, simple Galois theoretical arguments reduce the proof of the main theorem to three special cases. In two of them, the quotient fields of the rings are complete, hence the theorem follows from [HV]. In the third case, D is the ring $\mathbb{Z}[[x]]$ of formal power series over the integers. This ring does not satisfy the extra conditions, however $\mathbb{Z}[[x]][x^{-1}]$ does, and has the same quotient field as $\mathbb{Z}[[x]]$. This concludes the proof of the main theorem.

Finally, note that Lefcourt's result can also be reduced to the case of $\mathrm{Quot}(\mathbb{Z}[[x]])$. Thus, our main theorem is equivalent to that of Lefcourt.

Acknowledgment. I would like to thank Prof. Dan Haran for his guidance and teaching while working on this research. I also thank Prof. Moshe Jarden for his course notes [Ja]. These notes helped me in several important points of my work.

1. Algebraic Patching

The works [HV, §3] and [HJ, §1] develop a general setup in which given realizations of generating subgroups of a group G over a given field can be "patched together" into a realization of G over the same field. In this section we adjust this setup for our more general situation. The main difference is that we replace the fields Q_i in the patching data of [HV] and [HJ] by rings.

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

$$\mathcal{E} = (E, F_i, Q_i, \Omega; G_i, G)_{i \in I} \tag{1}$$

consists of fields $E \subseteq F_i \subseteq \Omega$, integral domains $Q_i \subseteq \Omega$, and finite groups $G_i \leq G$, $i \in I$, satisfying the following conditions:

(2a) F_i/E is a Galois extension with Galois 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) $F_i \cap \mathrm{Quot}(Q_i) = E$, $i \in I$.

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

(2e) $\bigcap_{i \in I} Q_i = E$.

In the rest of this section we prove that if $\mathcal{E}$ satisfies an extra condition called (COM), then G occurs over E as a Galois group.

Definition 1.2: Let $Q \subseteq P$ be integral domains and $\mathrm{Aut}(P)$ the group of automorphisms of P. Define $\mathrm{Aut}(P/Q) := \{\sigma \in \mathrm{Aut}(P) : \sigma x = x \text{ for all } x \in Q\}$. We say that P/Q is a **finite Galois domain extension**, if $P = Q[a]$ and $f = \mathrm{irr}(a, \mathrm{Quot}(Q))$ satisfies:

(a) $f \in Q[X]$, so that $P \cong Q[X]/\langle f \rangle$.

(b) f factors in $P[X]$ into a product of distinct linear monic polynomials.

We refer to a as a **primitive element** for the domain extension P/Q and call $\mathrm{Gal}(P/Q) = \mathrm{Aut}(P/Q)$ the **Galois group** of P/Q.

This notion of a Galois domain extension generalizes the notion of a Galois ring cover [FJ, Definition 6.1.3] — here we do not assume the domains P and Q to be integrally closed, nor do we assume that the discriminant of a is in $Q^\times$.

The following two lemmas follow from Definition 1.2 by basic Galois theory.

Lemma 1.3: *If P/Q is a finite Galois domain extension, then $\mathrm{Quot}(P)/\mathrm{Quot}(Q)$ is a finite Galois field extension, $\mathrm{Gal}(P/Q) \cong \mathrm{Gal}(\mathrm{Quot}(P)/\mathrm{Quot}(Q))$, the domain P is a free Q-module of rank $|\mathrm{Gal}(P/Q)|$, and $P^{\mathrm{Gal}(P/Q)} = Q$.*

Lemma 1.4: *Let F/E be a finite Galois extension of fields and let $Q \subseteq P$ be integral domains such that $E \subseteq Q$, $F \subseteq P$, $F \cap \mathrm{Quot}(Q) = E$ in $\mathrm{Quot}(P)$, and $QF = P$. Then P/Q is a finite Galois domain extension, and $\mathrm{Gal}(P/Q) \cong \mathrm{Gal}(F/E)$.*

We fix a generalized patching data $\mathcal{E} = (E, F_i, Q_i, \Omega; G_i, G)_{i\in I}$ for this section and extend it by more rings and algebras. For each $i \in I$ let $P_i = Q_iF_i$ be the compositum of F_i and Q_i in Ω. By condition (2c) P_i/Q_i is a Galois domain extension, the Galois group of P_i/Q_i is isomorphic (via the restriction of automorphisms) to $G_i = \mathrm{Gal}(F_i/E)$, P_i is a free Q_i-module of rank $|G_i|$, and $P_i^{\mathrm{Gal}(P_i/Q_i)} = Q_i$. Identify $\mathrm{Gal}(P_i/Q_i)$ with G_i via this isomorphism. Consider the algebra

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

of dimension $|G|$ over Ω. Addition and multiplication are defined in N componentwise; thus, $1 = \sum_{\theta\in G} \theta$, Ω is embedded diagonally in N, and G acts on N by

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

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:

(3)
$$N_i = \mathrm{Ind}_{G_i}^G P_i = \Big\{ \sum_{\theta\in G} a_\theta\theta \in N : a_\theta \in P_i,\ a_\theta^\tau = a_{\theta\tau} \text{ for all } \theta \in G,\ \tau \in G_i \Big\}.$$

If Δ is a system of representatives of G/G_i, then

(3′)
$$N_i = \mathrm{Ind}_{G_i}^G P_i = \Big\{ \sum_{\theta\in G} a_\theta\theta \in N : a_\theta \in P_i,\ a_\theta^\tau = a_{\theta\tau} \text{ for all } \theta\in\Delta,\ \tau\in G_i \Big\}.$$

Throughout this paper, whenever we consider a patching data as in (1), we automatically associate with it the rings $N, N_i, i \in I$, defined as above.

The next lemma gives the basic properties of the algebra N_i.

Lemma 1.5: *Let $i \in I$.*

(a) *N_i is G-invariant.*
(b) *$N_i^G = Q_i$.*
(c) *N_i is isomorphic over Q_i to the direct product of $(G : G_i)$ copies of P_i.*
(d) *N_i is a free Q_i-module of rank $|G|(= \dim_\Omega N)$.*

Proof. (a) Let $\alpha = \sum_{\theta\in G} a_\theta\theta \in N_i$ and $\sigma \in G$. Then $a_\theta^\tau = a_{\theta\tau}$ for each $\tau \in G_i, \theta \in G$, so $a_{\sigma\theta}^\tau = a_{\sigma\theta\tau}$, so $\alpha^\sigma = \sum_{\theta\in G} a_{\sigma\theta}\theta \in N_i$.

(b) The group G fixes $\alpha = \sum_{\theta\in G} a_\theta\theta \in N_i$ if and only if $a_{\sigma\theta} = a_\theta$ for all $\sigma, \theta \in G$, that is, $a_\theta = a_1$ for all $\theta \in G$. Thus

$$\begin{aligned} N_i^G &= \{\sum_{\theta\in G} a\,\theta : a \in P_i,\ a^\tau = a \text{ for all } \tau\in G_i\} \\ &= \{a \in P_i : a^\tau = a \text{ for all } \tau \in G_i\} = P_i^{G_i} = Q_i. \end{aligned}$$

(c) Let Δ be a system of representatives of G/G_i. It follows from (3′) that $\sum_{\theta\in G} a_\theta\theta \mapsto \sum_{\omega\in\Delta} a_\omega\omega$ is a Q_i-isomorphism $N_i \to P_i^{|\Delta|}$.

(d) Since $[P_i : Q_i] = |G_i|$, the assertion follows from (c). ∎

It follows from the preceding lemma that $F = \bigcap_{i\in I} N_i$ is an E-algebra which is G-invariant. We call F the **pre-compound** of the generalized patching data $\mathcal{E}$. We note that this was called “co-compound” in [HJ], however the name “pre-compound” is more appropriate.

Let $\mathcal{S} = (\theta|\theta \in G)$ be the standard basis of N over Ω.

Remark 1.6: A basis of N_t over Q_t

Let $t \in I$, $l = |G_t|$. Suppose β is a primitive element for P_t/Q_t, and let $\Delta = \{\omega_1, \dots, \omega_m\}$ be a system of representatives of G/G_t. Let $\tau_1, \dots, \tau_l$ be a listing of the elements of G_t. Then the following sequence of $|G|$ elements of N_t

$$\mathcal{C}_t = \left(\sum_{i=1}^{l} (\beta^{j-1})^{\tau_i}(\omega_k \tau_i) | 1 \le k \le m,\ 1 \le j \le l \right) \tag{4}$$

(say, with the lexicographical order) is a basis of N over Ω.

Indeed, let $B \in M_n(\Omega)$ be the transition matrix from $\mathcal{S}$ to $\mathcal{C}_t$, that is, the matrix defined by $\mathcal{C}_t = \mathcal{S}B$. Of course, B depends on the order of the sequence $\mathcal{S}$, but only up to the order of its columns, which will not be important in the sequel. For instance, write $\mathcal{S}$ as $(1(\omega_k\tau_i) \mid 1 \le k \le m,\ 1 \le i \le l)$, with the lexicographical order. Then B consists of m identical diagonal blocks $B_0 = \big((\beta^{j-1})^{\tau_i}\big) \in M_l(\Omega)$. These are Vandermonde matrices, hence $\det B_0 = \pm \prod_{\substack{\tau,\tau' \in G_t \\ \tau \neq \tau'}} [\beta^{\tau} - \beta^{\tau'}] \neq 0$. Therefore $\det B \neq 0$, so $B \in \mathrm{GL}_n(\Omega)$. Consequently, $\mathcal{C}_t$ is a basis of N over Ω.

Now we show that $\mathcal{C}_t$ is also a linear basis of N_t over Q_t. Indeed, let $\sum_{\theta \in G} a_\theta \theta = \sum_{\substack{1 \le k \le m \\ 1 \le i \le l}} a_{\omega_k\tau_i}\omega_k\tau_i$ be an arbitrary element of N_t. Since $1, \beta, \dots, \beta^{l-1}$ is a basis for P_t over Q_t, there exist elements $q_{k,j} \in Q_t, 1 \le k \le m$, $1 \le j \le l$, such that for each $1 \le k \le m$: $a_{\omega_k} = \sum_{1 \le j \le l} q_{k,j}\beta^{j-1}$. Thus $a_{\omega_k\tau_i} = a_{\omega_k}^{\tau_i} = \sum_{1 \le j \le l} q_{k,j}(\beta^{j-1})^{\tau_i}$ for each $1 \le k \le m, 1 \le i \le l$, so

$$\begin{aligned} \sum_{\substack{1 \le k \le m \\ 1 \le i \le l}} a_{\omega_k\tau_i}\omega_k\tau_i &= \sum_{\substack{1 \le k \le m \\ 1 \le i \le l}} \left(\sum_{1 \le j \le l} q_{k,j}(\beta^{j-1})^{\tau_i} \right) \omega_k\tau_i \\ &= \sum_{\substack{1 \le k \le m \\ 1 \le j \le l}} q_{k,j} \left(\sum_{1 \le i \le l} (\beta^{j-1})^{\tau_i}\omega_k\tau_i \right). \end{aligned}$$

Corollary 1.7: Let $t \in I$, β a primitive element of F_t/E and R be a subring of Ω that contains all of the conjugates β^τ of β over E and $(\mathrm{discr}_E\,\beta)^{-1}$. Then there exists a basis $\mathcal{C}_t$ of N_t over Q_t that is also a basis for N over Ω, and such that the transition matrix from $\mathcal{S}$ to $\mathcal{C}_t$ is in $\mathrm{GL}_n(R)$.

Proof. Since β is a primitive element for F_t/E, it is also a primitive element for P_t/Q_t. Now, simply note that all of the entries of the matrix B in the preceding remark lie in R, and $\det B$ is a power of $\pm\,\mathrm{discr}_E\,\beta$, so it belongs to $R^\times$. Hence $B \in \mathrm{GL}_n(R)$. ∎

Proposition 1.8: *Assume that:*

(Com) *There is a linear basis of N over Ω that is also a basis for N_i over Q_i for each $i \in I$.*

Then:

(a) *$F = \bigcap N_i$ is a field and F/E is a Galois extension with Galois group G.*
(b) *There is a linear basis of F over E that is also a basis of N_i over Q_i for each $i \in I$.*

Proof. By Lemma 1.5, N_i is an algebra over Q_i. We may view Q_i as an algebra over E, and so N_i is an E-algebra. Equation (3) gives an explicit presentation of F as

(5)
$$F = \left\{ \sum_{\theta \in G} a_\theta \theta \in \mathrm{Ind}_1^G \Omega : a_\theta \in \bigcap_{i \in I} P_i,\ a_{\theta\tau} = a_\theta^\tau \text{ for all } \theta \in G \text{ and } \tau \in \bigcup_{i \in I} G_i \right\}.$$

Proof of (b): Let $\mathcal{C} = (\alpha_1, \ldots, \alpha_n)$ be the basis mentioned in (COM). Then $\mathcal{C}$ is a basis of F as an algebra over E. Indeed, every $b \in N$ can be uniquely written as $b = a_1\alpha_1 + \cdots + a_n\alpha_n$ with $a_1, \ldots, a_n \in \Omega$. Then $b \in N_i$ if and only if $a_1, \ldots, a_n \in Q_i$. Since $\bigcap_{i \in I} Q_i = E$, we have $b \in F$ if and only if $a_1, \ldots, a_n \in E$.

Proof of (a): Observe that F is an integral domain. Indeed, suppose $\sum_{\theta \in G} a_\theta \theta$, $\sum_{\theta \in G} b_\theta \theta \in F$ and $\sum_{\theta \in G} a_\theta b_\theta \theta = 0$. In particular, $a_1 b_1 = 0$, so either $a_1 = 0$ or $b_1 = 0$. Without loss of generality, we may assume that $a_1 = 0$ (and prove that $a_\theta = 0$, for all $\theta \in G$). Let $\theta \in G$. Since $G = \langle G_i | i \in I \rangle$, we have $\theta = \tau_1\tau_2 \ldots \tau_l$, where $\tau_1, \ldots, \tau_l \in \bigcup_{i \in I} G_i$. Now $a_\theta = a_{\tau_1\tau_2\ldots\tau_l} = a_{\tau_1\cdots\tau_{l-1}}^{\tau_l} = \ldots = a_1^{\tau_1\cdots\tau_l} = 0^{\tau_1\cdots\tau_l} = 0$, as contended.

Since F is a commutative finitely generated algebra over the field E and has no zero divisors, F itself is a field. By Lemma 1.5(a), the N_i are G-invariant, hence so is F. By Lemma 1.5(b), $F^G = \bigcap_{i \in I} N_i^G = \bigcap_{i \in I} Q_i = E$. By (b), $[F : E] = |G|$, hence G acts faithfully on F. By Galois theory F/E is a Galois extension with group G. ∎

Definition 1.9: Consider the Ω-algebras homomorphism φ: $N \to \Omega$ given by $\sum a_\theta \theta \mapsto a_1$. Then $\varphi|_F$ is a monomorphism. Since E is invariant under φ, $\varphi(F)$ is a Galois extension of E with group isomorphic to G. We call $\varphi(F)$ the **compound** of the patching data.

2. Normed rings and power series

The works [HV, §1] and [HJ, §3] study rings of convergent power series in disks of radius 1 over complete rank-1 valued fields. In an unpublished manuscript, Haran follows [FrP] and generalizes these rings by allowing an arbitrary radius. A common feature of these "analytic" rings is that they are principal ideal domains. In this section and in the next one, we generalize Haran's analytic rings by taking rings of convergent power series with coefficients in a complete domain D, which need not be a field.

Definition 2.1: **Normed ring.** Let R be an associative ring with 1. A **norm** on R is a function $|\cdot|\colon R \to \mathbb{R}$ that satisfies the following conditions for all $a, b \in R$:

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

If there exists $a \in D$ with $0 < |a| < 1$, we say that $|\cdot|$ is **nontrivial**. If in addition to (a) and (b), $|\cdot|$ satisfies also:

(c′) $|ab| = |a| \cdot |b|$,

we say that $|\cdot|$ is an **absolute value** on R.

Every real-valued valuation v of R naturally corresponds to an absolute value given by $|x| = (1/2)^{v(x)}$.

Remark 2.2: Let R be a normed ring and let $a, b \in R$. Then:

(a) $|-a| = |a|$.

(b) If $|a| < |b|$, then $|a+b| = |b|$.

(c) A series $\sum_{n=0}^{\infty} a_n$ of elements of R is Cauchy if and only if $a_n \to 0$.

(d) If R is complete and $|a| < 1$, then $1-a \in R^\times$ and its inverse is of the form $1+b$ with $|b| < 1$ (so $|(1-a)^{-1}| = 1$). Indeed, $a + a^2 + \cdots$ converges, say, to $b \in R$, with $|b| = |a| < 1$. Since $(1-a)(1+a+\cdots+a^n) = 1-a^{n+1} \to 1$, we have $(1-a)(1+b) = 1$. Similarly $(1+b)(1-a) = 1$.

(e) An absolute value $|\cdot|$ on R can be extended to $\mathrm{Quot}(R)$ by $|a/b| = |a|/|b|$.

Now we discuss complete rings that are of significance to this work.

Example 2.3:

(a) The ring $\mathbb{Z}_p$ of p-adic integers is complete with respect to the p-adic valuation (and so also with respect to the corresponding absolute value).

Its quotient field $\mathbb{Q}_p$ is also complete with respect to the induced absolute value.

(b) Similarly, if F is a field, then the ring $F[[x]]$ of formal power series over F, as well as its quotient field $F((x))$, are complete with respect to the x-adic valuation.

(c) The ring $\mathbb{Z}[[x]]$ of formal power series over the integers is complete with respect to the x-adic valuation (and the corresponding absolute value). However, its quotient field is not complete with respect to the induced absolute value. To prove this, consider the ring $B = \{\frac{1}{c}\sum_{i=m}^{\infty}\frac{b_i}{a^i}x^i : b_i \in \mathbb{Z}, 0 \neq a, c \in \mathbb{Z}, m \in \mathbb{Z}\}$. This is a subring of the field $\mathbb{Q}((x))$ and $\mathbb{Z}[[x]] \subseteq B$. Moreover, $f^{-1} \in B$ for every $0 \neq f \in \mathbb{Z}[[x]]$, hence $\mathrm{Quot}(\mathbb{Z}[[x]]) \subseteq B$. Indeed, let $f = \sum_{n=m}^{\infty} a_n x^n \in \mathbb{Z}[[x]], a_i \in \mathbb{Z}, a_m \neq 0$. Since $x^{-m} \in B$, we may replace f by $x^{-m}f$ to assume that $m = 0$. Let $a = a_0$. Then $f = a(1 + a_1\frac{x}{a} + \cdots)$. The expression in the parentheses is an invertible element of $\mathbb{Z}[[\frac{x}{a}]] \subseteq B$, hence $f^{-1} \in B$. Now, let $f = \sum_{i=0}^{\infty} x^i/2^{i^2} \in \mathbb{Q}[[x]]$. Then, the sequence of partial sums of f is a Cauchy sequence in $\mathrm{Quot}(\mathbb{Z}[[x]])$, whose limit f is not in B, and hence is not in $\mathrm{Quot}(\mathbb{Z}[[x]])$. Indeed, let $0 \neq a, c \in \mathbb{Z}$, then for a large enough $i \in \mathbb{N}$ we have $a^i c \not\equiv 0(\bmod\ 2^{i^2})$. Hence, $f \neq \frac{1}{c}\sum_{i=0}^{\infty}\frac{b_i}{a^i}x^i$ for $\{b_i\} \subseteq \mathbb{Z}$, and so $f \notin B$. Thus, $\mathrm{Quot}(\mathbb{Z}[[x]])$ is not complete.

(d) The ring $D = \mathbb{Z}[[x]][x^{-1}]$. This subring of $\mathrm{Quot}(\mathbb{Z}[[x]])$ is complete with respect to the x-adic valuation v_x. Indeed, let f_i be a Cauchy series in D. We show that there is an integer k such that $x^k f_i \in \mathbb{Z}[[x]]$ for $i \geq 0$. Indeed, there exists $n \in \mathbb{N}$ such that $v_x(f_i - f_n) \geq 0$ for all $i \geq n$. There exists $k \in \mathbb{N}$ such that $v_x(f_i) \geq -k$ for all $1 \leq i \leq n$. For $i \geq n$ we have $v_x(f_i) = v_x(f_i - f_n + f_n) \geq \min(0, -k)$ for all $i \geq n$. Therefore, $x^k f_i \in \mathbb{Z}[[x]]$ for all $i \geq 0$.

Thus, $x^k f_i$ converges to a limit $g \in \mathbb{Z}[[x]]$, and f_i converges to $x^{-k}g \in D$.

Let R be a complete normed ring and z a free variable over R. Define

$$R\{z\} = \left\{ \sum_{n=0}^{\infty} a_n z^n : a_n \in R, \quad \lim_{n\to\infty} a_n = 0 \right\}. \tag{6}$$

This set is a ring under addition and multiplication of power series, in which z is in the center; It contains R.

Extend $|\cdot|$ from R to a function $|\cdot|\colon R\{z\} \to \mathbb{R}$ by $|\sum_n a_n z^n| = \max_n(|a_n|)$.

Lemma 2.4:

(i) *The function* $|\cdot|\colon R\{z\}\to\mathbb{R}$ *is a norm on* $R\{z\}$ *extending the norm of* R.

(ii) *The ring* $R\{z\}$ *is complete with respect to the norm* $|\cdot|$.

(iii) *Let* S *be a complete normed ring containing* R. *Each* $c\in S$ *with* $|c|\le 1$ *that commutes with the elements of* R *defines an* **evaluation homomorphism** $R\{z\}\to S$ *given by* $f=\sum_n a_nz^n\mapsto f(c)=\sum_n a_nc^n$.

Proof. (i) and (iii) are clear.

(ii) Consider a Cauchy sequence (f_n) in $R\{z\}$. This yields a Cauchy sequence in each coefficient, hence (f_n) converges coefficientwise to some formal sum $f=\sum_i a_iz^i$. Moreover, $f\in R\{z\}$ and $|f-f_n|\to 0$. ∎

Definition 2.5: For $g=\sum_{n=0}^{\infty}a_nz^n\neq 0$ in $R\{z\}$ define the **pseudodegree** of g to be the integer $d=\max(n\colon |a_n|=|g|)$. Call a_d the **pseudoleading coefficient** of g. Call g **regular**, if a_d is invertible in R and $|ca_d|=|c|\cdot|a_d|$ for all $c\in R$.

Definition 2.5 generalizes [HV, Definition 1.4], where $|\cdot|$ is an absolute value. However, with this modified definition, the Weierstrass Division Theorem [HV, Theorem 1.6], its corollary, and their proofs go through verbally.

Proposition 2.6 (HV, Theorem 1.6, Corollary 1.7):

(a) *Let* $f\in R\{z\}$ *and let* $g\in R\{z\}$ *be regular of pseudodegree* d. *Then there are unique* $q\in R\{z\}$ *and* $r\in R[z]$ *such that* $f=qg+r$. *Moreover,* $|q|\cdot|g|\le|f|$ *and* $|r|\le|f|$.

(b) *Let* $f\in R\{z\}$ *be regular of pseudodegree* d. *Then* $f=qg$, *where* q *is a unit of* $R\{z\}$ *and* $g\in R[z]$ *is a monic polynomial of degree* d *with* $|g|=1$.

3. Convergent power series

Let D be a complete domain with respect to a nontrivial norm $|\cdot|$, and let $K=\mathrm{Quot}(D)$. Let x be a free variable over K. In this section, we study elements of $K((x))$ which are separably algebraic over $K(x)$.

Consider the set $K[x^{-1}]+xD\{x\}=\{\sum_{n=m}^{\infty}a_nx^n\in K((x)) : a_n\in K$ if $n\le 0$ and $a_n\in D$ if$n>0, m\in\mathbb{Z}, |a_n|\overset{n\to\infty}{\longrightarrow}0\}$ as a D-submodule of $K((x))$.

Definition 3.1: An element $f(x) \in K((x))$ is **D-convergent** if there exists an element $0 \neq \beta \in K$ such that $f(\beta x) \in K[x^{-1}] + xD\{x\}$.

Remark 3.2: Suppose $f(x) \in K((x))$ is D-convergent. Then there exists an element $0 \neq \beta_1 \in D, |\beta_1| < 1$ such that $f(\beta_1 x) \in K[x^{-1}] + xD\{x\}$.

Indeed, let $0 \neq \beta \in K$ with $f(\beta x) = \sum_{n=m}^{\infty} \alpha_n x^n \in K[x^{-1}] + xD\{x\}$ and $|\alpha_n| \xrightarrow{n\to\infty} 0$. Write β as $\frac{\beta_1}{\beta_2}$, with $0 \neq \beta_1, \beta_2 \in D$. By multiplying the numerator and denominator with a sufficiently small element of D, we may assume that $|\beta_1|, |\beta_2| < 1$. Thus, $f(\beta_1 x) = f(\beta\beta_2 x) = \sum_{n=m}^{\infty} \alpha_n \beta_2^n x^n$. For $n \geq 0$ we have $|\alpha_n \beta_2^n| \leq |\alpha_n|$, so $|\alpha_n \beta_2^n| \xrightarrow{n\to\infty} 0$. Since $\alpha_n \beta_2^n \in D$ for $n \geq 1$, we have $f(\beta_1 x) \in K[x^{-1}] + xD\{x\}$.

Lemma 3.3: *An element $f(x) = \sum_{n=m}^{\infty} a_n x^n \in K((x))$ is D-convergent if and only if there exist $0 \neq \gamma \in D$ and $c \in \mathbb{R}$ such that:*

(i) *$\gamma^n a_n \in D$ for each $n \geq 1$; and*
(ii) *$|a_n| < c^n$ for each $n \geq 1$.*

Proof. First, suppose $f(x) = \sum_{n=m}^{\infty} a_n x^n \in K((x))$ is D-convergent. Then there is an element $0 \neq \gamma \in D$ such that $f(\gamma x) = \sum_{n=m}^{\infty} \alpha_n x^n$, where $\alpha_n \in D$ for each $n \geq 1$, $|\alpha_n| \xrightarrow{n\to\infty} 0$. Thus $\gamma^n a_n = \alpha_n \in D$ for each $n \geq 1$, and there exists $1 < s \in \mathbb{R}$ such that for each $n \geq 1$, $|\alpha_n| < s$. Hence for each $n \geq 1$, $|a_n| \leq s \cdot |1/\gamma^n| < c^n$, if c is sufficiently large.

Conversely, suppose that conditions (i), (ii) hold, for $0 \neq \gamma \in D$ and $c \in \mathbb{R}$. For each $n \geq 1$, $|a_n \gamma^n| < |\gamma|^n c^n < t^n$ for some $1 < t \in \mathbb{R}$. Now consider an element $0 \neq \beta \in D$ such that $|\beta| < t^{-2}$ (there must be such an element, since the norm of D is nontrivial). Then for all $n \geq 1$, we have $|a_n \gamma^n \beta^n| < t^{-n} \xrightarrow{n\to\infty} 0$ and $a_n \gamma^n \beta^n \in D$ for each $n \geq 1$. Thus $f(\beta\gamma x) \in K[x^{-1}] + xD\{x\}$, and so $f(x)$ is D-convergent. ∎

Lemma 3.4: *Let $f(x) \in K((x))$, and let $\beta \in K^{\times}$. Then $f(x)$ is D-convergent if and only if $f(\beta x)$ is D-convergent.*

Proof. First, suppose $f(x)$ is D-convergent. Then there exists $0 \neq \gamma \in D$ such that $f(\gamma x) = \sum_{n=m}^{\infty} \alpha_n x^n$, where $m \in \mathbb{Z}$, $\alpha_n \in D$ for each $n \geq 1$, $|\alpha_n| \xrightarrow{n\to\infty} 0$. Since $f(\gamma x) = f(\frac{\gamma}{\beta} \cdot \beta x)$, $f(\beta x)$ is also D-convergent. For the converse, suppose $f(\beta x)$ is D-convergent. Then $f(x) = f(\beta^{-1}\beta x)$ is D-convergent. ∎

Denote the set of all D-convergent elements of $K((x))$ by $K((x))_D$.

LEMMA 3.5: *Suppose $f_1, \dots, f_k \in K((x))_D, k \geq 1$. Then there exists $\beta \in D$, $0 < |\beta| < 1$ such that $f_1(\beta x), \dots, f_k(\beta x) \in K[x^{-1}] + xD\{x\}$.*

Proof. By Remark 3.2 there exist $0 \neq \beta_1, \dots, \beta_k \in D, |\beta_1|, \dots, |\beta_k| < 1$ such that for each $1 \leq i \leq k$, $f(\beta_i x) \in K[x^{-1}] + xD\{x\}$. Take $\beta = \prod_{i=1}^k \beta_i \neq 0$. For $1 \leq i \leq k$ we get $f(\beta x) \in K[x^{-1}] + xD\{x\}$, because $f(\beta x) = f(\beta/\beta_i \cdot \beta_i x)$ and $|\beta/\beta_i| = |\prod_{j \neq i} \beta_j| \leq 1$. ∎

PROPOSITION 3.6: *$K((x))_D$ is a field containing $K(x)$.*

Proof. By the preceding lemma, $K((x))_D$ is closed under addition. Let $f_1(x), f_2(x) \in K((x))_D$. We prove that $f_1(x)f_2(x) \in K((x))_D$. Let $f_2(x) = \sum_{n=m}^\infty a_n x^n$. By Lemma 3.3, there are $0 \neq \gamma \in D, c \in \mathbb{R}$ such that $a_n\gamma^n \in D, |a_n| < c^n$ for $n \geq 1$.

First consider the case where $f_1(x) = x^{-1}$. Then

$$f_1(x)f_2(x) = \sum_{n=m-1}^{\infty} a_{n+1}x^n.$$

Let $\delta = \gamma^2 \in D$. Then $\delta^n a_{n+1} = \gamma^{n-1}(\gamma^{n+1}a_{n+1}) \in D$ and $|a_{n+1}| < c^{n+1} < (c+1)^{n+1} \leq ((c+1)^2)^n$ for each $n \geq 1$. Hence $f_1(x)f_2(x) \in K((x))_D$.

Similarly, if $f_1(x) = x$, then $f_1(x)f_2(x) \in K((x))_D$.

Next, suppose that $f_1(x) = \alpha \in K$, say $\alpha = a/b$ with $a, b \in D$ and $0 \neq b$. Then $f_1(x)f_2(x) = \sum_{n=m}^\infty \frac{aa_n}{b} x^n$ and $\frac{aa_n}{b}(b\gamma)^n = ab^{n-1}(\gamma^n a_n) \in D$, $|\frac{aa_n}{b}| < \left(|\frac{a}{b}|c\right)^n$ for each $n \geq 1$. Hence $f_1(x)f_2(x) \in K((x))_D$.

Now let $f_1(x)$ be arbitrary. By the preceding cases $K((x))_D$ is closed under multiplication by an element of $K[x, x^{-1}]$. Hence we may assume that $f_1(x), f_2(x) \in xK[[x]]$. By Lemma 3.5, there exists $\delta \in K^\times$ such that $f_1(\delta x), f_2(\delta x) \in K[x^{-1}] + xD\{x\}$, hence $f_1(\delta x), f_2(\delta x) \in xD\{x\}$. But then $f_1(\delta x)f_2(\delta x) \in xD\{x\}$, so $f_1(x)f_2(x) \in K((x))_D$.

It remains to prove that each nonzero element of $K((x))_D$ is invertible. It suffices to show that $1/\Sigma_{i=m}^\infty a_i x^i \in K((x))_D$, where $a_i = \alpha_i/\gamma^i$ for $\alpha_i, \gamma \in D$ and $|a_i| \leq c^i$ for some $c > 1$ and for all $i \geq 1$. We have $K[x, x^{-1}] \subseteq K((x))_D$, so by multiplying with a power of x and an element of K, we may assume that $m = 0$ and $a_0 = 1$. We construct elements $\beta_0, \beta_1, \ldots \in D$ such that $a_0\beta_0 = 1$, and

$$\sum_{i+j=k} \alpha_i\beta_j = 0 \quad \text{and} \quad |\beta_k/\gamma^k| \leq c^k \tag{7}$$

for each $k \geq 1$ (and then $\sum \frac{\beta_n}{\gamma^n} x^n$ is the required inverse element). Indeed, take $\beta_0 = 1, \beta_1 = -\alpha_1$. Then (7) holds for $k = 1$. Suppose, by induction, that we have constructed elements $\beta_0, \beta_1, \ldots, \beta_n$ such that (7) holds for each $1 \leq k \leq n$. Now, take $\beta_{n+1} = -\sum_{\substack{i+j=n+1\\ j\leq n}} \alpha_i\beta_j$. Then $\sum_{i+j=n+1} \alpha_i\beta_j = 0$, $\beta_{n+1} \in D$, and $|\frac{\beta_{n+1}}{\gamma^{n+1}}| = |\sum_{\substack{i+j=n+1\\ j\leq n}} \frac{\alpha_i}{\gamma^i}\frac{\beta_j}{\gamma^j}| \leq \max_{\substack{i+j=n+1\\ j\leq n}} c^i c^j = c^{n+1}$.

Consequently $K((x))_D$ is a field that contains $K[x, x^{-1}]$, hence also $K(x)$. ∎

A simple case distinction verifies the next lemma.

Lemma 3.7: *Let $v_1, \ldots, v_d$ be a sequence in $\mathbb{R} \cup \{\infty\}$, such that $v_1 > 0$, $v_2, \ldots, v_d < 0$. Let $v_{\sigma(1)}, \ldots, v_{\sigma(k)}$ be a subsequence of $v_1, \ldots, v_d$. Then $v_{\sigma(1)} + \cdots + v_{\sigma(k)} \geq v_2 + \cdots + v_d$, and equality holds if and only if $k = d-1, \{\sigma(1), \ldots, \sigma(k)\} = \{2, 3, \ldots, d\}$.*

Lemma 3.8: *Let (F, v) be a valued field and $h(Y) = p_dY^d + \cdots + p_1Y + p_0 \in F[Y]$ a polynomial of degree d with d distinct roots $y_1, \ldots, y_d$ in F. Suppose $v(y_1) > 0$, and $v(y_2), \ldots, v(y_d) < 0$. Then $v(p_k) > v(p_1)$ for each $k \neq 1$.*

Proof. Observe that $h(Y)/p_d = \prod_{j=1}^d (Y - y_j)$. For $1 \leq k \leq d-1$ we have:

$$p_{d-k}/p_d = (-1)^k \sum_\sigma \prod_{i=1}^k y_{\sigma(i)},$$

where σ ranges over all injective maps $\{1, \ldots, k\} \to \{1, \ldots, d\}$. Suppose σ is such a map. Then, by Lemma 3.7, we have $v(\prod_{i=1}^k y_{\sigma(i)}) \geq v(y_2 \cdots y_d)$, and equality holds if and only if $k = d-1$, and $\{\sigma(1), \ldots, \sigma(k)\} = \{2, 3, \ldots, d\}$. Therefore, $v(\frac{p_{d-k}}{p_d}) \geq v(y_2 \cdots y_d)$ and equality holds if and only if $k = d-1$. Thus, for each $k \neq 1$, $v(p_k) - v(p_d) > v(y_2 \cdots y_d) = v(p_1) - v(p_d)$, hence $v(p_k) > v(p_1)$. ∎

Lemma 3.9: *Let F be a field, and let $h(Y) = p_dY^d + \cdots + p_1Y + p_0 \in F[x][Y]$ be a polynomial over $F[x]$. Suppose that for each $0 \leq k \leq d$ we have $p_k = \sum_{n=0}^\infty b_{k,n}x^n$, where $b_{k,n} \in F$ are almost all zero, and $b_{0,0} = 0, b_{1,0} = 1, b_{2,0} = \cdots = b_{d,0} = 0$. Let $y = \sum_{n=0}^\infty a_nx^n \in F[[x]]$ be 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 $j_0 + j_1 + \cdots + j_k = n$.*

Proof. We get $p_k y^k = (\sum_n b_{k,n}x^n)(\sum_n a_n x^n)^k = \sum_n c_{k,n}x^n$, for $0 \le k \le d$, where

$$c_{k,n} = \sum_{\sigma \in S_{k,n}} b_{k,\sigma(0)} \prod_{j=1}^{k} a_{\sigma(j)}$$

and

$$S_{k,n} = \{\sigma\colon \{0,\dots,k\} \to \{0,\dots,n\} : \sum_{j=0}^{k} \sigma(j) = n\}.$$

By considering the equality $p_d y^d + \cdots + p_1 y + p_0 = 0$ modulo (x), we get $0 = b_{d,0}a_0^d + \cdots + b_{1,0}a_0 + b_{0,0} = a_0$, and comparing coefficients at x^n we get:

$$c_{0,n} = b_{0,n} \text{ and } c_{1,n} = b_{1,0}a_n + \cdots + b_{1,n-1}a_1 \tag{8}$$

Let $k \ge 2$. Since $b_{k,0} = 0$, all terms in $c_{k,n}$ that contain a_n vanish, and therefore:

$$c_{k,n} = \Bigg[\text{sum of products of the form } b_{k,\sigma(0)} \prod_{j=1}^{k} a_{\sigma(j)} \text{ with } \sigma(j) < n, 1 \le j \le k, \sum_{j=0}^{k} \sigma(j) = n\Bigg]. \tag{9}$$

From the relation $\sum_{k=0}^{d} p_k y^k = h(y) = 0$ we conclude that $\sum_{k=0}^{d} c_{k,n} = 0$, for each $n \ge 0$. Hence, by (8) and (9),

$$\begin{aligned} a_n =& b_{1,0}a_n \\ =& \Bigg[\text{sum of products of the form} \pm b_{k,\sigma(0)} \prod_{j=1}^{k} a_{\sigma(j)}, \text{ with } 0 < \sigma(j) < \\ & n, 1 \le j \le k, \sum_{j=0}^{k} \sigma(j) = n\Bigg]. \end{aligned}$$ ∎

Proposition 3.10: *Let $y \in K((x))$ be separably algebraic over $E = K(x)$. Then y is D-convergent.*

Proof. By Proposition 3.6, $E \subseteq K((x))_D$. Thus we may assume that $y \notin E$. Let $y = \sum_{n=l}^{\infty} a_n x^n$.

Part A: A shift of y.

Let $y_1, y_2, \ldots, y_d$ ($d \geq 2$) with $y_1 = y$ be the distinct conjugates of y over E. Let v be the natural valuation of $K((x))$ defined by $v(\sum_{n=k}^{\infty} b_n x^n) = \min\{i : b_i \neq 0\}$, $v(0) = \infty$. Extend v to the algebraic closure of $K((x))$ and let $r = \max\{v(y - y_i) : i = 2, \ldots, d\}$ ($\neq \infty$), $s = r + 1$. Define: $y_i' := x^{-s}(y_i - \sum_{n=l}^{s} a_n x^n)$, for each $1 \leq i \leq d$. Then $y_1', \ldots, y_d'$ are the distinct conjugates of y_1' over E. Moreover, $v(y_1') \geq 1$, hence for $2 \leq i \leq d$: $v(y_1' - y_i') = v(y_1 - y_i) - s \leq r - s = -1$, so $v(y_i') \leq -1$.

In view of Proposition 3.6, y_1' is D-convergent if and only if y_1 is D-convergent. So, replace 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, $y = \sum_{i=0}^{\infty} a_n x^n$ with $a_0 = 0$ and $y_1, \ldots, y_d$ are the roots of an irreducible separable polynomial $h(Y) = p_d Y^d + \cdots + p_1 Y + p_0 \in E[Y]$ with $d \geq 2$.

Part B: The value of the coefficients p_k.

Multiplying by an element of $D[x]$, we may assume $p_i \in D[x]$. By Lemma 3.8 we have $e = v(p_1) < v(p_i)$ for each $i \neq 1$. Divide the p_i by x^e to assume that $v(p_1) = 0 < v(p_i)$ for each $i \neq 1$. Therefore, for each $k = 0, \ldots, d$: $p_k = \sum_{n=0}^{t} b_{k,n} x^n$, where $b_{k,n} \in D, t \in \mathbb{N}, b_{1,0} \neq 0$, and for each $k \neq 1 : b_{k,0} = 0$. For all $0 \leq k \leq d$ and $n > t$ let $b_{k,n} = 0$ and denote $\beta = b_{1,0}$.

By Lemma 3.4 it suffices to prove that $\tilde{y} = \sum_{i=0}^{\infty} a_i (\beta x)^i$ is D-convergent. The substitution $x \mapsto \beta x$ defines an automorphism of $K((x))$, hence the following equality follows from $h(y) = 0$:

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

The coefficients in this equality are all in $D[x]$, in particular $\frac{p_1(\beta x)}{\beta} = \frac{\beta + b_{1,1}\beta x + \ldots}{\beta} = 1 + b_{1,1} x + \cdots$. Thus, without loss of generality, we may assume $\beta = 1$.

Part C: The coefficients a_n.

By Lemma 3.9, a_n is a sum of products of the form

$$\pm b_{k,j_0} a_{j_1} a_{j_2} \cdots a_{j_k}, \tag{10}$$

with $0 \leq k \leq d,\ 0 \leq j_0 \leq n,\ 0 < j_1, \ldots, j_k < n$ such that $j_0 + j_1 + \cdots + j_k = n$.

Claim I: $\{a_n\}_{n=0}^{\infty} \subseteq D$.

Indeed, $a_0 = 0 \in D$. Assume that $a_m \in D$ for each $0 \leq m \leq n - 1$. Then, each summand in (10) belongs to D, hence $a_n \in D$.

Claim II: There exists $1 < c \in \mathbb{R}$ such that $|a_n| \le c^n$, for all $n \ge 0$.

Take an element $1 < c \in \mathbb{R}$ such that $|b_{k,n}| \le c^n$ for each $0 \le k \le d$ and $n \ge 1$. We prove, by induction, that $|a_n| \le c^n$ for each $n \ge 0$. For $n = 0$ this holds trivially. Suppose the claim holds for each $0 \le m \le n-1$. For each summand in (10) we have $|b_{k,j_0} \prod_{l=1}^{k} a_{j_l}| \le c^{\sum_{l=0}^{k} j_l} = c^n$, thus $|a_n| \le c^n$, as contended.

We conclude that y is D-convergent. ■

Corollary 3.11: *Let $f_1(x), \ldots, f_k(x) \in K[[x]]$ be separably algebraic over $K(x)$. Then there exist $c \in K^\times$ such that $f_1(cx), \ldots, f_k(cx) \in K + xD\{x\}$.*

Proof. By Proposition 3.10, $f_1(x), \ldots, f_k(x) \in K((x))_D$. By Lemma 3.5, there exists $c \in K^\times$ such that $f_1(cx), \ldots, f_k(cx) \in (K[x^{-1}] + xD\{x\}) \cap K[[x]] = K + xD\{x\}$. ■

4. Rings of convergent power series in several dependent variables

Let D be an integral domain, complete with respect to a norm $|\cdot|$, and let I be a finite set. For each $i \in I$ let $r, c_i \in D$ such that $r, c_i - c_j \in D^\times$ if $i \ne j$. Assume that:

$$\left|\frac{r}{c_i - c_j}\right| \le 1 \quad \text{for all } i \ne j. \tag{11}$$

Let $K = \mathrm{Quot}(D)$, and let $E = K(x)$ be the field of rational functions over K in the free variable x. For each $i \in I$ let $w_i = r/(x - c_i) \in K(x)$.

Lemma 4.1: (a) *For all $i \ne j$ in I and for each nonnegative integer m*

$$w_i w_j^m = \frac{r^m}{(c_i - c_j)^m} w_i - \sum_{k=1}^{m} \frac{r^{m+1-k}}{(c_i - c_j)^{m+1-k}} w_j^k. \tag{12}$$

(b) *Let D_0 be $\mathbb{Z}$ if* $\mathrm{char}(K) = 0$ *and $\mathbb{F}_p$ if* $\mathrm{char}(K) = p$. *Set $D_0' = D_0[\frac{r}{c_i - c_j} \mid i \ne j \in I]$. Given nonnegative integers m_i, $i \in I$, not all zero, there exist $a_{ik} \in D_0'$ such that*

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

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

$$f = a_0 + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in} w_i^n \tag{13}$$

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

(d) *Let $i \neq j \in I$. Then $w_i/w_j = 1 + (c_i - c_j)/rw_i \in D[w_i]$ is invertible in $D[w_i, w_j]$.*

Proof.

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

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

one proves (12) by induction on m. Induction on $|I|$ and $\max_{i \in I} m_i$ gives (b).

Proof of (c): The existence of the presentation (13) follows from (b). Note that $D_0' \subseteq D$ because $c_i - c_j \in D^\times$. To prove the uniqueness we assume that $f = 0$ in (13) 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.

Proof of (d): Multiply $r/w_j - r/w_i = c_i - c_j$ by w_i/r to get that

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

is in $D[w_i]$. Similarly, $w_j/w_i \in D[w_j]$. Hence w_i/w_j is invertible in $D[w_i, w_j]$. ∎

Consider the subset $R_0 = \sum_{i \in I} D[w_i]$ of the field $E = K(x)$. It follows from Lemma 4.1 that R_0 is the subring $D[w_i | i \in I]$ of E. Define a real valued function $\| \cdot \|$ on R_0 using the unique presentation (13)

$$\left\| a_0 + \sum_{i \in I} \sum_{n \geq 1} a_{in} w_i^n \right\| = \max_{i,n} \{ |a_0|, |a_{in}| \}.$$

It follows by Lemma 4.1(a) that $\| \cdot \|$ is a **norm** on R_0, in the sense of Definition 2.1. Indeed, the only nontrivial condition is $\|fg\| \leq \|f\| \cdot \|g\|$ for $f, g \in R_0$. Let $f = a_0 + \sum_{i \in I} \sum_{m \geq 1} a_{im} w_i^m$, $g = b_0 + \sum_{i \in I} \sum_{k \geq 1} b_{ik} w_i^k$. Denote $fg = c_0 + \sum_{i \in I} \sum_{n \geq 1} c_{in} w_i^n$. By Lemma 4.1, each of the coefficients c_0, c_{in} is a sum of elements of the form $\alpha \cdot a_{im} \cdot b_{jk}$, $\alpha \in D_0[\frac{r}{c_i - c_j}]$, where D_0 is the prime ring of D. By (11), $|\alpha| \leq 1$. Thus $|\alpha \cdot a_{im} \cdot b_{jk}| \leq 1 \cdot |a_{im}||b_{jk}| \leq \|f\| \cdot \|g\|$, hence $\|fg\| \leq \|f\| \cdot \|g\|$.

Let $R = D\{w_i : i \in I\}$ be the completion of $R_0 = D[w_i \mid i \in I]$ with respect to $\|\cdot\|$, and extend $\|\cdot\|$ to R.

Lemma 4.2: *Each element f of R has a unique presentation as a multiple power series:*

$$f = a_0 + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in} w_i^n, \tag{14}$$

where $a_0, a_{in} \in D$, and $|a_{in}| \to 0$ as $n \to \infty$. Moreover,

$$\|f\| = \max_{i,n}\{|a_0|, |a_{in}|\}.$$

Proof. The completion R is the ring of Cauchy sequences of elements of R_0 modulo the sequences converging to 0. Each f as in (14) represents the Cauchy sequence $\{f_d\}_{d \geq 1}$ of its partial sums $f_d = a_0 + \sum_{i \in I} \sum_{n=1}^{d} a_{in} w_i^n \in R_0$, and as such represents an element of the completion R. Since $\|f_d\| = \max_{i,n}\{|a_0|, |a_{in}|\}$ for each sufficiently large d, we have $\|f\| = \max_{i,n}\{|a_0|, |a_{in}|\}$. Thus, if $f = 0$, then $a_0 = 0$ and $a_{in} = 0$ for all i and n. Consequently, the presentation (14) is unique.

Now we prove the existence of the presentation (14) for each element of R. If $g_k = a_{k,0} + \sum_{i \in I} \sum_{n=1}^{\infty} a_{k,in} w_i^n$, $k = 1, 2, 3, \ldots$, is a Cauchy sequence in R_0, then each of the sequences $\{a_{k,0} : k = 1, 2, 3, \ldots\}$ and $\{a_{k,in} : k = 1, 2, 3, \ldots\}$ is Cauchy. Since D is complete, $a_{k,0} \to a_0$ and $a_{k,in} \to a_{in}$ for some $a_0, a_{in} \in D$. Fix $i \in I$ and let $\varepsilon > 0$ be a real number. There is an m such that for all $k \geq m$ and all n we have $|a_{k,in} - a_{m,in}| \leq \|g_k - g_m\| \leq \varepsilon$. If n is sufficiently large, then $a_{m,in} = 0$, and hence $|a_{k,in}| \leq \varepsilon$. Therefore $|a_{in}| \leq \varepsilon$. It follows that $|a_{in}| \to 0$. Define f by equation (14). Then $f \in R$ and $g_k \to f$ in R. ∎

When $I = \emptyset$, then $R = R_0 = D$.

We call the partial sum $\sum_{n=1}^{\infty} a_{in} w_i^n$ in (14) the i-**component** of f.

For each $J \subseteq I$ we denote the completion R_J of $D[w_j \mid j \in J]$ by $D\{w_j : j \in J\}$. By Lemma 4.2, R_J is contained in R_I.

Remark 4.3: (a) Let $i \in I$. Then $D\{w_i\} = \{\sum_{n=0}^{\infty} a_n w_i^n : a_n \to 0\}$ is a subring of R, the completion of $D[w_i]$ with respect to the norm. Consider the ring $D\{z\}$ of converging power series over D. By Lemma 2.4(iii), there is a homomorphism $D\{z\} \to D\{w_i\}$ given by $\sum_{n=0}^{\infty} a_n z^n \mapsto \sum_{n=0}^{\infty} a_n w_i^n$. By Lemma 4.2, this is a norm preserving isomorphism of normed rings. It extends to the natural isomorphism $K((z)) \to K((w_i))$.

(b) Let $c \in D$ such that $c - c_i \in D^\times$ and $\left|\frac{r}{c-c_i}\right| \leq 1$ for each $i \in I$. Define an evaluation homomorphism $\varphi\colon R_0 \to D$ by $w_i \mapsto r/(c-c_i), i \in I$. Then $|\varphi(f)| \leq |f|$ for each $f \in R_0$. Hence, if f_n is a null series in R_0, then $\varphi(f_n)$ is a null series in D. Therefore, φ extends to a continuous homomorphism $\varphi\colon R \to D$.

(c) Suppose J, J' are subsets of I. Then by the unique presentation (14), we have $R_J \cap R_{J'} = R_{J\cap J'}$.

Lemma 4.4 (Degree shifting): *Let $f \in R$ be given by (14). Fix distinct $i, j \in I$. Let $\sum_{n=1}^\infty a'_{in} w_i^n$ be the i-component of $\frac{w_j}{w_i} f \in R$. Then*

$$\begin{aligned} a'_{in} &= -\sum_{\nu=n+1}^{\infty} \frac{a_{i\nu} r^{\nu-n}}{(c_j-c_i)^{\nu-n}} \\ &= \frac{-r}{c_j-c_i} \sum_{\nu=n+1}^{\infty} a_{i\nu}\Bigl(\frac{r}{c_j-c_i}\Bigr)^{\nu-(n+1)} \qquad n = 1,2,3,\dots \end{aligned} \tag{15}$$

Furthermore, let m be a positive integer and let $\sum_{n=1}^\infty b_{in} w_i^n$ be the i-component of $(w_j/w_i)^m f$. 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 $|b_{in}| \leq |\frac{r}{c_j-c_i}|^m \epsilon$ 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 $|b_{in}| < |\frac{r}{c_j-c_i}|^m \epsilon$ for each $n \geq d+1-m$ and $|b_{i,d-m}| = |\frac{r}{c_j-c_i}|^m \epsilon$.*

(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.*

(d) *If the i-component of f is zero, then so is the i-component of $\bigl(\frac{w_j}{w_i}\bigr)^m f$.*

Proof. Since $r \in D^\times$, it follows by the equality $\frac{w_j}{w_i} = 1 + \frac{c_j-c_i}{r} w_i$ that $\frac{w_j}{w_i} f \in R$. So, the above statements make sense.

Proof of (15): We may assume that $a_0 = a_{i1} = 0$ and $a_{k\nu} = 0$ for each $k \neq i$ and each ν. Indeed, $\frac{w_j}{w_i} = 1 + (c_j - c_i)\frac{w_j}{r} \in D\{w_j\}$. Hence, by (12), $\frac{w_j}{w_i} \cdot w_k^\nu \in D\{w_l : l \neq i\}$. Furthermore, $\frac{w_j}{w_i} \cdot w_i = w_j \in D\{w_l : l \neq i\}$. Hence a_0, a_{i1}, and the $a_{k\nu}$ do not contribute to the i-component of $\frac{w_j}{w_i} f$.

Thus, $f=\sum_{\nu=2}^{\infty} a_{i\nu} w_i^{\nu}$. Hence, by (12),

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

from which (15) 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 $|a_{in}| \le \varepsilon$ for each $n \ge d{+}1$, then $|a'_{in}| \le |\frac{r}{c_j-c_i}|\varepsilon$ for each $n \ge d$. (b) assuming $d \ge 2$, if $|a_{in}| < \varepsilon$ for each $n \ge d+1$ and $|a_{id}| = \varepsilon$, then $|a'_{in}| < |\frac{r}{c_j-c_i}|\varepsilon$ for each $n \ge d$ and $|a'_{i,d-1}| = |\frac{r}{c_j-c_i}|\varepsilon$. By (11), $|\frac{r}{c_i-c_j}| \le 1$. Hence, (a) follows from (15) with $n=d, d+1, d+2, \ldots$ and (b) follows from (15) 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 $a_{i\nu} = 0$ for all large ν. It follows from (15) that $a'_{in} = 0$ for all sufficiently large n. Therefore, $\sum_{n=1}^{\infty} a'_{in} w_i^n$ 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 $a_{id} \ne 0$. Increasing d, if necessary, we may assume that $|a_{in}| < |a_{id}|$ for each $n \ge d+1$. By (b), $a'_{i,d-1} \ne 0$. Consequently, $\sum_{n=1}^{\infty} a'_{in} w_i^n$ is not a polynomial. ∎

The next three claims prove that if D is a field and the norm $|\cdot|$ is an absolute value, then R is a principal ideal domain. The proof is due to Dan Haran. The case where K is algebraically closed appears in [FrP, Theorem 2.2.9].

Lemma 4.5: *Suppose $D = K$ and $|\cdot|$ is an absolute value. Let $0 \ne f \in R$. Then either $f \in R^{\times}$ or there is an $i \in I$ such that $f = pu$ with $p \in K[w_i]$ and $u \in R^{\times}$.*

Proof. If $I = \emptyset$, then $f \in K^{\times} = R^{\times}$. Suppose $|I| \ge 1$ and continue by induction on I.

Write f in the form (14). There is a coefficient with absolute value $\|f\|$. 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 Remark 2.2(d), $f \in R^\times$, and we are done.

Case II: There exist i and $d \geq 1$ such that $|a_{id}| = \|f\|$ Increase d, if necessary, to assume that $|a_{in}| < |a_{id}| = \|f\|$ for all $n > d$.

Let $A = K\{w_k : k \neq i\}$. This is a complete subring of R. Introduce a new variable z, and consider the ring $A\{z\}$ of convergent power series in z over A (Lemma 2.4). Since $a_{id} \in K^\times \subseteq A^\times$, the element

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

of $A\{z\}$ is regular of pseudodegree d (Definition 2.5). By Proposition 2.6(b) we have $\hat{f} = \hat{p}\hat{u}$, where $\hat{u}$ is a unit of $A\{z\}$ and $\hat{p}$ is a monic polynomial of degree d in $A[z]$.

By definition, $\|w_i\| = 1$. By Lemma 2.4(iii) the evaluation homomorphism θ: $A\{z\} \to R$ defined by $\sum c_n z^n \mapsto \sum c_n w_i^n$, with $c_n \in A$, maps $\hat{f}$ onto f, $\hat{u}$ onto a unit of R, and $\hat{p}$ onto a polynomial p of degree d in $A[w_i]$. Replace f by p to assume that $f \in A[w_i]$ is a polynomial of degree d in w_i, that is, $a_{in} = 0$ for all $n > d$.

If $I = \{i\}$, then $A[w_i] = K[w_i]$, and so we are done. If $|I| \geq 2$, choose $j \in I$, $j \neq i$. By Lemma 4.1(d), $w_j/w_i = 1 + (c_j - c_i)/rw_j$ is invertible in R_0, hence in R. As $w_j/w_i \in A$, we have $\frac{w_j}{w_i}(\sum_{k\neq i}\sum_{n=1}^{\infty} a_{kn}w_k^n) \in A$. On the other hand,

$$\frac{w_j}{w_i}\sum_{n=1}^{d} a_{in}w_i^n = \sum_{n=1}^{d} a_{in}w_i^{n-1}w_j$$

is a polynomial in $A[w_i]$ of degree $\leq d-1$, by (12). Therefore, multiplying f by a suitable power of w_j/w_i, we may assume that $f \in A$. Now we apply the induction hypothesis to conclude the proof. ∎

Lemma 4.6: *Suppose $D = K$ and $|\cdot|$ is an absolute value. Let $j \in I$. Then each $0 \neq f \in R$ can be written as $f = pu$ with $p \in K[w_j]$ monic, $\|p\| = 1$, and $u \in R^\times$.*

Proof. By the preceding lemma we may assume that $f \in K[w_i]$, where $i \neq j$, say, $f = \sum_{n=0}^{d} a_n w_i^n$, with $a_d \neq 0$. By Lemma 4.1(d), w_i/w_j is invertible in

R_0, hence in R. Multiply f by $(w_j/w_i)^d$ to get

$$\Big(\frac{w_j}{w_i}\Big)^d f = \sum_{n=0}^{d} a_n \Big(\frac{w_j}{w_i}\Big)^{d-n} w_j^n = \sum_{n=0}^{d} a_n \Big(1 + \frac{c_j - c_i}{r} w_j\Big)^{d-n} w_j^n \in K[w_j].$$

By Remark 4.3(a) $K\{w_j\} \cong K\{z\}$, so the claim follows by Proposition 2.6(b). ∎

Proposition 4.7: *Suppose $D = K$ and $|\cdot|$ is an absolute value. Then the ring $R = K\{w_i : i \in I\}$ is a principal ideal domain, hence an integrally closed domain. Moreover, for each $i \in I$, every ideal $\mathfrak{a}$ of R is generated by an element $p \in K[w_i]$ such that $\mathfrak{a} \cap K[w_i] = pK[w_i]$.*

Proof. Let $f_1, f_2 \in R \smallsetminus \{0\}$ such that $f_1 f_2 = 0$. Choose $i \in I$. By the preceding lemma, $f_1 = p_1 u_1$ and $f_2 = p_2 u_2$ with $p_1, p_2 \in K[w_i]$ and $u_1, u_2 \in R^\times$. Then $p_1 p_2 = f_1 f_2 (u_1 u_2)^{-1} = 0$, hence either $p_1 = 0$ or $p_2 = 0$. We conclude that either $f_1 = 0$ or $f_2 = 0$, a contradiction. Therefore, R is an integral domain.

By the preceding lemma, 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 $p \in K[w_i]$. Consequently, $\mathfrak{a} = pR$ is a principal ideal. ∎

The domain D need not be a field, nor need the norm $|\cdot|$ on D be an absolute value. If D is not a field, then R need not be a principal domain (as is the case in [HJ]). Indeed, suppose there exists $c \in D$ with $c - c_i \in D^\times$, $\left|\frac{r}{c-c_i}\right| \le 1$ for each $i \in I$. Choose a nonzero prime ideal $\mathfrak{p}$ of D. Let φ: $R \to D$ be the evaluation homomorphism $w_i \mapsto \frac{r}{c-c_i}$, $i \in I$ (Remark 4.3). Then $\mathrm{Ker}(\varphi) \subset \varphi^{-1}(\mathfrak{p})$ are nonzero prime ideals of R. Thus, $\dim(R) \ge 2$, so R is not a principal ideal domain. However, we gain information on R by embedding it into a suitable principal ideal domain.

For the rest of this section assume that the norm $|\cdot|$ on D is an **absolute value**. We note that for our needs in this work, we could have assumed this to be the case all along. However, all the properties we have proven so far do not rely on this assumption, and we have chosen to present them in full generality – they will be useful in future work.

Extend the absolute value to the quotient field K. Let $\hat{K}$ be the completion of K with respect to $|\cdot|$. We consider the ring $\hat{K}\{w_i : i \in I\}$ and its subrings $\hat{K}\{w_i : i \in J\}, J \subseteq I$. Then for each $J \subseteq I$, the ring R_J is contained in $\hat{K}\{w_i : i \in J\}$.

By Proposition 4.7, $\hat{K}\{w_i : i \in I\}$ is an integral domain, hence so is its subring $R = D\{w_i : i \in I\}$. Denote the quotient ring of R by Ω. For each $J \subseteq I$ consider the rings $O_J = D[w_i \mid i \in J]$ and $Q_J = (O_J \smallsetminus \{0\})^{-1} R_J = \big\{f/a : f \in R_J,\ a \in O_J \smallsetminus \{0\}\big\}$. Recall that $E = K(x)$.

Lemma 4.8: *Let J be a nonempty subset of I. Then:*

(a) $E = \mathrm{Quot}(O_J)$.

(b) *The ring Q_J is the compositum of E and R_J in Ω.*

(c) *If $j \in J$ then $Q_J = (O_{\{j\}} \smallsetminus \{0\})^{-1} R_J$.*

Proof.

Proof of (a): We have

$$\begin{aligned}\mathrm{Quot}(O_J) &= \mathrm{Quot}(D[w_j \mid j \in J]) = \mathrm{Quot}(D[w_j^{-1} \mid j \in J]) \\ &= \mathrm{Quot}(D[x - c_j : j \in J]) = \mathrm{Quot}(D[x]) = E.\end{aligned}$$

Proof of (b): Since $E, R_J \subseteq Q_J$ we have $ER_J \subseteq Q_J$. Let $f/p \in Q_J$, $f \in R_J$, $0 \neq p \in O_J$. Then $1/p \in \mathrm{Quot}(O_J) = E$, hence $f/p = \frac{1}{p} \cdot f \in ER_J$.

Proof of (c): Since $E = \mathrm{Quot}(D[w_j])$, it follows that $ER_J = \mathrm{Quot}(D[w_j])R_J$, hence $Q_J = ER_J = (D[w_j] \smallsetminus \{0\})^{-1} R_J$. ∎

For each $J \subseteq I$, we denote the integral closure of Q_J inside its quotient field by $C(Q_J)$. View $C(Q_J)$ as a subring of Ω.

Now we present the main result of this section.

Proposition 4.9: *Let J, J' be nonempty subsets of I.*

(a) *If $J \cap J' \neq \emptyset$, then $Q_J \cap Q_{J'} = Q_{J \cap J'}$.*

(b) *If $J \cap J' = \emptyset$, then $Q_J \cap C(Q_{J'}) = E$.*

Proof.

Proof of (a): By definition, $Q_{J \cap J'} \subseteq Q_J \cap Q_{J'}$. Conversely, let $0 \neq y \in Q_J \cap Q_{J'}$. Fix $j \in J \cap J'$. By Lemma 4.8(c), $y = g_1/q_1$ with $g_1 \in R_J, 0 \neq q_1 \in O_{\{j\}}$ and $y = g_2/q_2$ with $g_2 \in R_{J'}, 0 \neq q_2 \in O_{\{j\}}$. This yields $q_2 g_1 = q_1 g_2 \in R_J \cap R_{J'} = R_{J \cap J'}$ (by Remark 4.3(c)), hence $y = \frac{g_1 q_2}{q_1 q_2} \in Q_{J \cap J'}$.

Proof of (b): We have $E \subseteq ER_J \cap ER_{J'} = Q_J \cap Q_{J'} \subseteq Q_J \cap C(Q_{J'})$.

Conversely, let $0 \neq y \in Q_J \cap C(Q_{J'})$. Fix $j \in J$ and $j' \in J'$. By Lemma 4.8(c), $y = g_1/q_1$ with $0 \neq q_1 \in O_{\{j\}}$ and $g_1 \in D\{w_i : i \in J\}$. By Proposition 4.7, $\hat{K}\{w_i : i \in J'\}$ is integrally closed, hence so is the localization $(O_{\{j'\}} \smallsetminus \{0\})^{-1}\hat{K}\{w_i : i \in J'\}$. Since $O_{J'} = (O_{\{j'\}} \smallsetminus \{0\})^{-1}R_{J'}$ and $R_{J'} \subseteq \hat{K}\{w_i :\in J'\}$, we have $y = g_2/q_2$ with $0 \neq q_2 \in O_{\{j'\}}$, $g_2 \in \hat{K}\{w_i : i \in J'\}$.

Write q_1 as $\sum_{n=0}^{d_1} b_n w_j^n$, with $b_n \in D$. Put $h_1 = (\frac{w_{j'}}{w_j})^{d_1} q_1$. We have $\frac{w_{j'}}{w_j} \in D[w_{j'}]$ and thus $h_1 = \sum_{n=0}^{d_1} b_n (\frac{w_{j'}}{w_j})^{d_1-n} w_{j'}^n \in D[w_{j'}]$ (by Lemma 4.1(d)). Similarly there exists $d_2 \geq 0$ such that $h_2 = (\frac{w_j}{w_{j'}})^{d_2} q_2 \in D[w_j]$. Let $d = d_1 + d_2$. Then, for each $k \in J$

$$g_1 h_2 \cdot \left(\frac{w_{j'}}{w_k}\right)^d = g_2 h_1 \cdot \left(\frac{w_j}{w_k}\right)^d. \tag{16}$$

Note that $g_1 h_2 \in D\{w_i : i \in J\}$ while $g_2 h_1 \in \hat{K}\{w_i : i \in J'\}$. In particular, the k-th component of $g_2 h_1$ is zero. By Lemma 4.4(d), the k-th component of $g_2 h_1 \cdot \left(\frac{w_j}{w_k}\right)^d$ is zero. By (16), the k-th component of $g_1 h_2 \cdot \left(\frac{w_{j'}}{w_k}\right)^d$ is also zero. Hence, by Lemma 4.4(c), the k-th component of $g_1 h_2$ is a polynomial in $\hat{K}[w_k]$. Since the coefficients of $g_1 h_2$ belong to D (and the presentation as a sum of components is unique), we conclude that the k-th component of $g_1 h_2$ belongs to $D[w_k]$. Thus $g_1 h_2 \in D[w_k \mid k \in J]$, so $y = \frac{g_1 h_2}{q_1 h_2} \in \mathrm{Quot}(D[w_k \mid k \in I]) = E$. ∎

For each $i \in I$, let $Q_i = Q_{I \smallsetminus \{i\}}, Q'_i = Q_{\{i\}}$. Note that by this notation $Q_i \neq Q_{\{i\}}$.

Corollary 4.10: $\bigcap_{i \in I} Q_i = E$.

Proof. Let $j \in I$. By Proposition 4.9(a), $\bigcap_{i \in I} Q_i = Q_j \cap Q'_j$, and by Proposition 4.9(b), $Q_j \cap Q'_j \subseteq Q_j \cap C(Q'_j) = E$. It follows that $\bigcap_{i \in I} Q_i = E$. ∎

5. Factorization of matrices over complete rings

In this section we show how to decompose a matrix over a complete ring into a product of matrices over certain subrings. We recall the corresponding notion from [HJ, §4] and prove a somewhat different factorization result than that of [HJ].

Lemma 5.1: *Cartan's Lemma, [FrP, Lemma 4.5.3], [Vo, Lemma 11.14] Let M be a complete normed ring (Definition 1.1). 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 $\|a^+\|, \|a^-\| \le \|a\|$ such that $a = a^+ + a^-$.*

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

The reader looking for a proof of the preceding lemma may find it more convenient to look at the proof of [HV, Lemma 2.2].

For the rest of this section let A be a commutative ring with respect to a nontrivial norm $|\cdot|$.

Example 5.2: Let n be a positive integer and let M be the ring $M_n(A)$ 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) of Definition 2.1. If A is complete, then so is M. In this case suppose that A_1 and A_2 are complete subrings of A. Then $M_1 = M_n(A_1)$ and $M_2 = M_n(A_2)$ are complete subrings of M. If A satisfies the condition

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

then M satisfies condition (d) above.

Corollary 5.3: Let A, A_1, and A_2 be complete domains satisfying the condition (d′) above. Let A_0 be a dense subring of A and let $E_0 = \mathrm{Quot}(A_0)$. Then, for each $b \in \mathrm{GL}_n(A)$ there are $b_1 \in \mathrm{GL}_n(A_1)$, $b_2 \in \mathrm{GL}_n(A_2), b_0 \in \mathrm{GL}_n(E_0)$ such that $b = b_1 b_2 b_0$.

Proof. Since A_0 is dense in A, there exists $a \in M_n(A_0)$ such that $\|b^{-1} - a\| < 1/\|b\|$. Then $\|1 - ba\| \le \|b\| \cdot \|b^{-1} - a\| < 1$, so by Lemma 5.1 there exist $b_i \in \mathrm{GL}_n(A_i)$, $i = 1, 2$, such that $ba = b_1 b_2$. In particular, $\det(a) \ne 0$, hence $a \in \mathrm{GL}_n(E_0)$. Let $b_0 = a^{-1} \in \mathrm{GL}_n(E_0)$. Then $b = b_1 b_2 b_0$. ∎

We apply Corollary 5.3 to the rings and fields of §4.

Theorem 5.4: *Suppose that $I = J \cup J'$ is a partition of I into nonempty sets J and J', and let $b \in \mathrm{GL}_n(R_I)$.*

(a) *There exist $b_1 \in \mathrm{GL}_n(R_J)$ and $b_2 \in \mathrm{GL}_n(Q_{J'})$ such that $b = b_1 b_2$.*

(b) *There exist* $\hat{b}_1 \in \mathrm{GL}_n(Q_J)$ *and* $\hat{b}_2 \in \mathrm{GL}_n(R_{J'})$ *such that* $b = \hat{b}_1\hat{b}_2$.

Proof. We prove (a). The proof of (b) is symmetrical.

By definition R_J and $R_{J'}$ are complete rings. Given $f \in R_I$, 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 $|f_i| \le |f|$, $i = 1, 2$ and $f = f_1 + f_2$. This proves condition (d$'$). Next note that $A_0 = D[w_i \mid i \in I]$ is dense in R_I and its quotient field $E = K(x)$ is contained in $Q_{J'}$. By Example 5.2 and Corollary 5.3 we have $b = b_1b_2'b_0$, with $b_1 \in \mathrm{GL}_n(R_J), b_2' \in \mathrm{GL}_n(R_{J'}) \subseteq \mathrm{GL}_n(Q_{J'}), b_0 \in \mathrm{GL}_n(E) \subseteq \mathrm{GL}_n(Q_{J'})$. Take $b_2 = b_2'b_0$. ∎

Our matrix factorization theorem has a somewhat “asymmetrical” form (compare it with the factorization theorems [HJ, Corollary 4.5] or [HV, Corollary 2.3]). However, this result is exactly the one we need in order to establish condition (COM) of Proposition 1.8.

6. Patching of abelian groups and prime divisors

In this section we show how to patch realizations of abelian groups over complete domains satisfying certain conditions. In the next section we apply a reduction step that removes these conditions.

Let K be a field, and let $E = K(x)$ be the field of rational functions over K.

Proposition 6.1: *Suppose K is infinite. Let G be a finite abelian group. Then there exists a finite Galois extension F/E with* $\mathrm{Gal}(F/E) \cong G$*, such that F/K has a prime divisor of degree* 1 *which is unramified over E.*

Proof. By [FJ, Proposition 16.3.5], E has a Galois extension F with group G such that F is regular over K. We wish to replace F/K with an isomorphic extension F'/K with a prime of degree 1, such that the K-isomorphism $F \to F'$ maps E onto itself, and F' is an unramified extension of E . This is exactly [HV, Lemma 4.5]. ∎

Lemma 6.2: *Let F be a finite Galois extension of E contained in $K((x))$. Let S be the integral closure of $K[x]$ in F, and let $d = [F : E]$. Then S has exactly d prime ideals lying over (x), and $S/\mathfrak{m} \cong K$ for each such ideal $\mathfrak{m}$.*

Proof. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_g$ be all of the prime ideals of S lying over $xK[x]$. Since $F \subseteq K((x))$, one of them is unramified with residue field K. Since F is Galois over K, each of them has that property. Hence, the formula $d = \sum_{i=1}^{g} e_i f_i$ for algebraic function fields of one variable implies that $e_i = f_i = 1$ for all i and $g = d$. ∎

For the rest of this section assume that $K = \mathrm{Quot}(D)$, where D is a complete domain with respect to a nontrivial norm $|\cdot|$. Moreover, we assume that D is **large** in the following sense:

(Large) For each $n \in \mathbb{N}$ there exist $b_1, \ldots, b_n \in D$ such that $b_i - b_j \in D^\times$ for all $i \neq j$.

For example, every infinite field is large in this sense but $\mathbb{Z}$ is not. The main significance of this condition is to enable us to construct variables for rings of convergent power series over D (which are easy to choose in the case where D is field, as in [HJ]).

Lemma 6.3: *Let F be a finite Galois extension of E such that F/K has a prime divisor $\mathfrak{P}$ of degree* 1 *which is unramified over E. Then:*

(a) *There is a K-automorphism θ of E that extends to a K-embedding $\theta\colon F \to K((x))$.*

(b) *Assume that $F \subseteq K((x))$. Then there exists a K-automorphism μ of $K((x))$ with $\mu(E) = E$ and $F' = \mu(F) = E(\beta)$, where β and its conjugates over E are in $D\{x\}$ and* $\mathrm{discr}(\mathrm{irr}(\beta, E)) \in (D\{x\})^\times$.

Proof.

Proof of (a): See [HV, Lemma 4.2(a)].

Proof of (b): Let $d = [F : E]$ and let S be the integral closure of $K[x]$ in F. Since $K[[x]]$ is integrally closed, $S \subseteq K[[x]]$. By Lemma 6.2, S has d distinct prime ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_d$ which lie over $xK[x]$. By condition (Large), there exist $b_1, \ldots, b_d \in D$ such that $b_i - b_j \in D^\times$ for all $i \neq j$. Since $\mathfrak{m}_1, \ldots, \mathfrak{m}_d$ are maximal ideals, the Chinese Remainder Theorem gives $y \in S$ with $y \equiv b_i \mod \mathfrak{m}_i$ for $i = 1, \ldots, d$. The prime ideal $\mathfrak{m} = xK[[x]] \cap S$ lies over $xK[x]$. Since F/E is Galois, we may list the elements of $\mathrm{Gal}(F/E)$ as $\sigma_1, \ldots, \sigma_d$ such that $\mathfrak{m} = \mathfrak{m}_i^{\sigma_i}$, $i = 1, \ldots, d$. Let $y_i = y^{\sigma_i}$. Then $y_i \equiv b_i \mod \mathfrak{m}$, $i = 1, \ldots, m$. In particular, $y_1, \ldots, y_d$ are distinct, hence $F = E(y)$.

Now consider the epimorphism $\varphi\colon K[[x]] \to K$ defined by $\varphi(x) = 0$ and $\varphi(a) = a$ for $a \in K$. Then $\varphi(\mathfrak{m}) = 0$, so $\varphi(y_i) = b_i$. If $i \neq j$, then

$\varphi(y_i - y_j) = b_i - b_j \in D^\times$, hence $\varphi(y_i - y_j) \neq 0$, so $(y_i - y_j)^{-1} \in K[[x]]$. For each $c \in D$, let μ_c be the K-automorphism of $K((x))$ given by $\mu_c(f(x)) = f(cx)$. By Corollary 3.11, there exists $c \in K^\times$ such that

$$\mu_c(y_i), \mu_c((y_i - y_j)^{-1}) \in K + xD\{x\}.$$

Note that $\mu_c(y_i)(0) = y_i(0) = \varphi(y_i) = b_i \in D$ and

$$(\mu_c((y_i - y_j)^{-1}))(0) = (y_i - y_j)^{-1}(0) = \varphi((y_i - y_j)^{-1}) = (b_i - b_j)^{-1} \in D.$$

Therefore, $\mu_c(y_i) \in D + xD\{x\} = D\{x\}$ and also $\mu_c((y_i - y_j)^{-1}) \in D\{x\}$. Set $\mu = \mu_c$, $\beta = \mu_c(y)$, and $\beta_i = \mu_c(y_i)$, $i = 1 \ldots, d$. Then $\mu(F) = E(\beta)$, $\beta_1, \ldots, \beta_d$ are the conjugates of β, they belong to $D\{x\}$, and $\mathrm{discr}(\mathrm{irr}(\beta, E)) = \pm \prod_{i \neq j} (\beta_i - \beta_j) \in D\{x\}^\times$. ∎

We add further assumptions on to our setup. Fix (for this section) a positive integer k, and assume that there exist elements $r, c_1, \ldots, c_k \in D$ such that $r, c_i - c_j \in D^\times$ and $\left|\frac{r}{c_i - c_j}\right| \leq 1$ for all $i \neq j$.

Let $I = \{1, 2, \ldots, k\}$ and $w_i = \frac{r}{x - c_i}$ for each $i \in I$. For each $J \subseteq I$ we put, as in Section 3, $R_J = D\{w_i : i \in J\}$. Then R_J is contained in $R = R_I$.

For the rest of this section assume that the norm $|\cdot|$ is an absolute value, and extend it to K. Let $\hat{K}$ be the completion of K with respect to $|\cdot|$. Then R is an integral domain, contained in the principal ideal domain $\hat{K}\{w_i : i \in I\}$ (Proposition 4.7). Let $\Omega = \mathrm{Quot}(R)$. For each $i \in I$ let

$$Q_i = Q_{I \smallsetminus \{i\}} = (D[w_j \mid j \neq i] \smallsetminus \{0\})^{-1} R_{I \smallsetminus \{i\}} \quad \text{and} \quad Q_i' = Q_{\{i\}}$$

(we use the notation of Section 4). By definition $Q_J \subseteq Q_I$ if $J \subseteq I$.

Lemma 6.4: *Let c be an element of D such that $c - c_i \in D^\times, |\frac{r}{c - c_i}| \leq 1$ for each $1 \leq i \leq k$. Consider the evaluation homomorphism φ_c: $R \to D$ defined by $w_1 \mapsto \frac{r}{c - c_1}, \ldots, w_k \mapsto \frac{r}{c - c_k}$. Set $p = w_1 - \frac{r}{c - c_1} \in R$. Then:*

(a) $\mathrm{Ker}(\varphi_c)$ *is a principal ideal of R, generated by p;*

(b) *the localization $R_p = \{a/b \in \Omega : a \in R,\ b \in R \smallsetminus pR\}$ is a valuation ring of Ω.*

Proof. By Remark 4.3(b), φ_c is indeed a homomorphism.

(a) Let $f \in \mathrm{Ker}(\varphi_c)$, so $f = \sum_{i=1}^k f_i$, $f_i \in D\{w_i\}, 1 \leq i \leq k$. For each $1 \leq i \leq k$ let $p_i = p \frac{w_i}{w_1} \frac{c - c_1}{c - c_i}$. Since $\frac{w_i}{w_1} = 1 + \frac{c_i - c_1}{r} w_i$ and $w_i w_1 = \frac{r}{c_i - c_1}(w_i - w_1)$ (Lemma 4.1),

$$\begin{aligned}
p_i &= \Big(w_1 - \frac{r}{c-c_1}\Big)\Big(1 + \frac{c_i - c_1}{r} w_i\Big)\frac{c-c_1}{c-c_i} \\
&= \Big(w_1 + \frac{c_i - c_1}{r} w_i w_1 - \frac{r}{c-c_1} + \frac{c_i - c_1}{c_1 - c} w_i\Big)\frac{c-c_1}{c-c_i} \\
&= \Big(w_1 + (w_i - w_1) - \frac{r}{c-c_1} + \frac{c_i - c_1}{c_1 - c} w_i\Big)\frac{c-c_1}{c-c_i} \\
&= \Big(w_i \frac{c-c_i}{c-c_1} - \frac{r}{c-c_1}\Big)\frac{c-c_1}{c-c_i} \\
&= w_i - \frac{r}{c-c_i}.
\end{aligned}$$

In particular, $p_i \in \mathrm{Ker}(\varphi_c)$. Since $\frac{c-c_i}{c-c_1} \in D^\times$ and $\frac{w_i}{w_1} \in R^\times$, the element p of R divides p_i. Since $|\frac{r}{c-c_i}| \le 1$, p_i is a regular element of $D\{w_i\}$ of pseudo degree 1.

By Proposition 2.6(a), there exist $q_i \in D\{w_i\}$ and $r_i \in D[w_i]$ such that $f_i = q_i p_i + r_i$ and $\deg(r_i) < 1$, so $r_i \in D$.

Since $f, p_i \in \mathrm{Ker}(\varphi_c)$, we get $\sum_{i=1}^k r_i = f - \sum_{i=1}^k q_i p_i \in D \cap \mathrm{Ker}(\varphi_c)$, hence $\sum_{i=1}^k r_i = 0$. Thus, $p|f$. Consequently, $\mathrm{Ker}(\varphi_c)$ is a principal ideal, generated by p.

(b) Put $\hat{R} = \hat{K}\{w_i : 1 \le i \le k\}$. Note that p belongs to the kernel of the evaluation homomorphism $\hat{R} \to \hat{K}$ given by $w_1 \mapsto \frac{r}{c-c_1}, \dots, w_k \mapsto \frac{r}{c-c_k}$. Since this is not the zero map, p is not invertible in $\hat{R}$.

We show that every element $f \in R$ can be uniquely written as $f = p^n g$, with $n \in \mathbb{N}$, $g \in R$ and $\varphi_c(g) \ne 0$. The only nontrivial part is to show that an element $f \in R$ is not divisible by p infinitely many times. To see that, note that if $p^n|f$ in R for all $n \in \mathbb{N}$, then also $p^n|f$ in $\hat{R}$ for all $n \in \mathbb{N}$ — but $\hat{R}$ is a factorial ring (Proposition 4.7), and p is not in $(\hat{R})^\times$ — a contradiction. Thus $R_p = \{a/b \in \Omega : a \in R, b \in R \smallsetminus pR\}$ is a discrete valuation ring of Ω. ∎

In the next lemma we use our asymmetrical factorization theorem to enable the patching of Galois groups.

Lemma 6.5: *Let $\{F_i\}_{i\in I}$ be fields, and let $G, \{G_i\}_{i\in I}$ be groups such that $\mathcal{E} = (E, F_i, Q_i, \Omega; G_i, G)_{i\in I}$ is a generalized patching data (Definition 1.1). Assume that for each $i \in I$ we have $F_i = E(\beta_i)$, where β_i and its conjugates over E are in R, and $\mathrm{discr}_E(\mathrm{irr}(\beta_i, E)) \in R^\times$. Then:*

(a) *Condition (COM) of Section 1 holds for $\mathcal{E}$.*

(b) *Suppose there exists $c \in D$ such that $c - c_i \in D^\times$ and $|\frac{r}{c-c_i}| \leq 1$ for each $i \in I$. Then the compound F' of $\mathcal{E}$ has a K-rational place φ_c such that $\varphi_c(x) = c$.*

Proof.

Proof of (a): Let $\mathcal{S} = (g \mid g \in G)$ be the standard basis of $N = \mathrm{Ind}_1^G \Omega$ over Ω, and let $n = |G|$. For each $i \in I$ we use Corollary 1.7 to choose a matrix $B_i \in \mathrm{GL}_n(R)$ and a basis $\mathcal{V}_i$ for $N_i = \mathrm{Ind}_{G_i}^G F_i Q_i$ over Q_i such that $\mathcal{V}_i B_i = \mathcal{S}$.

For each $J = \{1, 2, \ldots, l\} \subseteq I, 1 \leq l \leq k$ and each $i \in J$ we will find a matrix $A_i \in \mathrm{GL}_n(Q_i)$ such that $\mathcal{U} = \mathcal{V}_i A_i$ is independent of i, and $A_1 \in \mathrm{GL}_n(R_{I \smallsetminus \{1\}}) \subseteq \mathrm{GL}_n(Q_1)$. Then $\mathcal{V}_i$ is a basis for N over Q, hence so is $\mathcal{U}$. For $J = I$, $\mathcal{U}$ will also be a basis for N_i over Q_i, for all $i \in I$. This will prove (COM).

If $J = \{1\}$, take A_1 as the unit matrix. Now suppose that $J = \{1, 2, \ldots, l\}$, $1 \leq l < k$. By induction on l we assume that for each $i \in J$ there exists $A'_i \in \mathrm{GL}_n(Q_i)$ such that $\mathcal{U}' = \mathcal{V}_i A'_i$ is independent of i, and that $A'_1 \in \mathrm{GL}_n(R_{I \smallsetminus \{1\}})$. Let $r = l + 1$. Then, $\mathcal{V}_r \cdot B_r B_1^{-1} A'_1 = \mathcal{U}'$ and $B_r B_1^{-1} A'_1 \in \mathrm{GL}_n(R)$, but we cannot guarantee that $B_r B_1^{-1} A'_1 \in \mathrm{GL}_n(Q_r)$. However, by Theorem 5.4(b) there exist $A_r \in \mathrm{GL}_n(Q_r)$ and $M \in \mathrm{GL}_n(R_{\{r\}}) \subseteq \mathrm{GL}_n(Q_i), i \in J$, such that $B_r B_1^{-1} A'_1 = A_r M$. For each $i \in J$ let $A_i = A'_i M^{-1} \in \mathrm{GL}_n(Q_i)$. Note that $A_1 = A'_1 M^{-1} \in \mathrm{GL}_n(R_{I \smallsetminus \{1\}})$. Let also $\mathcal{U} = \mathcal{U}' M^{-1}$. Then, for each $i \in J$, $\mathcal{U} = \mathcal{V}_i A'_i M^{-1} = \mathcal{V}_i A_i$. For r we have $\mathcal{V}_r A_r = \mathcal{V}_r B_r B_1^{-1} A'_1 M^{-1} = \mathcal{S} B_1^{-1} A_1 = \mathcal{V}_1 A_1 = \mathcal{U}$. This finishes the induction.

Proof of (b): Let $\varphi_c \colon R \to D$ be the evaluation homomorphism $w_1 \mapsto \frac{r}{c-c_1}, \ldots, w_k \mapsto \frac{r}{c-c_k}$. By Lemma 6.4, $\mathrm{Ker}(\varphi_c)$ is a principal ideal, generated by $p = w_1 - \frac{r}{c-c_1}$ and $R_p = \{a/b \in \Omega : a \in R, b \in R \smallsetminus pR\}$ is a valuation ring of Ω. The corresponding place is an extension of φ_c – for each $y = \alpha/\beta \in R_p$ with $\varphi_c(\beta) \neq 0$ it is defined by $\varphi_c(y) = \varphi_c(\alpha)/\varphi_c(\beta)$, and $\varphi_c(y) = \infty$ for all $y \in \Omega \smallsetminus R_p$. This is a K-rational place $\Omega \to K \cup \{\infty\}$. Its restriction to F' is a K-rational place, since $K \subseteq F'$. Finally, $\varphi_c(x) = \varphi_c(c_1 + x - c_1) = c_1 + \varphi_c(\frac{1}{x-c_1})^{-1} = c_1 + \varphi_c(\frac{1}{r} \cdot w_1)^{-1} = c_1 + r \cdot (\frac{r}{c-c_1})^{-1} = c_1 + c - c_1 = c$. ■

Proposition 6.6: *Let G be a finite group, generated by abelian subgroups $G_1, \ldots, G_k$. Suppose there exists $c \in D$ such that $c - c_i \in D^\times$ and $|r/(c - c_i)| \leq 1$ for all $1 \leq i \leq k$. Then there exists a Galois extension F/E such that*

$\mathrm{Gal}(F/E) \cong G$ and F/K is a regular extension that has a prime of degree 1 unramified over E.

Proof. By condition (Large), D is infinite, and so is K. By Lemma 6.1, for each $1 \le i \le k$ there exists a Galois extension F_i/E with group G_i, such that F_i/K has a prime divisor of degree 1 unramified over E.

By Remark 4.3(a) the map $w_i \mapsto x$ extends to a K-isomorphism of $K((w_i))$ onto $K((x))$ which maps $R_{\{i\}}$ onto $D\{x\}$. Hence by Lemma 6.3, we may replace F_i/E by an isomorphic extension such that $F_i = E(\beta_i)$, where β_i and its conjugates over E belong to $R_{\{i\}}$, and $\mathrm{discr}_E(\mathrm{irr}(\beta_i, E)) \in R_{\{i\}}^\times$. In particular, $F_i \subseteq Q_i'$.

Now, $\mathcal{E} = (E, F_i, Q_i, \Omega; G_i, G)_{i\in I}$ is a generalized patching data. Indeed, conditions (2a), (2b), (2d) of Definition 1.1 have been established. Condition (2c) follows from Proposition 4.9(b), and condition (2e) holds by Corollary 4.10.

By Lemma 6.5(a), condition (COM) of Proposition 1.8 holds for $\mathcal{E}$. Let F' be the compound F' of $\mathcal{E}$ (Definition 1.9). By Proposition 1.8, $\mathrm{Gal}(F/E) \cong G$, hence also $\mathrm{Gal}(F'/E) \cong G$.

Choose an element $a \in D$ such that $0 < |a| < \min_i(1, |c - c_i|)$ (we may do so, since $|\cdot|$ is nontrivial) and define $d_j = c + a^j$ for all $j \ge 1$. Then $d_j - c_i = (c - c_i)(1 + \frac{a^j}{c-c_i})$. By our assumption, $|\frac{a^j}{c-c_i}| \le |a^j| \cdot |\frac{1}{c-c_i}| \le |a| \cdot |\frac{1}{c-c_i}| < 1$, thus $d_j - c_i \in D^\times$ for all $1 \le i \le k$ and $j \ge 1$, by Remark 2.2(d). Moreover, $|\frac{r}{d_j-c_i}| = |\frac{r}{c+a^j-c_i}| \le |\frac{r}{c-c_i}| \cdot |\frac{1}{1+a^j/(c-c_i)}| \le 1 \cdot |(1 + \frac{a^j}{c-c_i})^{-1}| = 1$, again by Remark 2.2(d).

For each $j \ge 1$, Lemma 6.5(b) gives the K-rational place φ_{d_j}, satisfying $\varphi_{d_j}(x) = d_j$. Out of the infinitely many places φ_{d_j} only finitely many are ramified over E. ∎

7. Realization of groups

In this section we prove that every finite group is regularly realizable over a field containing a complete domain.

It will be convenient to give a name to the following property.

Definition 7.1: Let K be a field, and let x be a free variable over K. We say that K is **rationaly Galois** if for every finite group G there exists a Galois extension F of $K(x)$ with group G, such that $F \subseteq K((x))$ (in particular, F/K is regular).

Lemma 7.2: *Let K be a field. If K contains a rationaly Galois field K_0, then K itself is rationaly Galois.*

Proof. Let G be a finite group, and let x be a free variable over K. Since K_0 is rationaly Galois, there exists a Galois extension F of $K_0(x)$ contained in $K_0((x))$ with group G. We have the following diagram of fields:

$$\begin{tikzcd}
K_0((x)) \arrow[r, dash] \arrow[d, dash] & K((x)) \arrow[d, dash] \\
F \arrow[r, dash] \arrow[d, dash] & FK \arrow[d, dash] \\
K_0(x) \arrow[r, dash] \arrow[d, dash] & K(x) \arrow[d, dash] \\
K_0 \arrow[r, dash] & K
\end{tikzcd}$$

Since x is free over K, the fields $K_0((x))$ and K are linearly disjoint over K_0. Indeed, suppose $c_1, \dots, c_n \in K$ are linearly independent over K_0, and let $f_1 = \sum_{i=m}^{\infty} a_{1i}x^i, \dots, f_n = \sum_{i=m}^{\infty} a_{ni}x^i \in K_0((x))$ such that $\sum_{j=1}^{n} f_j c_j = 0$. Then $\sum_{i=m}^{\infty}(\sum_{j=1}^{n} a_{ji}c_j)x^i = 0$ in $K((x))$, hence $\sum_{j=1}^{n} a_{ji}c_j = 0$ for each $i \geq m$, and thus $a_{ji} = 0$ for all $1 \leq j \leq n$ and $i \geq m$, so $f_1 = \cdots = f_n = 0$.

It follows that F and K are linearly disjoint over K_0, and so by the tower property F and $K(x)$ are linearly disjoint over $K_0(x)$. Thus $F \cap K(x) = K_0(x)$. We have $FK \subseteq K((x))$, and by Galois theory

$$\mathrm{Gal}(FK/K(x)) \cong \mathrm{Gal}(F/K_0(x)) = G. \qquad \blacksquare$$

We need the following technical lemma.

Lemma 7.3: *Let D be a complete domain with respect to an absolute value $|\cdot|$. Assume that there exists $x \in D^\times$ such that $|x| < 1$. Let k be a positive integer. Then there exist elements $r \in D^\times$ and $c_1, c_2, \dots, c_k, c_{k+1} \in D$ such that:*

(a) *$c_i - c_j \in D^\times$ for all $1 \leq i < j \leq k+1$ (In particular, condition (Large) of Section 6 holds).*

(b) *$|\frac{r}{c_i - c_j}| \leq 1$ for all $1 \leq i < j \leq k+1$.*

Proof. Take $c_i = 1 + x^i, r = x^{k+1}$. Then $c_i - c_j = x^i - x^j = x^i(1 - x^{j-i})$. By Remark 2.2(d), this element is in $D^\times$, which proves (a). If $1 \leq i < j \leq k+1$, then $|\frac{r}{c_i - c_j}| = |x|^{k+1}|\frac{1}{x^i(1-x^{j-i})}| = |x|^{k+1-i} \leq 1$, which proves (b). ∎

PROPOSITION 7.4: *Let D be a complete domain with respect to a nontrivial absolute value. Assume that there exists an element $x \in D^\times$ such that $|x| < 1$. Then $K = \mathrm{Quot}(D)$ is rationaly Galois.*

Proof. Let $E = K(x)$. Let G be a finite group. Then G is generated by a finite number of abelian subgroups $G_1, \ldots, G_k$ (e.g., its cyclic subgroups). By Lemma 7.3 D satisfies condition (Large) of Section 6, and we may choose $r, c_1, c_2, \ldots, c_k, c_{k+1} \in D$ such that $r, c_i - c_j \in D^\times$ and $|\frac{r}{c_i - c_j}| \leq 1$ for $1 \leq i < j \leq k+1$. Put $c = c_{k+1}$. This puts us in the setup assumed in Section 6. The claim follows by Proposition 6.6 and Lemma 6.3(a). ∎

Proposition 7.4 reproves the main result of [HV]:

Corollary 7.5: Let K be a complete field with respect to a nontrivial absolute value. Then K is rationaly Galois.

Proof. Since the absolute value is nontrivial, there exists $x \in K$ such that $0 < |x| < 1$. In particular, $x \in K^\times$. Hence the assertion follows from Proposition 7.4. ∎

LEMMA 7.6: *Let D be a complete domain with respect to a nontrivial ultrametric absolute value. Then D contains one of the following rings:*

(a) *the ring $\mathbb{Z}_p$ of p-adic numbers, for some prime number p;*
(b) *the ring $\mathbb{Z}[[x]]$ of formal power series over $\mathbb{Z}$;*
(c) *the ring $F[[x]]$ of formal power series over some finite prime field F.*

Proof. First we assume that $\mathrm{char}(D) = 0$, so $\mathbb{Z} \subseteq D$.

Suppose that $|\cdot|$ is nontrivial on $\mathbb{Z}$ (i.e., there exists an element $x \in \mathbb{Z}$ such that $0 < |x| < 1$). Then the absolute value on $\mathbb{Z} \subseteq D$ corresponds to a p-adic valuation, for some prime number p. Since D is complete, it contains $\mathbb{Z}_p$.

If $|\cdot|$ is trivial on $\mathbb{Z}$, we choose an element $x \in D \smallsetminus \mathbb{Z}$ with $0 < |x| < 1$. Then the valuation that corresponds to the absolute value $|\cdot|$ (restricted to $\mathbb{Z}[x]$) is given by $v(\sum_{n=0}^d a_n x^n) = \min(i \mid a_i \neq 0)$ for each $0 \neq \sum_{n=0}^d a_n x^n \in \mathbb{Z}[x]$. Since $|0| = 0$ (or $v(0) = \infty$), x is free over $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$. As D is complete, it contains the completion $\mathbb{Z}[[x]]$ of $\mathbb{Z}[x]$ with respect to this absolute value.

Now assume that $\mathrm{char}(D) = p$ for some prime number p. Let $F = \mathbb{Z}/p\mathbb{Z} \subseteq D$. Then $|\cdot|$ is trivial on F, and hence, by similar arguments to the ones given above, D contains $F[[x]]$, and x is free over F. ∎

Lemma 7.6 enables us to reduce the proof of our main result from the case of a general complete absolute valued domain to three specific cases. Lemma 3.14 of [Le] proves a similar reduction, from the case of a complete domain at a prime ideal to the same three cases. Thus the result of [Le] is equivalent to our main result, which is:

Theorem 7.7: *Let D_0 be a complete domain with respect to a non-trivial absolute value. Let D be a domain containing D_0. Then $K = \mathrm{Quot}(D)$ is rationaly Galois.*

Proof. By Lemma 7.2 and Lemma 7.6, it suffices to prove the theorem for the the rings $\mathbb{Z}_p, \mathbb{F}_p[[x]], \mathbb{Z}[[x]]$, for each prime number p. The first two cases have complete quotient fields, hence the claim follows for them by Corollary 7.5. Thus we may assume, without loss of generality, that $D = \mathbb{Z}[[x]]$.

Note that D is complete with respect to the valuation given by

$$v(\sum_{n=0}^{\infty} a_n x^n) = \min(i \mid \ a_i \neq 0)$$

for each $0 \neq \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Z}[[x]]$. Unfortunately, its quotient field is not complete with respect to this valuation (Example 2.3(c)), and every element of $D^\times$ is of absolute value 1, so we may not directly apply Proposition 7.4. However, $\mathrm{Quot}(D)$ contains the ring $\mathbb{Z}[[x]][x^{-1}] = \{\sum_{n=m}^{\infty} a_n x^n : m \in \mathbb{Z}, a_n \in \mathbb{Z}\}$, which is also complete with respect to the valuation induced by D on its quotient field (Example 2.3(d)). The element x is in $(\mathbb{Z}[[x]][x^{-1}])^\times$ and satisfies $|x| < 1$. Hence the claim follows by Proposition 7.4. ∎

References

[FJ] M. Fried and M. Jarden, *Field Arithmetic, 2nd edition,* revised and enlarged by M. Jarden, Ergebnisse der Mathematik III, vol. 11, Springer-Verlag, Berlin, 2005.

[FrP] J. Fresnel and M. v.d. Put, *Rigid Analytic Geometry and its Applications,* Progress in Mathematics, vol. 218, Birkhäuser, Boston, 2004.

[Ha] D. Harbater, *Galois coverings of the arithmetic line,* in *Lecture Notes in Mathematics* vol. 1240, Springer, Berlin, 1987, pp. 165–195

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

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

[Ja] M. Jarden, *Regular split embedding problems over complete valued fields,* Notes of a series of talks given in Heidelberg university in 1995–1996.

[Le] T. Lefcourt, *Galois groups and complete domains,* Israel Journal of Mathematics **114** (1999), 323–346.

[Li] Q. Liu, *Tout groupe fini est un groupe de Galois sur $\mathbb{Q}_p(T)$, d'après Harbater,* Proceedings of the Joint AMS Summer Conference "Recent Developments in the Inverse Galois Problem", Seattle, 1993.

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

[Se] J.-P. Serre, *Topics in Galois Theory,* Jones and Bartlett, 1992.