ISRAEL JOURNAL OF MATHEMATICS 93 (1996), 9–27

GALOIS GROUPS OVER COMPLETE VALUED FIELDS

BY

DAN HARAN

Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University, Tel Aviv 69978, Israel
e-mail: haran@math.tau.ac.il

AND

HELMUT VÖLKLEIN*

University of Florida
Gainesville, FL 32611, USA
and
Universität Erlangen, Germany
e-mail: helmut@math.ufl.edu

ABSTRACT

We propose an elementary algebraic approach to the patching of Galois groups. We prove that every finite group is regularly realizable over the field of rational functions in one variable over a complete discrete valued field.

Introduction

Harbater introduced "patching" in [H1] to prove that each finite group occurs as a Galois group over the field of rational functions $K(z)$, where K is the field of fractions of a complete local ring. In particular, this holds if K is any discrete complete valued field. Harbater's work is phrased in the language of formal geometry (i.e., formal schemes). Liu [Li] and Serre [Se, Theorem 8.4.6] translated it into the language of rigid analytic geometry. Both approaches rely on general GAGA theorems relating formal (resp., rigid analytic) geometry to algebraic geometry.

* Partially supported by NSF grant DMS 9306479.
Received March 8, 1995 and in revised form June 2, 1995

In the present paper we give an elementary proof of this theorem that replaces these general GAGA principles by a simple ring-theoretic "GAGA" correspondence based on the so-called "Cartan's Lemma". This approach also yields a short proof of a recent result of Harbater [H5] and Pop [Po]: If K is a countable algebraically closed field, then the absolute Galois group of $K(z)$ is the free profinite group $\hat{F}_\omega$ of countable rank. This implies that $\hat{F}_\omega$ is the absolute Galois group of every function field L of one variable over K, since such L is finite over $K(z)$ (Corollary 4.7).

Cartan's Lemma is basic for the development of rigid analytic geometry. Matrix factorizations as in Cartan's Lemma have also been used by Harbater ([H2] and [H3]) in his formal geometry approach. One of the contributions of this paper lies in isolating a particularly weak variant of Cartan's Lemma that succeeds to render our ring-theoretic version of GAGA.

Further development of Harbater's patching method has culminated in (the first part of) the proof of Abhyankar's Conjecture given by Raynaud [Ray] and Harbater [H4]. (The second part uses other methods from reduction theory.)

The material in this paper is presented from a slightly different point of view in Chapter 11 of the forthcoming book [V].

ACKNOWLEDGEMENT: We thank M. Jarden for many stimulating conversations and suggestions on the topic of this paper. Further, we acknowledge a helpful talk of M. van der Put (Oberflockenbach, February 1994) on the proof of Serre and Liu.

1. Rings of convergent power series

The results of this and the next section are well known. The reader may find them scattered in [BGR] and [FP]. We reprove them here in order to be self-contained, without relying on the whole machinery of rigid analytic geometry.

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

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

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

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

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

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

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

Assume, furthermore, that

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

It then follows from (d) that a series $\sum_{n=0}^{\infty} a_n$ of elements of R converges if and only if $a_n \to 0$.

Remark 1.1: If $a \in R$ and $|a| < 1$, then $1 - a \in R^{\times}$. Indeed, $1 + a + a^2 + \cdots$ converges, say, to $b \in R$. As $(1-a)(1+a+\cdots+a^n) = 1 - a^{n+1} \to 1$, we have $(1-a)b = 1$.

Example 1.2: (i) Let p be a prime. The field $\mathbb{Q}_p$ of p-adic numbers is complete with respect to the p-adic absolute value.

(ii) Let K_0 be a field, and let $0 < \varepsilon < 1$. The field $K_0((t))$ of formal power series $\sum_{i=N}^{\infty} a_i t^i$ with coefficients in K_0 and $N \in \mathbb{Z}$ is complete with respect to the absolute value $|\sum_{i=N}^{\infty} a_i t^i| = \varepsilon^{\min(i|\ a_i \neq 0)}$.

See Lemma 1.3 below for additional examples.

Let z be a free variable over R. Define

$$R\{z\} = \{\sum_{n=0}^{\infty} a_n z^n |\ a_n \in R, \quad \lim_{n\to\infty} a_n = 0\};$$

$$R\{z, z^{-1}\} = \{\sum_{n=-\infty}^{\infty} a_n z^n |\ a_n \in R, \quad \lim_{|n|\to\infty} a_n = 0\}.$$

These sets are commutative rings under the obvious addition and multiplication. Indeed, if $\sum_i a_i z^i, \sum_j a_j z^j \in R\{z, z^{-1}\}$, then $\sum_{i+j=n} a_i b_j$ converges for each $n \in \mathbb{Z}$, say, to $c_n \in R$, and $c_n \to 0$ as $\pm n \to \infty$. Thus $\sum_i a_i z^i \cdot \sum_j b_j z^j = \sum_n c_n z^n \in R\{z, z^{-1}\}$.

View $R\{z\}$ as a subring of $R\{z, z^{-1}\}$.

Define the **norm** $|f|$ of $f = \sum_n a_n z^n \in R\{z, z^{-1}\}$ by $|f| = \max(|a_n|)$.

LEMMA 1.3:

(i) *The norm is an ultrametric absolute value on $R\{z, z^{-1}\}$, extending that on R.*

(ii) *Both $R\{z\}$ and $R\{z, z^{-1}\}$ are complete with respect to the norm.*

(iii) *Each $c \in R$ with $|c| = 1$ defines an* **evaluation homomorphism** $R\{z, z^{-1}\} \to R$ *given by* $f = \sum_n a_n z^n \mapsto f(c) = \sum_n a_n c^n$.

(iv) *Each $c \in R$ with $|c| \leq 1$ defines an* **evaluation homomorphism** $R\{z\} \to R$ *given by* $f = \sum_n a_n z^n \mapsto f(c) = \sum_n a_n c^n$.

(v) *For each $f \in R\{z, z^{-1}\}$ there are $f^+ \in R\{z\}$ and $f^- \in R\{z^{-1}\}$ such that* $f = f^+ + f^-$ and $|f^+|, |f^-| \leq |f|$.

Proof: (i) We check that $|fg| = |f| \cdot |g|$ for $f, g \in R\{z, z^{-1}\}$. Let $f = \sum_{i=-\infty}^{\infty} a_i z^i$ and $g = \sum_{i=-\infty}^{\infty} b_i z^i$. We may assume $f \neq 0$ and $g \neq 0$. Clearly $|fg| \leq |f| \cdot |g|$. Conversely, let n, m be the largest indices such that $|a_n| = |f|$ and $|b_m| = |g|$, let $\ell = n + m$, and consider the coefficient c_ℓ of z^ℓ in fg. If $i + j = \ell$ and $(i, j) \neq (n, m)$ then $i > n$ or $j > m$. Hence $|a_i| < |f|$ or $|b_j| < |g|$, and therefore $|a_i| \cdot |b_j| < |f| \cdot |g|$. Thus $\max_{i+j=\ell}(|a_i b_j|) = |a_n| \cdot |b_m| = |f| \cdot |g|$, and this maximum is obtained only when $(i, j) = (n, m)$. Hence $|c_\ell| = |\sum_{i+j=\ell} a_i b_j| = |f| \cdot |g|$ (by (d′) above), and so $|fg| \geq |f| \cdot |g|$.

Axioms (a), (b), and (d) for an ultrametric absolute value hold trivially.

(ii) Consider a Cauchy sequence (f_n) in $R\{z, z^{-1}\}$. This yields a Cauchy sequence in each coefficient, hence (f_n) converges coefficientwise to some formal sum $f = \sum_n a_n z^n$. It is easy to show that actually $f \in R\{z, z^{-1}\}$ and $|f - f_n| \to 0$. If $f_n \in R\{z\}$ for each n, then $f \in R\{z\}$.

(iii) and (iv) are straightforward.

(v) If $f = \sum_{n=-\infty}^{\infty} a_n z^n$, let $f^+ = \sum_{n=0}^{\infty} a_n z^n$ and $f^- = \sum_{n=-\infty}^{-1} a_n z^n$. ∎

Definition 1.4: For $f = \sum_{n=0}^{\infty} a_n z^n \neq 0$ in $R\{z\}$ define the **pseudodegree** of f to be the integer $d = \max(n : |a_n| = |f|)$. Call f **regular**, if a_d is invertible in R.

Remark 1.5: The map $z \mapsto z^{-1}$ defines a norm-preserving R-automorphism ω of $R\{z, z^{-1}\}$ of order 2. It maps $R\{z\}$ onto $R\{z^{-1}\}$. Thus $R\{z\} \cong R\{z^{-1}\}$. Furthermore, ω maps $R[z]$ onto $R[z^{-1}]$, and $R[z, z^{-1}]$ onto itself.

THEOREM 1.6 (Weierstrass Division Theorem): *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 $f = qg + r$ and $\deg r < d$. Moreover,*

$$|q| \cdot |g| \leq |f| \quad \text{and} \quad |r| \leq |f|. \tag{1}$$

Proof:

PART I: *Estimates (1).* Assume that $f = qg + r$, where $\deg r < d$. If $q = 0$, then (1) is clear. Assume that $q \neq 0$ and let l be the pseudodegree of q. Then $|qg| = |q| \cdot |g|$ equals the value of the coefficient of z^{d+l} in qg; this coefficient is also the coefficient of z^{d+l} in $f = qg + r$, since $\deg r < d + l$. Therefore $|q| \cdot |g| \leq |f|$. It follows that $|r| = |f - qg| \leq \max(|f|, |qg|) \leq |f|$.

PART II: *Uniqueness.* Assume that $f = qg+r = q'g+r'$, where $\deg r, \deg r' < d$. Then $0 = (q - q')g + (r - r')$. By Part I, $|q - q'| = |r - r'| = 0$. Hence $q = q'$ and $r = r'$.

PART III: *Existence if g is a polynomial of degree d.* Write f as $\sum_{n=0}^{\infty} b_n z^n$. For each $m \geq 0$ let $f_m = \sum_{n=0}^{m} b_n z^n \in R[z]$. As g is regular of pseudodegree d, its leading coefficient is invertible. Euclid's algorithm for polynomials over R produces $q_m, r_m \in R[z]$ such that $f_m = q_m g + r_m$ and $\deg r_m < \deg g$. Thus for all k, m we have $f_m - f_k = (q_m - q_k)g + (r_m - r_k)$. By Part I, $|q_m - q_k| \cdot |g|, |r_m - r_k| \leq |f_m - f_k|$. Thus $\{q_m\}_{m=0}^{\infty}$ and $\{r_m\}_{m=0}^{\infty}$ are Cauchy sequences in $R\{z\}$, and hence they converge to $q \in R\{z\}$ and $r \in R[z]$. Clearly $f = qg + r$ and $\deg r < d$.

PART IV: *Existence for arbitrary g.* If $g = \sum_{n=0}^{\infty} a_n z^n$, put $g_0 = \sum_{n=0}^{d} a_n z^n \in R[z]$. Then $|g - g_0| < |g|$. By Part III with g_0 and f there are $q_0 \in R\{z\}$ and $r_0 \in R[z]$ such that $f = q_0 g_0 + r_0$ and $\deg r_0 < d$. By Part I, $|q_0| \leq \frac{|f|}{|g|}$ and $|r_0| \leq |f|$. Thus $f = q_0 g + r_0 + f_1$, where $f_1 = -q_0(g - g_0)$, and $|f_1| \leq \frac{|g-g_0|}{|g|} \cdot |f|$.

Put $f_0 = f$. By induction we get, for each $k \geq 0$, elements $f_k, q_k \in R\{z\}$ and $r_k \in R[z]$ such that $\deg r < d$ and

$$f_k = q_k g + r_k + f_{k+1}, \quad |q_k| \leq \frac{|f_k|}{|g|}, \; |r_k| \leq |f_k|, \quad \text{and} \quad |f_{k+1}| \leq \frac{|g - g_0|}{|g|}|f_k|.$$

It follows that $|f_k| \to 0$, whence also $|q_k|, |r_k| \to 0$. Therefore $q = \sum_{k=0}^{\infty} q_k \in R\{z\}$ and $r = \sum_{k=0}^{\infty} r_k \in R[z]$. Clearly $f = qg + r$ and $\deg r < d$. ∎

COROLLARY 1.7: *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 $|g| = 1$.*

Proof: By Theorem 1.6 there are $q' \in R\{z\}$ and $r' \in R[z]$ of degree $< d$ such that $z^d = q'f + r'$ and $|r'| \leq |z^d| = 1$. Put $g = z^d - r'$. Then g is monic of degree d, and $g = q'f$. Clearly $|g| = 1$. It remains to show that $q' \in R\{z\}^{\times}$.

Notice that g is regular of pseudodegree d. By Theorem 1.6 again, there are $q \in R\{z\}$ and $r \in R[z]$ such that $f = qg + r$ and $\deg r < d$. Thus $f = qq'f + r$. But $f = 1f + 0$ as well. By the uniqueness in Theorem 1.6, $qq' = 1$. Hence $q' \in R\{z\}^\times$. ∎

For the rest of this section let K be a field complete with respect to a non-trivial ultrametric absolute value. Every non-zero $g \in K\{z\}$ is regular. If $g \in K[z]$ is monic of degree d and $|g| = 1$, then g is of pseudodegree d.

COROLLARY 1.8: *Let $g \in K[z]$ be monic of degree d, irreducible in $K[z]$, and $|g| = 1$. Then g is irreducible in $K\{z\}$.*

Proof: The irreducibility of g in $K[z]$ implies that $d > 0$. Therefore g is not a unit in $K\{z\}$, otherwise the two presentations $1 = gg^{-1} + 0$ and $1 = g0 + 1$ contradict the uniqueness in Theorem 1.6.

Suppose that $g = g_1 g_2$, where $g_1, g_2 \in K\{z\}$ are not units. By Corollary 1.7 we may assume that g_1 is a monic polynomial in z, say, of degree d_1, and $|g_1| = 1$. Hence g_1 is of pseudodegree d_1. By Euclid's algorithm there are $q, r \in K[z]$ such that $\deg r < d_1$ and $g = g_1 q + r$. But $g = g_1 g_2 + 0$ as well. The uniqueness in Theorem 1.6 gives $g_2 = q \in K[z]$. Thus either $g_1 \in K[z]^\times \subseteq K\{z\}^\times$ or $g_2 \in K[z]^\times \subseteq K\{z\}^\times$, a contradiction. ∎

LEMMA 1.9: *Let A be either $K\{z\}$ or $K\{z, z^{-1}\}$. Each $f \in A$ can be written as $f = pu$ with $p \in K[z]$ and $u \in A^\times$.*

Proof: For $A = K\{z\}$ the claim follows from Corollary 1.7 (with $R = K$).

Let $A = K\{z, z^{-1}\}$, and let $f = \sum_{n=-\infty}^{\infty} a_n z^n \in A$. We may assume that $f \neq 0$, and $-1 = \min(n : |a_n| = |f|)$ (after multiplying f by a power of z, which is a unit of A).

Set $R = K\{z\}$, and introduce a new variable w. Consider the ring $R\{w\}$ of power series $\sum_{j=0}^{\infty} \alpha_j w^j$ with $\alpha_j \in R$ and $|\alpha_j| \to 0$. Setting $\alpha_0 = \sum_{n=0}^{\infty} a_n z^n$ and $\alpha_j = a_{-j}$ for $j > 0$ we obtain an element $\hat{f} = \sum_{j=0}^{\infty} \alpha_j w^j$ of $R\{w\}$ that is regular of pseudodegree 1. By Corollary 1.7 (with w instead of z) we have $\hat{f} = \hat{p}\hat{u}$, where $\hat{u}$ is a unit of $R\{w\}$ and $\hat{p} = w + \beta$ for some $\beta \in R$.

In particular, $\hat{u}$ is a unit of $A\{w\}$. We have $|z^{-1}| = 1$. The evaluation homomorphism $\theta : A\{w\} \to A$ given by $F \mapsto F(z^{-1})$ maps $\hat{u}$ onto a unit u' of A. Thus $f = \theta(\hat{f}) = \theta(\hat{p})\theta(\hat{u}) = (z^{-1} + \beta)u' = (1 + z\beta)z^{-1}u'$. Replacing f by $f' = 1 + z\beta \in R = K\{z\}$ reduces us to the case that $f \in K\{z\}$. But this case has already been dealt with. ∎

THEOREM 1.10: *The rings $K\{z, z^{-1}\}$, $K\{z\}$, and $K\{z^{-1}\}$ are principal ideal domains. Each ideal is generated by an element of $K[z, z^{-1}]$.*

Proof: Let A be either $K\{z\}$ or $K\{z, z^{-1}\}$. By Lemma 1.9, each ideal I of A is generated by $I' = I \cap K[z]$. This I' is an ideal of $K[z]$, hence $I' = pK[z]$ for some $p \in K[z]$ (since $K[z]$ is a principal ideal domain). Thus $I = pA$ is a principal ideal.

The case of $K\{z^{-1}\}$ follows by Remark 1.5. ∎

Let Q_1, Q_2, and $\hat{Q}$ be the fields of fractions of $K\{z\}$, $K\{z^{-1}\}$, and $K\{z, z^{-1}\}$, respectively. View Q_1, Q_2 as embedded into $\hat{Q}$.

COROLLARY 1.11: *The intersection of Q_1 and Q_2 inside $\hat{Q}$ equals $K(z)$.*

Proof: We have $K[z] \subseteq K\{z\}$ and $K[z^{-1}] \subseteq K\{z^{-1}\}$, hence $K(z) \subseteq Q_1 \cap Q_2$. For the converse, let $f \in Q_1 \cap Q_2$. By Corollary 1.7, $f = f_1/p_1$ with $f_1 \in K\{z\}$ and $0 \neq p_1 \in K[z]$. By Remark 1.5, $f = f_2/p_2$ with $f_2 \in K\{z^{-1}\}$ and $0 \neq p_2 \in K[z^{-1}]$. There are $n, m \in \mathbb{N}$ such that $z^n p_2 \in K[z]$ and $z^{n-m} p_1 \in K[z^{-1}]$. Then the element $g = (z^n p_2) f_1 = z^m (z^{n-m} p_1) f_2$ lies in $K\{z\}$, and $z^{-m} g$ lies in $K\{z^{-1}\}$. Clearly this implies that $g \in K[z]$ (of degree $\leq m$). Thus $f = f_1/p_1 = g/(z^n p_2 p_1) \in K(z)$. ∎

2. GAGA

As in section 1, let K be a field complete with respect to a non-trivial ultrametric absolute value $|\ |$. Let $R_1 = K\{z\}$, $R_2 = K\{z^{-1}\}$, and $R = K\{z, z^{-1}\}$. Let Q_1, Q_2, and $\hat{Q}$ be their fields of fractions, respectively. View Q_1, Q_2 as subfields of $\hat{Q}$.

For a matrix $A = (a_{ij}) \in \mathrm{M}_n(R)$ define the **norm** $||A|| = \max_{ij} |a_{ij}|$ of A.

LEMMA 2.1:

(i) *Every Cauchy sequence in $\mathrm{M}_n(R)$ converges.*

(ii) *$||A + B|| \leq \max(||A||, ||B||)$;*

(iii) *$||AB|| \leq ||A|| \cdot ||B||$;*

(iv) *if $||A|| < 1$, then $I_n - A \in \mathrm{GL}_n(R) = \big(\mathrm{M}_n(R)\big)^\times$.*

(v) *Let $0 < c < 1$. Let (A_i) be a sequence of matrices in $\mathrm{M}_n(R)$ such that $||A_i|| \leq c$ for each i, and $||A_i|| \to 0$. Let $P_i = (I_n - A_1) \cdots (I_n - A_i)$, for $i \geq 1$. Then the sequence (P_i) converges to a matrix in $\mathrm{GL}_n(R)$.*

Proof: Assertions (i), (ii), and (iii) follow from the properties of $|\ |$. The proof of (iv) is a straightforward analogue of Remark 1.1.

(v) Put $P_0 = I_n$. By (ii) and (iii) we have $||P_i|| \le 1$ for each i. Hence

$$(2) \qquad ||P_i - P_{i-1}|| = ||P_{i-1}(I_n - A_i - I_n)|| \le ||P_{i-1}|| \cdot ||A_i|| \le ||A_i|| \to 0.$$

Thus (P_i) is a Cauchy sequence, and hence converges so some $P \in \mathrm{M}_n(R)$. Furthermore, by (ii) and by (2), $||P_j - I_n|| = ||\sum_{i=1}^{j}(P_i - P_{i-1})|| \le \max ||A_i|| \le c$. Hence $||P - I_n|| < 1$, and therefore $P \in \mathrm{GL}_n(R)$ by (iv). ∎

Lemma 2.2 (Cartan's lemma [FP, III.6.3]): *Let $B \in \mathrm{M}_n(R)$ such that $||B - I_n|| < 1$. Then there are $B_1 \in \mathrm{GL}_n(R_1)$ and $B_2 \in \mathrm{GL}_n(R_2)$ such that $B = B_1 B_2$.*

Proof: Deduce from Lemma 1.3(v) that for each $A \in \mathrm{M}_n(R)$ there are $A^+ \in R_1$ and $A^- \in R_2$ such that $A = A^+ + A^-$ and $||A^+||, ||A^-|| \le ||A||$. Let $A_1 = B - I_n$ and $c = ||A_1||$. Then $0 \le c < 1$. The condition

$$I_n + A_{j+1} = (I_n - A_j^+)(I_n + A_j)(I_n - A_j^-)$$

defines recursively a sequence $(A_j)_{j=1}^{\infty}$ in R. From

$$A_{j+1} = A_j^+ A_j^- - A_j^+ A_j - A_j A_j^- + A_j^+ A_j A_j^-$$

it follows that $||A_{j+1}|| \le ||A_j||^2$. By induction, $||A_j|| \le c^j$, and hence $A_j \to 0$. Further,

$$(3) \qquad I_n + A_{j+1} = (I_n - A_j^+) \cdots (I_n - A_1^+)\ B\ (I_n - A_1^-) \cdots (I_n - A_j^-).$$

We have $||A_j^-|| \le ||A_j|| \le c < 1$ and $||A_j^-|| \to 0$. Hence by the Lemma 2.1(v), the partial products $(I_n - A_1^-) \cdots (I_n - A_j^-)$ converge to some $B_2' \in \mathrm{GL}_n(R_2)$. Similarly, the products $(I_n - A_j^+) \cdots (I_n - A_1^+)$ converge to some $B_1' \in \mathrm{GL}_n(R_1)$. Passing to the limit in (3) we get $I_n = B_1' B B_2'$. Hence $B = (B_1')^{-1}(B_2')^{-1}$. ∎

Corollary 2.3: *Let $B \in \mathrm{GL}_n(R)$. Then there are $B_1 \in \mathrm{GL}_n(R \cap Q_1)$ and $B_2 \in \mathrm{GL}_n(R \cap Q_2)$ such that $B = B_1 B_2$.*

Proof: As $K[z, z^{-1}]$ is dense in R, there is $A \in \mathrm{M}_n(K[z, z^{-1}])$ such that $||B^{-1} - A|| < \frac{1}{||B||}$. Then $||BA - I_n|| = ||B(A - B^{-1})|| \le ||B|| \cdot ||A - B^{-1}|| < 1$.

By Lemma 2.1(v), $BA \in \mathrm{GL}_n(R)$. In particular, $A \in \mathrm{GL}_n(R)$ is a regular matrix over $K(z)$, whence $A \in \mathrm{GL}_n(Q_2)$. By Cartan's lemma there are $B_1 \in \mathrm{GL}_n(R_1)$ and $B_2' \in \mathrm{GL}_n(R_2)$ such that $BA = B_1B_2'$. Thus $B = B_1B_2$, where $B_1 \in \mathrm{GL}_n(R_1) \subseteq \mathrm{GL}_n(R \cap Q_1)$ and $B_2 = B_2'A^{-1} \in \mathrm{GL}_n(R) \cap \mathrm{GL}_n(Q_2)$. ∎

3. Patching

Fix a field $\hat{Q}$ and a finite group G. Let $\mathrm{Ind}_1^G \hat{Q} = \{\sum_{g\in G} a_g g |\ a_g \in \hat{Q}\}$ be the free $\hat{Q}$-module with basis G. Then G acts on $\mathrm{Ind}_1^G \hat{Q}$ from the left by $\sigma(ag) = a(\sigma g)$. Turn $\mathrm{Ind}_1^G \hat{Q}$ into a commutative $\hat{Q}$-algebra by $\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g = \sum_{g\in G} a_g b_g g$. (Thus, as a ring, $\mathrm{Ind}_1^G \hat{Q}$ is the direct product of $|G|$ copies of $\hat{Q}$.) The G-action on $\mathrm{Ind}_1^G \hat{Q}$ preserves this multiplication. The unity of $\mathrm{Ind}_1^G \hat{Q}$ is $\sum_{g\in G} 1g$, and $\hat{Q}$ (and every subfield of $\hat{Q}$) embeds into $\mathrm{Ind}_1^G \hat{Q}$ via $a \mapsto \sum_{g\in G} ag$.

For a Galois extension P/Q contained in $\hat{Q}$ such that its Galois group H is a subgroup of G we define

(4)
$$\mathrm{Ind}_H^G P = \{\sum_{g\in G} a_g g \in \mathrm{Ind}_1^G \hat{Q} |\ a_g \in P,\ a_{g\tau} = \tau^{-1}(a_g) \text{ for all } g \in G,\ \tau \in H\}.$$

If Ω is a system of representatives of G/H, then

(4′)
$$\mathrm{Ind}_H^G P = \{\sum_{g\in G} a_g g \in \mathrm{Ind}_1^G \hat{Q} |\ a_\omega \in P,\ a_{\omega\tau} = \tau^{-1}(a_\omega) \text{ for all } \omega \in \Omega,\ \tau \in H\}.$$

LEMMA 3.1: *$\mathrm{Ind}_H^G P$ is a subring of $\mathrm{Ind}_1^G \hat{Q}$. Moreover,*

(a) *$\mathrm{Ind}_H^G P$ is G-invariant.*

(b) *$(\mathrm{Ind}_H^G P)^G = Q$.*

(c) *$\mathrm{Ind}_H^G P$ is isomorphic over Q to the direct product of $(G : H)$ copies of P.*

(d) *$\dim_Q \mathrm{Ind}_H^G P = |G| = \dim_{\hat{Q}} \mathrm{Ind}_1^G \hat{Q}$.*

Proof: (a) Let $\alpha = \sum_{g\in G} a_g g \in \mathrm{Ind}_H^G P$ and $\sigma \in G$. Then $\alpha = \sum_{g\in G} a_{\sigma^{-1}g}\sigma^{-1}g$ and $a_{\sigma^{-1}g\tau} = \tau^{-1}(a_{\sigma^{-1}g})$ for all $g \in G$ and $\tau \in H$. As $\sigma(\alpha) = \sum_{g\in G} a_g(\sigma g) = \sum_{g\in G} a_{\sigma^{-1}g} g$, the last condition implies $\sigma(\alpha) \in \mathrm{Ind}_H^G P$.

(b) The group G fixes $\alpha = \sum_{g\in G} a_g g \in \mathrm{Ind}_H^G P$ if and only if $a_{\sigma g} = a_g$ for all

$\sigma, g \in G$, that is, $a_g = a_1$ for all $g \in G$. Thus

$$(\mathrm{Ind}_H^G P)^G = \{\sum_{g\in G} a\, g |\, a \in P,\ a = \tau^{-1}(a) \text{ for all } \tau \in H\}$$
$$= \{\sum_{g\in G} a\, g |\, a \in Q\} = Q.$$

(c) Let Ω be a system of representatives of G/H. It follows from (4′) that $\sum_{g\in G} a_g g \mapsto \sum_{\omega\in\Omega} a_\omega \omega$ is a Q-isomorphism $\mathrm{Ind}_H^G P \to P^\Omega$.

(d) The assertion follows from (c). ∎

Remark 3.2: A basis of $\mathrm{Ind}_H^G P$ *over* Q. Let β be a primitive element for P/Q, and let $\Omega = \{\omega_1, \ldots, \omega_m\}$ be a system of representatives of G/H. Let $\tau_1, \ldots, \tau_l$ be an enumeration of the elements of H. The following sequence of $|G|$ elements of $\mathrm{Ind}_H^G P$

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

(say, with the lexicographical order) is a basis of $\mathrm{Ind}_1^G \hat{Q}$ over $\hat{Q}$.

Indeed, let $\mathcal{S} = (1g|\ g \in G)$ be the standard basis of $\mathrm{Ind}_1^G \hat{Q}$ over $\hat{Q}$, and let $B \in \mathrm{M}_n(\hat{Q})$ be the transition matrix from $\mathcal{S}$ to $\mathcal{C}$, that is, the matrix defined by $\mathcal{C} = \mathcal{S}B$. 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 $(1(\omega_k\tau_i)|\ 1 \le k \le m,\ 1 \le i \le l)$ (with the lexicographical order). Then B consists of m identical diagonal blocks $B_0 = \big(\tau_i^{-1}(\beta^{j-1})\big) \in \mathrm{M}_l(\hat{Q})$. These are Vandermonde matrices, and hence

$$\det B_0 = \prod_{\substack{\tau,\tau'\in H \\ \tau\neq\tau'}} [\tau(\beta) - \tau'(\beta)] = \pm\, \mathrm{discr}_Q\, \beta \neq 0.$$

Thus $B \in \mathrm{GL}_n(\hat{Q})$, and therefore $\mathcal{C}$ is a basis of $\mathrm{Ind}_1^G \hat{Q}$ over $\hat{Q}$.

By Lemma 3.1(d), $\mathcal{C}$ is also basis of $\mathrm{Ind}_H^G P$ over Q.

Moreover, let R be a subring of $\hat{Q}$ that contains all conjugates $\tau(\beta)$ of β over Q and such that $\mathrm{discr}_Q\, \beta$ is invertible in R. Then the entries of the transition matrix B lie in R, and $\det B \in R^\times$. Hence $B \in \mathrm{GL}_n(R)$.

Definition 3.3: Let I be a set of indices, $|I| \ge 2$.

Patching data $\mathcal{E} = (E, F_i, Q_i, \hat{Q}; G_i, G)_{i\in I}$ consist of fields $E \subseteq F_i, Q_i \subseteq \hat{Q}$ and finite groups $G_i \le G$, for each $i \in I$, such that

(i) F_i/E is a Galois extension with group G_i, for every $i \in I$;
(ii) $F_i \subseteq \bigcap_{j\neq i} Q_j$, for every $i \in I$;
(iii) $\bigcap_{i\in I} Q_i = E$; and
(iv) the subgroups G_i generate G.

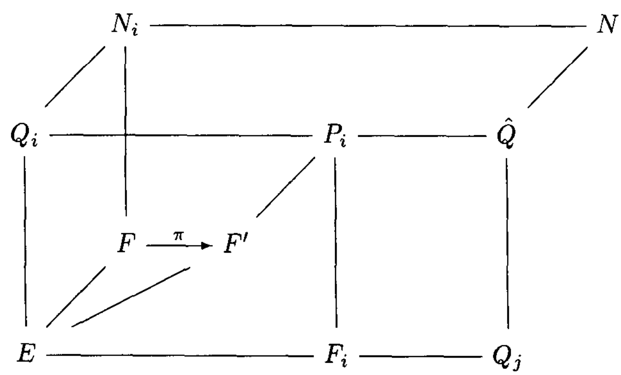
For each $i \in I$ put $P_i = F_iQ_i$, the compositum of F_i and Q_i in $\hat{Q}$. Conditions (ii) and (iii) imply that $F_i \cap Q_i = E$. Hence P_i/Q_i is a Galois extension with group isomorphic (via the restriction of automorphisms) to $G_i = G(F_i/E)$. Identify $G(P_i/Q_i)$ with G_i via this isomorphism.

Let $N = \mathrm{Ind}_1^G \hat{Q}$ and $N_i = \mathrm{Ind}_{G_i}^G P_i \subseteq N$, for each $i \in I$. Let $F = \bigcap_i N_i$. Call $\mathcal{E}' = (E, F_i, Q_i, \hat{Q}; G_i, G;\ P_i, N, N_i, F)_{i\in I}$ the **full patching data** associated with $\mathcal{E}$.

Fix, for the rest of this section, a full patching data

$$\mathcal{E}' = (E, F_i, Q_i, \hat{Q}; G_i, G;\ P_i, N, N_i, F)_{i\in I}.$$

PROPOSITION 3.4: *Assume that:*
(COM) *There is a linear basis of N over $\hat{Q}$ contained in each N_i.*
Then
(a) *F is a Galois field extension of E with group G (via restriction from N);*
(b) *for each i there is a linear basis of F over E that is a basis of N_i over Q_i.*



Proof: By Lemma 3.1, F is an E-algebra. Definition (4) gives an explicit presentation of F as

(5)
$$F = \left\{ \sum_{g\in G} a_g g \in \mathrm{Ind}_1^G \hat{Q} \mid a_g \in \bigcap_{i\in I} P_i,\ a_{g\tau} = \tau^{-1}(a_g) \text{ for all } g \in G,\ \tau \in \bigcup_{i\in I} G_i \right\}.$$

(b) Let $\mathcal{C} = (\alpha_1, \ldots, \alpha_n)$ be the basis mentioned in (COM). Then $\alpha_1, \ldots, \alpha_n \in F$. By Lemma 3.1(b), N_i is a Q_i-algebra, and by Lemma 3.1(d), $\dim_{Q_i} N_i = \dim_{\hat{Q}} N = \#\mathcal{C}$. Therefore $\mathcal{C}$ is a basis of N_i over Q_i. Moreover, $\mathcal{C}$ is a basis of F over E. Indeed, every $b \in N$ can be uniquely written as $b = a_1\alpha_1 + \cdots + a_n\alpha_n$ with $a_1, \ldots, a_n \in \hat{Q}$. Then $b \in N_i$ if and only if $a_1, \ldots, a_n \in Q_i$. Hence $b \in F$ if and only if $a_1, \ldots, a_n \in \bigcap_i Q_i = E$.

(a) We first show that F is a field. Let $\alpha = \sum_{g\in G} a_g g \in F$. Assume that $\alpha \neq 0$. Then the set $X = \{g \in G | \ a_g \neq 0\}$ is not empty. By (5), $X = X(\bigcup_{i\in I} G_i)$. Hence $X = X\langle G_i | \ i \in I\rangle = XG = G$. Let $\alpha' = \sum_{g\in G} a_g^{-1} g$. By (5), $\alpha' \in F$. Clearly $\alpha\alpha' = 1$. Thus α is invertible in F, which proves that F is a field.

By Lemma 3.1(a), the N_i are G-invariant, and hence so is F. By Lemma 3.1(b), $F^G = \bigcap_i N_i^G = \bigcap_i Q_i = E$. By (b), $[F : E] = |G|$, and hence G acts faithfully on F. By Galois theory $G(F/E) = G$. ∎

Condition (COM) is crucial for Proposition 3.4. We will achieve it only in a very special situation.

It will be convenient to identify the field F constructed in Proposition 3.4 with a subfield of $\hat{Q}$:

Definition 3.5: Consider the homomorphism of $\hat{Q}$-algebras π: $\mathrm{Ind}_1^G \hat{Q} \to \hat{Q}$ given by $\sum_{g\in G} a_g g \mapsto a_1$. Then $\pi|_F$ is an isomorphism. We call $\pi(F)$ the **compound** of $\mathcal{E}'$.

We now list some properties of the patching.

LEMMA 3.6: *Assume that $\mathcal{E}'$ satisfies (COM), and let F' be its compound. Then*

(a) *F'/E is a Galois extension with group G.*

(b) *$P_i = F'Q_i$, and the restriction $G(P_i/Q_i) \to G(F'/E)$ is the given inclusion $G_i \to G$, for each $i \in I$.*

(c) *Let L/E be a finite Galois extension, and let ρ: $G \to G(L/E)$ be an epimorphism. Assume that $L \subseteq \bigcap_{i\in I} P_i$ and that $\mathrm{res}_{P_i/L}\tau_i = \rho(\tau_i)$, for every $\tau_i \in G_i \leq G$ and each i. Then $L \subseteq F'$ and $\mathrm{res}_{F'/L}\sigma = \rho(\sigma)$ for each $\sigma \in G$.*

(d) *Let $I = \{1, 2\}$. If G is the semidirect product $G_1 \rtimes G_2$, then $F_2 = (F')^{G_1}$ and res_{F'/F_2} is the projection ρ: $G \to G_2$ (that is the identity on G_2 and $G_1 = \ker\rho$).*

(e) *Fix $i \in I$. Let v be a discrete valuation of E. Assume that it extends to a valuation v_i of Q_i such that the extension Q_i/E is immediate. Then*

(i) *v ramifies in F' if and only it ramifies in F_i;*

(ii) *a decomposition (resp. inertia) group of v in F' is contained in G_i.*

Proof: Let $N = \mathrm{Ind}_1^G \hat{Q}$, and for each $i \in I$ let $P_i = F_i Q_i$ and $N_i = \mathrm{Ind}_{G_i}^G P_i \subseteq N$. Let $F = \bigcap_i N_i$, and let $\pi\colon \mathrm{Ind}_1^G \hat{Q} \to \hat{Q}$ be the projection $\sum_{g\in G} a_g g \mapsto a_1$.

(a) This follows from Proposition 3.4(a). The restriction from N to F is an isomorphism $G \to G(F/E)$. The isomorphism $\pi\colon F \to F'$ induces the isomorphism $G(F/E) \to G(F'/E)$ by $\sigma \mapsto \pi \circ \sigma \circ \pi^{-1}$. Thus G acts on F' by

$$\sigma(\pi(\alpha)) = \pi(\sigma(\alpha)), \qquad \sigma \in G,\ \alpha \in F. \tag{6}$$

(b) By (5), $F' \subseteq P_i$. Let $\tau \in G_i = G(P_i/Q_i)$, and $\alpha = \sum_{g\in G} a_g g \in F$. Then $\tau(\pi(\alpha)) = \tau(a_1) = a_{\tau^{-1}} = \pi(\sum_{g\in G} a_{\tau^{-1}g} g) = \pi(\tau(\alpha))$. By (6), $\mathrm{res}_{F'}\tau = \tau$. In particular, $G(P_i/Q_i) \to G(F'/E)$ is injective, and hence $P_i = F'Q_i$.

(c) Define an embedding $\lambda\colon L \to N$ by $\lambda(a) = \sum_{g\in G} \rho(g^{-1})(a)g$. Clearly $\pi \circ \lambda = \mathrm{id}_L$. If $g \in G$ and $\tau \in G_i$, then

$$\rho((g\tau)^{-1})(a) = \rho(\tau^{-1})\big(\rho(g^{-1})(a)\big) = \tau^{-1}\big(\rho(g^{-1})(a)\big).$$

By (4), $\lambda(L) \subseteq N_i$ for each i, and hence $\lambda(L) \subseteq F$. Thus $L = \pi(\lambda(L)) \subseteq \pi(F) = F'$.

Identify $G(F/E)$ with G via restriction to F. If $\sigma \in G$ and $a \in L$, then

$$\sigma(\lambda(a)) = \sum_{g\in G} \rho(g^{-1})(a)\ (\sigma g) = \sum_{g\in G} \rho((\sigma g)^{-1})\big(\rho(\sigma)(a)\big)\ (\sigma g) = \lambda(\rho(\sigma)(a)).$$

Hence, by (6), $\sigma(a) = \sigma(\pi(\lambda((a))) = \pi(\sigma(\lambda((a))) = \pi(\lambda(\rho(\sigma)(a))) = \rho(\sigma)(a)$.

(d) Let $L = F_2$. If $\tau_1 \in G_1 = G(P_1/Q_1)$, then $\rho(\tau_1) = 1$, and $\mathrm{res}_{P_1/L}(\tau_1) = 1$, since $L = F_2 \subseteq Q_1$. If $\tau_2 \in G_2 = G(P_2/Q_2)$, then $\rho(\tau_2) = \tau_2$, and $\mathrm{res}_{P_2/L}(\tau_2) = \tau_2$, by our identifications. Hence the assertion follows from (c).

(e) All the information comes from completions: Extend v_i to P_i and let $\hat{P}_i/\hat{Q}_i$ be the completion of P_i/Q_i (that is, $\hat{P}_i$ be the completion of P_i, and $\hat{Q}_i$ be the closure of Q_i in $\hat{P}_i$). Let $\hat{v}_i$ be the extension of v_i to $\hat{P}_i$. Then the restriction $G(\hat{P}_i/\hat{Q}_i) \to G(P_i/Q_i)$ maps $G(\hat{P}_i/\hat{Q}_i)$ onto a decomposition group of v_i in P_i, and the inertia group of $\hat{v}_i$ onto an inertia group of v_i in P_i.

As Q_i/E is immediate, and, by (b), $P_i = F'Q_i$, we get that $\hat{P}_i/\hat{Q}_i$ is the completion of F'/E. Thus a decomposition (resp. inertia) group of v in F' is contained in the image G_i of the restriction map $G(P_i/Q_i) \to G(F/E)$. In particular, v ramifies in F' if and only if v_i ramifies in P_i.

Similarly, since $P_i = F_i Q_i$, we get that v ramifies in F_i if and only if v_i ramifies in P_i. Thus v ramifies in F_i if and only if v ramifies in F'. ∎

4. Realization of groups

Let K be a complete field with respect to a non-trivial ultrametric absolute value and let z be transcendental over K. Let $R_1 = R_2' = K\{z\}$, let $R_2 = R_1' = K\{z^{-1}\}$ and $R = K\{z, z^{-1}\}$. Let $Q_1, Q_2, \hat{Q}$ be the quotient fields of R_1, R_2, R, respectively, and let $E = K(z)$. Then $E \subseteq Q_1, Q_2 \subseteq \hat{Q}$. By Corollary 1.11 we have $Q_1 \cap Q_2 = E$. Also denote $R_{10}' = K[z^{-1}]$ and $R_{20}' = K[z]$. Let $Q_1' = Q_2$ and $Q_2' = Q_1$.

LEMMA 4.1: *With $E, Q_1, Q_2, \hat{Q}$ as above, let*

$$(E, F_i, Q_i, \hat{Q}; G_i, G)_{i=1,2} \tag{7}$$

be a patching data. Assume that $F_i = E(\beta_i)$, where β_i and all its conjugates over E are in $Q_i' \cap R$, and $\mathrm{discr}_E\, \beta_i \in R^\times$, for $i = 1, 2$. Then

(a) *condition (COM) of Proposition 3.4 holds;*

(b) *the compound F' of (7) has an unramified K-rational place.*

Proof: Recall (Definition 3.3) that (7) being a patching data means that G is a finite group generated by the subgroups G_1, G_2, we have $F_1 \subseteq Q_2$ and $F_2 \subseteq Q_1$, and F_i/E is a Galois extension with group G_i, for $i = 1, 2$.

(a) Let $1 \le i \le 2$. By Remark 3.2 there is a basis $\mathcal{C}_i$ of $N_i = \mathrm{Ind}_{G_i}^G F_i Q_i$ over Q_i that is also a basis of $N = \mathrm{Ind}_1^G \hat{Q}$ over $\hat{Q}$ such that the transition matrix B_i from the standard basis of N to $\mathcal{C}_i$ is in $\mathrm{GL}_n(R)$. Therefore the transition matrix $B_1^{-1}B_2$ from $\mathcal{C}_1$ to $\mathcal{C}_2$ is in $\mathrm{GL}_n(R)$. By Corollary 2.3 there are $A_1 \in \mathrm{GL}_n(Q_1)$ and $A_2 \in \mathrm{GL}_n(Q_2)$ such that $B_1^{-1}B_2 = A_1A_2$. Put $\mathcal{C} = \mathcal{C}_1A_1 = \mathcal{C}_2A_2^{-1}$. Then $\mathcal{C}$ is a basis of N over $\hat{Q}$ contained in both N_1 and N_2. This gives (COM).

(b) Recall that $F' \subseteq \hat{Q}$. Each $a \in K$ with $|a| = 1$ induces the evaluation homomorphism $z \mapsto a$ from R to K. As R is a principal ideal domain (Theorem 1.10), this homomorphism extends to a K-place $\hat{Q} \to K \cup \{\infty\}$. Its restriction ϕ_a to F' is a K-place. There are infinitely many $a \in K$ with $|a| = 1$. For all but finitely many of them ϕ_a is unramified over E. ∎

Let F/E be a finite Galois extension with group G, and let $\pi\colon F \to F'$ be an isomorphism of fields that maps E onto itself. Then π induces an isomorphism $\mathcal{G}(F/E) \to \mathcal{G}(F'/E)$, and hence $\mathcal{G}(F/E) = G$, where G acts on F' via (6).

In the next lemma consider both $K((z))$ and R as submodules of the K-module of formal double sided power series $\sum_{i=-\infty}^{\infty} a_i z^i$ with coefficients in K.

For $c \neq 0$ in K let μ_c be the automorphism of the field $K((z))$ mapping $f(z) = \sum_{i=N}^{\infty} a_i z^i$ to $f(cz) = \sum_{i=N}^{\infty}(a_i c^i)z^i$. Note that μ_c leaves $E = K(z)$ invariant.

LEMMA 4.2: *Let F/E be a finite Galois extension such that F/K has an unramified prime divisor $\mathcal{P}$ of degree 1.*

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

(b) *Assume that $F \subseteq K((z))$. Let β be a primitive element for F/E. Then there is $r > 0$ with the following property: If $c \in K^\times$ and $|c| < r$, then $\mu_c(\beta)$ and all its conjugates over E are in $Q_1 \cap R$ and $\mathrm{discr}_E\, \mu_c(\beta) \in R^\times$.*

Proof: (a) Let $\mathfrak{p}$ be the prime of E/K below $\mathcal{P}$. Let $\hat{F}$ be the completion of F at $\mathcal{P}$, and let $\hat{E} \subseteq \hat{F}$ be the completion of E at $\mathfrak{p}$. Then $[\hat{F} : \hat{E}] = e(F/E)\, f(F/E) = 1$. Apply an automorphism of E/K to assume that $\mathfrak{p}$ is $z \to 0$. Then $\hat{E} = K((z))$. Hence $F \subseteq \hat{F} = K((z))$.

(b) Let $\beta_1, \ldots, \beta_m$ be the conjugates of β over E. For $i \neq j$ set $\lambda_{ij} = (\beta_i - \beta_j)^{-1} \in F$. All β_i and all λ_{ij} lie in $K((z))$ and are algebraic over E. By a theorem of Artin [Ar, Theorem 2.14] there is $c_0 \in K^\times$ such that the β_i and the λ_{ij} converge at $z = c_0$. Let $c \in K^\times$ such that $|c| < |c_0|$. Then the β_i and the λ_{ij} converge at $z = c$. It follows that we may consider the convergent series $\mu_c(\beta_i), \mu_c(\lambda_{ij})$ as elements of $Q_1 \cap R$ (such that the coefficient of z^{-n} is 0 for sufficiently large n). As $\mu_c(\beta_i - \beta_j)\mu_c(\lambda_{ij}) = 1$, we have $\mu_c(\beta_i) - \mu_c(\beta_j) \in R^\times$. Hence $\mathrm{discr}_E\, \mu_c(\beta) \in R^\times$. ∎

PROPOSITION 4.3: *Let G be a finite group generated by subgroups G_1 and G_2. For $i = 1, 2$ let F_i be a Galois extension of $E = K(z)$ with group G_i such that F_i/K is a regular extension that has an unramified prime of degree 1. Then there exists a Galois extension F of E with group G such that F/K is a regular extension that has an unramified prime of degree 1.*

Moreover, if G is the semidirect product $G_1 \rtimes G_2$, then we may choose F so that $F_2 \subseteq F$ and the restriction map $G(F/E) \to G(F_2/E)$ is the canonical projection $\rho\colon G \to G_2$.

Proof: We may replace F_2 by $F_2' = \theta_2(F_2)$, where $\theta_2\colon F_2 \to F_2'$ is an isomorphism of fields that restricts to an automorphism of E. Indeed, θ_2 induces an isomorphism $G(F_2/E) \to G(F_2'/E)$, and hence $G(F_2'/E) = G_2$. Suppose that $G = G_1 \rtimes G_2$ and that F'/E is a Galois extension with group G so that $F_2' \subseteq F'$ and the restriction map $G(F'/E) \to G(F_2'/E)$ is ρ. Extend θ_2 to an isomorphism of fields $\theta\colon F \to F'$. Then θ induces an isomorphism $G(F/E) \to G(F'/E)$, and hence $G(F/E) = G$, and the restriction map $G(F/E) \to G(F_2/E)$ is ρ.

Apply Lemma 4.2 to replace F_2/E by an isomorphic extension so that $F_2 = E(\beta_2)$, where β_2 and all its conjugates over E are in $Q_1 \cap R$ and $\mathrm{discr}_E\, \beta_2 \in R^\times$. By the same argument and by Remark 1.5 we may assume that $F_1 = E(\beta_1)$, where β_1 and all its conjugates over E are in $Q_2 \cap R$ and $\mathrm{discr}_E\, \beta_1 \in R^\times$. By Lemma 4.1(a) the patching data (7) satisfies (COM) and its compound has an unramified K-rational place. The first assertion follows by Lemma 3.6(a). The second assertion follows by Lemma 3.6(d). ∎

Recall that a local integral domain R with a maximal ideal $\mathfrak{m}$ is complete if $R = \varprojlim_n R/\mathfrak{m}^n$.

THEOREM 4.4 (Harbater): *Let K be the quotient field of a complete local integral domain, properly contained in K. Let G be a finite group. Then there is a Galois extension $F/K(z)$ such that $G(F/K(z)) \cong G$ and F/K is a regular extension that has an unramified prime of degree* 1.

Proof: By [Ja, Corollary 1.6] we may assume that K is a complete field with respect to a non-trivial ultrametric absolute value. Apply inductively Proposition 4.3. Thus it suffices to assume that G is abelian (or even a cyclic p-group). Such a construction is well known (see [FJ, Lemma 24.46] or [V, Section 10.4.2]), except perhaps for the existence of an unramified prime of degree 1. But this follows from the next lemma: ∎

LEMMA 4.5: *Let K be an infinite field, and let $F/K(z)$ be a Galois extension with abelian group G, such that F/K is regular. Then there exists a Galois extension $F'/K(z)$ with group G, regular over K such that F'/K is regular and has an unramified K-rational prime (i.e., a prime of degree 1).*

Proof: Let $E = K(z)$. Only finitely many primes of F/K are ramified over E. Therefore there is a prime $\mathfrak{p}$ of E/K with residue field K and a prime $\mathcal{P}$ of F/K above $\mathfrak{p}$ that is unramified over E. Let L be the residue field of $\mathcal{P}$. Then L/K is a finite Galois extension. As F/K is regular, F and L are linearly disjoint over K. Therefore FL/E is a Galois extension, and $G(FL/E) \cong G(F/E) \times G(L/K)$. Let $\mathfrak{q}$ be a prime of FL/L above $\mathcal{P}$. As FL/L is a constant field extension of F/K, the prime $\mathfrak{q}$ is unramified over F, and hence also over E, and its residue field is L.

Let Δ be the decomposition group of $\mathfrak{q}$ over E, let $F' = (FL)^{\Delta}$ be the decomposition field, and let $\mathcal{P}'$ be the prime of F' below $\mathfrak{q}$. Then the residue field of $\mathcal{P}'$ is K. The algebraic closure of K in F' is contained in the residue field, and hence it is K. Furthermore, F'/K is separable, since FL/K is. Hence F'/K is regular.

It remains to show that Δ is normal in $G(FL/E)$ and $G(FL/E)/\Delta \cong G$. This will follow if we show that $G(FL/E) = G(FL/EL) \times \Delta$.

The restriction π: $G(FL/E) \to G(EL/E)$ maps Δ onto the decomposition group of $\mathfrak{q} \cap EL$ over E. As EL/L is a constant field extension of E/K, this decomposition group is $G(EL/E)$. Therefore $\Delta \cdot G(FL/EL) = \Delta \cdot \mathrm{Ker}(\pi) = G(FL/E)$. As the inertia group of $\mathfrak{q}$ over E is trivial, there is an isomorphism $\Delta \to G(L/K)$, and hence $|\Delta| = [EL : E]$. It follows that $\pi|_{\Delta}$ is an isomorphism, and therefore $\Delta \cap G(FL/EL) = \Delta \cap \mathrm{Ker}(\pi) = 1$. Finally, as $G(FL/E) = G(FL/EL) \times G(FL/F)$, and $G(FL/EL) \cong G$ is abelian, $G(FL/EL)$ lies in the center of $G(FL/E)$. Hence $G(FL/EL)$ commutes with Δ. ∎

THEOREM 4.6: *Let K_0 be an algebraically closed field. Then every finite embedding problem over $K_0(z)$ is solvable.*

Proof: By Tsen's theorem [Ri, Proposition V.5.2], $K_0(z)$ has cohomological dimension 1. Hence the absolute Galois group of $K_0(z)$ is projective [FJ, Remark on p. 293]. By Jarden's lemma [Ma, p. 231] it suffices to show that all split embedding problems over $K_0(z)$ are solvable. So consider the split embedding problem given by a finite Galois extension $L_0/K_0(z)$ and a split surjection ρ: $G \to G(L_0/K_0(z))$. As K_0 is algebraically closed, each (unramified) prime of L_0/K_0 is of degree 1.

PART I: *Solution over a complete field.* Let t be transcendental over L_0, and let $K = K_0((t))$. By Example 1.2, K is complete with respect to a non-trivial ultrametric absolute value. Consider L_0 and $E = K(z)$ as subfields of $L_0((t))$. Then $L_0 \cap K(z) = K_0(z)$. Thus $L = L_0K$ is a Galois extension of E, and the restriction $G(L/E) \to G(L_0/K_0(z))$ is an isomorphism. Each unramified prime of L_0/K_0 extends to an unramified prime of L/K of degree 1.

By Theorem 4.4 there is a Galois extension F_1 of E with group $\mathrm{Ker}\rho$ such that F_1/K is a regular extension that has an unramified prime of degree 1. By Proposition 4.3 there is a Galois extension F of E that contains L and such that $G(F/E) \cong G$ and the surjection $G(F/E) \to G(L/E)$ is ρ. Moreover, F/K is regular. Let α be a primitive element for F/E, integral over $K[z]$. Let $f \in K[Z,Y]$ such that $f(z,Y)$ is the monic irreducible polynomial of α over E. Then F is the quotient field of $K[Z,Y]/f$; as F/K is regular, f is absolutely irreducible.

PART II: *Construction of a Galois cover.* There is a finite sequence $\mathbf{x}$ of elements of K such that $F' = K_0(\mathbf{x}, z, \alpha)$ is a Galois extension of $E' = K_0(\mathbf{x}, z)$ with Galois group isomorphic to $G(F/K(z))$ via the restriction to F'. We may assume that $\mathbf{x}$ contains all coefficients of f. By Bertini-Noether theorem [FJ, Proposition 8.8] we may add to $\mathbf{x}$ the inverse c^{-1} of a suitable $c \in K_0[\mathbf{x}]$ and thus assume that $\phi(f)$ is irreducible over K_0 for every homomorphism $\phi\colon K_0[\mathbf{x}] \to K_0$. Furthermore [FJ, Lemma 17.28] there is a polynomial $g(\mathbf{X}, Z) = g_0(\mathbf{X})Z^m + \cdots + g_m(\mathbf{X})$ over K_0 such that $g_0(\mathbf{x}) \neq 0$, the ring $A = K_0(z)[\mathbf{x}, g(\mathbf{x}, z)^{-1}]$ is integrally closed, and $B = A[\alpha]$ is a Galois ring cover [FJ, p. 57] of A with primitive element α.

PART III: *Specialization.* By Hilbert's Nullstellensatz there is a sequence $\mathbf{a}$ of elements of K_0 such that $g_0(\mathbf{a}) \neq 0$ and $\mathbf{x} \to \mathbf{a}$ is a specialization over K_0. Extend $\mathbf{x} \to \mathbf{a}$ to a $K_0(z)$-homomorphism $\phi\colon A \to K_0(z)$ by $z \mapsto z$, and then to a homomorphism ϕ from B into the algebraic closure $\widetilde{L_0}$ of L_0. Composing ϕ with an automorphism of $\widetilde{L_0}/K_0(z)$, we may assume that ϕ is the identity on L_0.

Let $F_0 = K_0(z, \phi(\alpha))$ be the residue field of ϕ. As $\phi(f)$ is irreducible, $\phi(f)(z,Y)$ is the monic irreducible polynomial of $\phi(\alpha)$ over $K_0(z)$. Hence $[F_0 : K_0(z)] = \deg_Y \phi(f) = \deg_Y f = |G|$. By [FJ, Lemma 5.5], ϕ induces a group isomorphism $G(F'/E') \to G(F_0/K_0(z))$ that extends the restriction $G(L_0E'/E') \to G(L_0/K_0(z))$. Thus F_0 is a solution to the embedding problem. ∎

COROLLARY 4.7: *Let K_0 be a countable algebraically closed field, and let L be a function field of one variable over K_0. Then the absolute Galois group of L is the free profinite group $\hat{F}_\omega$ on countably many generators.*

Proof: By assumption, L is a finite separable extension of $K_0(z)$. By Theorem 4.6 and by Iwasawa's criterion [FJ, Corollary 24.2], $G(K_0(z)) \cong \hat{F}_\omega$. As $G(L)$ is an open subgroup of $G(K_0(z))$, also $G(L) \cong \hat{F}_\omega$ [FJ, Proposition 24.7]. ∎

References

[Ar] E. Artin, *Algebraic Numbers and Algebraic Functions*, Nelson, London, 1968.

[BGR] S. Bosch, U. Güntzer and R. Remmert, *Non-Archimedean Analysis*, Springer-Verlag, Berlin, 1984.

[FJ] M. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik III **11**, Springer-Verlag, Berlin, 1986.

[FP] J. Fresnel and M. van der Put, *Géométrie Analytique Rigide et Applications*, Birkhäuser, Boston, 1981.

[H1] D. Harbater, *Galois coverings of the arithmetic line*, Lecture Notes in Mathematics **1240**, Springer-Verlag, Berlin, 1987, pp. 165–195.

[H2] D. Harbater, *Convergent arithmetic power series*, American Journal of Mathematics **106** (1984), 801–846.

[H3] D. Harbater, *Formal patching and adding branch points*, American Journal of Mathematics **115** (1993), 487–508.

[H4] D. Harbater, *Abhyankar's conjecture on Galois groups over curves*, Inventiones mathematicae **117** (1994), 1–25.

[H5] D. Harbater, *Fundamental groups and embedding problems in characteristic p*, to appear in: Proceedings of the 1993 Seattle Joint AMS Summer Conference "Recent Developments in the Inverse Galois Problem".

[Ja] M. Jarden, *The inverse Galois problem over formal power series fields*, Israel Journal of Mathematics **85** (1994), 263–275.

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

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

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

[Ri] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's University, Kingston, 1970.

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

[Ray] M. Raynaud, *Revêtements de la droite affine en caractéristique* $p > 0$ *et conjecture d'Abhyankar*, Inventiones mathematicae **116** (1994), 425–462.

[V] H. Völklein, *Groups as Galois groups — an introduction*, in preparation.