20 February, 2012

Algebraic Patching*

by

Moshe Jarden, Tel Aviv University

Introduction

The ultimate main goal of Galois theory is to describe the structure of the absolute Galois group $\mathrm{Gal}(\mathbb{Q})$ of $\mathbb{Q}$. This structure will be specified as soon as we know which finite embedding problems can be solved over $\mathbb{Q}$. If every finite Frattini embedding problem and every finite split embedding problem is solvable, then every embedding problem is solvable. However, not every finite Frattini problem over $\mathbb{Q}$ can be solved. For example,

$$(\mathrm{Gal}(\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}),\ \mathbb{Z}/4\mathbb{Z} \to \mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}))$$

is an unsolvable Frattini embedding problem. So, one may ask:

PROBLEM A: *Is every finite split embedding problem over* $\mathbb{Q}$ *solvable?*

More generally, one would like to know:

PROBLEM B: *Let K be a Hilbertian field. Is every finite split embedding problem over K solvable?*

An affirmative answer to Problem B will follow from an affirmative answer to the problem for the subfamily of Hilbertian fields consisting of all rational fields:

PROBLEM C (Débes–Deschamps): *Let K be a field and x a variable. Is every finite split embedding problem over $K(x)$ solvable?*

---

* For more details, including exact references, see "Algebraic Patching", Springer 2011, by Moshe Jarden.

1. Ample Fields

The most significant developement around Problem C is its affirmative solution for ample fields K. This family includes two subfamilies that seemed to have nothing in commen: PAC fields and Henselian fields. Indeed, if K is a PAC field and v is a valuation of K, then the Henselization K_v of K at v is the separable closure K_s of K. In particular, if a PAC field is not separably closed, then it is not Henselian.

Florian Pop made a surprising yet simple and usefull obsrevation that both PAC fields and Henselian fields are existentially closed in the fields of formal power series over them. This property is one of a few equivalent definitions of an ample field.

PROPOSITION 1.1: *The following conditions on a field K are equivalent:*

(a) *For each absolutely irreducible polynomial $f \in K[X,Y]$, the existence of a point $(a,b) \in K^2$ such that $f(a,b)=0$ and $\frac{\partial f}{\partial Y}(a,b) \neq 0$ implies the existence of infinitely many such points.*

(b) *Every absolutely irreducible K-curve C with a simple K-rational point has infinitely many K-rational points.*

(c) *If an absolutely irreducible K-variety V has a simple K-rational point, then $V(K)$ is Zariski-dense in V.*

(d) *Every function field of one variable over K that has a K-rational place has infinitely many K-rational places.*

(e) *K is existentially closed in each Henselian closure $K(t)^h$ of $K(t)$ with respect to the t-adic valuation.*

(f) *K is existentially closed in $K((t))$.*

Proof of (f) $\Longrightarrow$ (a): Inductively suppose there exist $(a_i,b_i) \in K^2$, $i=1,\ldots,n$, such that $f(a_i,b_i)=0$ and $a_1,\ldots,a_n$ are distinct. We choose $a' \in K[[t]]$, t-adically close to a such that $a' \neq a_i$, $i=1,\ldots,n$. Then $f(a',b)$ is t-adically close to 0 and $\frac{\partial f}{\partial Y}(a',b) \neq 0$. Since $K((t))$ is Henselian, there exists $b' \in K[[t]]$ such that $f(a',b')=0$ and $\frac{\partial f}{\partial Y}(a',b') \neq 0$. Since K is existentially closed in $K((t))$, there exists $a_{i+1}, b_{i+1} \in K$ such that $f(a_{i+1},b_{i+1})=0$ and $a_{i+1} \neq a_1,\ldots,a_n$. This concludes the induction. ∎

COROLLARY 1.2: *Every ample field is infinite.*

It is possible to strengthen Condition (b) of Proposition 1.1 considerably.

LEMMA 1.3 (Arno Fehm): *Let K be an ample field, C an absolutely irreducible curve defined over K with a simple K-rational point, and $\varphi\colon C \to C'$ a separable dominant K-rational map to an affine curve $C' \subseteq \mathbb{A}^n$ defined over K. Then, for every proper subfield K_0 of K,* $\mathrm{card}(\varphi(C(K)) \smallsetminus \mathbb{A}^n(K_0)) = \mathrm{card}(K)$.

The proof uses among others a trick of Jochen Koenigsmann that Florian Pop applied to prove Corollary 1.4(b) below.

PROPOSITION 1.4: *Let K be an ample field, V an absolutely irreducible variety defined over K with a K-rational simple point, and K_0 a subfield of K. Then:*

(a) $K = K_0(V(K))$.

(b) $\mathrm{card}(V(K)) = \mathrm{card}(K)$.

PROPOSITION 1.5 (Pop): *Every algebraic extension of an ample field is ample.*

PROBLEM 1.6: *Let L/K be a finite separable extension such that L is ample. Is K ample?*

2. Examples of Ample Fields

The properties causing a field K to be ample vary from diophantine, arithmetic, to Galois theoretic.

(a) PAC fields, in particular, algebraically closed fields.

(b) Henselian fields.

More generally, we say that a pair $(A, \mathfrak{a})$ consisting of a domain A and an ideal $\mathfrak{a}$ of A is **Henselian** if for each $f \in A[X]$ satisfying

$$f(0) \equiv 0 \mod \mathfrak{a} \quad \text{and} \quad f'(0) \text{ is a unit} \mod \mathfrak{a}$$

there exists $x \in \mathfrak{a}$ such that $f(x) = 0$.

Pop has observed that the proof that Henselian fields are ample can be adjusted to a proof that if $(A, \mathfrak{a})$ is a Henselian pair, than $\mathrm{Quot}(A)$ is ample.

(c) If A is complete with respect to a nonzero ideal $\mathfrak{a}$, then $(A, \mathfrak{a})$ is a Henselian pair, hence $\mathrm{Quot}(A)$ is ample.

For example, $K((X_1, \ldots, X_n))$, with $n \geq 1$ and K is any field are ample. So is, for example, the field $\mathrm{Quot}(\mathbb{Z}[[X_1, \ldots, X_n]])$. Note that if $n \geq 2$, then $F = K((X_1, \ldots, X_n))$ is Hilbertian (by Weissauer), hence F is not Henselian (by Geyer) although the ring $K[[X_1, \ldots, X_n]]$ is complete and therfore Henselian.

(d) Real closed fields.

(e) Field satisfying a local global principle.

Let K be a field and $\mathcal{K}$ be a family of field extensions of K. We say that K is P$\mathcal{K}$C (or also that K satisfies a **local global principle** with respect to $\mathcal{K}$) if every nonempty absolutely irreducible variety defined over K with a simple $\bar{K}$-rational point for each $\bar{K} \in \mathcal{K}$ has a K-rational point. In this case, if each $\bar{K} \in \mathcal{K}$ is ample, then K is also ample.

For example, let K be a countable Hilbertian field and S a finite set of **local primes** of K. Thus, each $\mathfrak{p} \in S$ is an equivalent class of absolute values whose completion $\hat{K}_\mathfrak{p}$ is a local field. Let $K_\mathfrak{p} = K_s \cap \hat{K}_\mathfrak{p}$. Consider also an e-tuple $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e)$ taken in random in $\mathrm{Gal}(K)^e$ (with respect to the Haar measure). Let $K_s(\boldsymbol{\sigma})$ be the fixed field in K_s of $\sigma_1, \ldots, \sigma_e$ and let $K_s[\boldsymbol{\sigma}]$ be the maximal Galois extension of K in

$K_s(\boldsymbol{\sigma})$. Then the field

$$K_{\mathrm{tot,S}}[\boldsymbol{\sigma}] = K_s[\boldsymbol{\sigma}] \cap \bigcap_{\mathfrak{p}\in S} \bigcap_{\rho\in\mathrm{Gal}(K)} K_{\mathfrak{p}}^{\rho}$$

is ample (Geyer-Jarden).

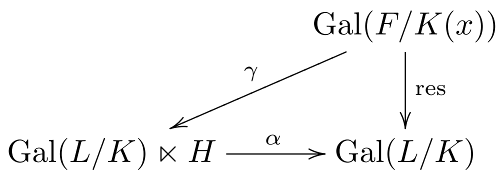
(f) Fields with a pro-p absolute Galois group (Colliot-Thélène, Jarden).

PROBLEM 2.1: *Let K be a field such that the order of* $\mathrm{Gal}(K)$ *is divisible by only finitely many prime numbers. Is K ample?*

3. Finite Split Embedding Problems

The raison d'etre of ample fields is that they are the only known fields for which Problem C has an affirmative answer.

Theorem 3.1 (Pop, Haran-Jarden): *Let K be an ample field, L a finite Galois extension of K, and x a variable. Suppose $\mathrm{Gal}(L/K)$ acts on a finite group H. Then $K(x)$ has a Galois extension F that contains L and there is a commutative diagram*



in which α is the projection on the first component and γ is an isomorphism.

The proof of Theorem 3.1 is done in two steps. First one solves the corresponding embedding problem over the field $\hat{K} = K((t))$ using patching. Then one reduces the solution obtained over $\hat{K}(x)$ to a solution over $K(x)$, using that K is existentially closed in $\hat{K}$.

The most striking application of Theorem 3.1 is a solution of a problem of Field Arithmetic that stayed open for a long time:

Theorem 3.2: *Every PAC Hilbertian field K is ω-free (that is, every finite embedding problem over K is solvable). In particular, if K is countable, then $\mathrm{Gal}(K) \cong \hat{F}_\omega$.*

For the next application we need an improvment of Theorem 3.1.

Theorem 3.3 (Harbater-Stevenson, Pop, Haran-Jarden): *Let K be an ample field and x a variable. Then every finite split embedding problem over $K(x)$ has as many solutions as the cardinality of K.*

In particular, this theorem applies when K is algebraically closed. Since $\mathrm{Gal}(K(x))$ is projective, we get the following generalization of a theorem that was proved in characteristic 0 with the help of Riemann existence theorem.

Corollary 3.4 (Harbater, Pop, Haran-Jarden): *Let K be an algebraically closed field of cardinality m. Then* $\mathrm{Gal}(K) \cong \hat{F}_m$.

Actually, Theorem 3.3 was proved in a stronger form, in which $K(x)$ is replaced by an arbitrary function field E of one variable over K and the solution field is regular over the field of constants of E.

Harbater-Stevenson proved that every finite split embedding problem over $K((t_1, t_2))$ has as many solutions as the cardinality of K. Moreover, this property is inherited by $K((t_1, t_2))_{\mathrm{ab}}$. Finally, the absolute Galois group of the latter field is projective. Together, this proves the following result:

Theorem 3.5: *Let K be a separably closed field and $E = K((t_1, t_2))$. Then* $\mathrm{Gal}(E_{\mathrm{ab}})$ *is isomorphic to the free profinite group $\hat{F}_m$ of cardinality $m = \mathrm{card}(E)$.*

Theorem 3.3 can be improved even more.

Theorem 3.6 (Bary-Soroker, Haran, Harbater; Jarden): *Let E be a function field of one variable over an ample field K. Then* $\mathrm{Gal}(E)$ *is* **semi-free**. *That is, every finite split embedding problem over E*

$$(\mathrm{res}\colon \mathrm{Gal}(E) \to \mathrm{Gal}(F/E),\ \alpha\colon G \to \mathrm{Gal}(F/E))$$

has $\mathrm{card}(E)$**-linearly disjoint solution fields** F_α *(i.e. the fields F_α are linearly disjoint extensions of F.)*

Combining this proposition with results of Bary-Soroker-Haran-Harbater, Efrat, and Pop, we were able to prove the following result.

Theorem 3.7 (Jarden): *Let K be a PAC field of cardinality m and x a variable. For each irreducible polynomial $p \in K[x]$ and every positive integer n satisfying* $\mathrm{char}(K) \nmid n$ *let $\sqrt[n]{p}$ be an nth root of p such that $(\sqrt[mn]{p})^m = \sqrt[n]{p}$ for all m, n. Let $F = K(\sqrt[n]{p})_{p,n}$. Then, F is Hilbertian and* $\mathrm{Gal}(F) \cong \hat{F}_m$.

Here is a special case:

COROLLARY 3.8 (Jarden): *Let K be an PAC field of cardinality m and x a variable. Suppose K contains all root of unity. Then* $\mathrm{Gal}(K(x)_{\mathrm{ab}}) \cong \hat{F}_m$.

And here is another example of a semi-free absolute Galois group:

THEOREM 3.9 (Pop): *Each of the following fields K is Hilbertian and Ample. Moreover,* $\mathrm{Gal}(K)$ *is semi-free of rank* $\mathrm{card}(K)$.

(a) $K = K_0((X_1, \ldots, X_n))$, *whre K_0 is an arbitrary field and $n \geq 2$.*

(b) $K = \mathrm{Quot}(R_0[[X_1, \ldots, X_n]])$, *where R_0 is a Noetherian domain which is a not a field and $n \geq 1$.*

More about Theorem 3.9 can be found in Chapter 12 of "Algebraic Patching".

PROBLEM 3.10: *Give an example of non-ample field K such that every finite split embedding over $K(x)$ is solvable.*

Note that the existence of example as in Problem 3.10 will give a negative answer to Problem C. Conversely, a positive answer to Problem C is a negative answer to Problem 3.10.

4. Axioms for Algebraic Patching

Let E be a field, G a finite group, and $(G_i)_{i \in I}$ a finite family of subgroups of G that generates G. Suppose for each $i \in I$ we have a finite Galois extension F_i of E with Galois group G_i. We use these extensions to construct a Galois extension F of E (not necessarily containing F_i) with Galois group G. First we 'lift' each F_i/E to a Galois field extension Q_i/P_i, where P_i is an appropriate field extension of E (that we refer to as "analytic") such that $P_i \cap F_i = E$ and all of the Q_i's are contained in a common field Q. Then we define F to be the maximal subfield contained in $\bigcap_{i \in I} Q_i$ on which the Galois actions of $\mathrm{Gal}(Q_i/P_i)$ combine to an action of G.

$$\begin{array}{ccccc} P_i & \overset{G_i}{\text{———}} & Q_i & \text{———} & Q \\ | & & | & & \\ E & \overset{G_i}{\text{———}} & F_i & & \end{array}$$

The construction works if certain patching conditions on the initial data are satisfied.

Definition 4.1: Patching data. Let I be a finite set with $|I| \geq 2$. **Patching data**

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

consists of fields $E \subseteq F_i, P_i \subseteq Q$ and finite groups $G_i \leq G$, $i \in I$, such that the following conditions hold.

(1a) F_i/E is a Galois extension with Galois group G_i, $i \in I$.

(1b) $F_i \subseteq P_i'$, where $P_i' = \bigcap_{j \neq i} P_j$, $i \in I$.

(1c) $\bigcap_{i \in I} P_i = E$.

(1d) $G = \langle G_i \mid i \in I \rangle$.

(1e) (Cartan's decomposition) Let $n = |G|$. Then for every $B \in \mathrm{GL}_n(Q)$ and each $i \in I$ there exist $B_1 \in \mathrm{GL}_n(P_i)$ and $B_2 \in \mathrm{GL}_n(P_i')$ such that $B = B_1 B_2$. ∎

We extend $\mathcal{E}$ by more fields. For each $i \in I$ let $Q_i = P_i F_i$ be the compositum of P_i and F_i in Q. Conditions (1b) and (1c) imply that $P_i \cap F_i = E$. Hence Q_i/P_i is a Galois extension with Galois group isomorphic (via restriction of automorphisms) to $G_i = \mathrm{Gal}(F_i/E)$. We identify $\mathrm{Gal}(Q_i/P_i)$ with G_i via this isomorphism.

Definition 4.2: Compound. The **compound** of the patching data $\mathcal{E}$ is the set F of all $a \in \bigcap_{i \in I} Q_i$ for which there exists a function $f\colon G \to \bigcap_{i \in I} Q_i$ such that

(2a) $a = f(1)$ and

(2b) $f(\zeta\tau) = f(\zeta)^\tau$ for every $\zeta \in G$ and $\tau \in \bigcup_{i \in I} G_i$.

Note that f is already determined by $f(1)$. Indeed, by (1d), each $\tau \in \bigcup_{i \in I} G_i$ can be written as $\tau = \tau_1 \tau_2 \cdots \tau_r$ with $\tau_1, \ldots, \tau_r \in \bigcup_{i \in I} G_i$. Hence, by (2b), $f(\tau) = f(1)^{\tau_1 \cdots \tau_r}$.

We call f the **expansion** of a and denote it by f_a. Thus, $f_a(1) = a$ and $f_a(\zeta\tau) = f_a(\zeta)^\tau$ for all $\zeta \in G$ and $\tau \in \bigcup_{i \in I} G_i$. ∎

We list some elementary properties of the expansions:

LEMMA 4.3: *Let F be the compound of $\mathcal{E}$. Then:*

(a) *Every $a \in E$ has an expansion, namely the constant function $\zeta \mapsto a$.*

(b) *Let $a, b \in F$. Then $a+b, ab \in F$; in fact, $f_{a+b} = f_a + f_b$ and $f_{ab} = f_a f_b$.*

(c) *Let $0 \neq a \in F$, then $a^{-1} \in F$. More precisely: $f_a(\zeta) \neq 0$ for all $\zeta \in G$, and $\zeta \mapsto f_a(\zeta)^{-1}$ is the expansion of a^{-1}.*

(d) *Let $a \in F$ and $\sigma \in G$. Then $f_a(\sigma) \in F$; in fact, $f_{f_a(\sigma)}(\zeta) = f_a(\sigma\zeta)$.*

Proof: Statement (a) holds, because $a^\tau = a$ for each $\tau \in \bigcup_{i\in I} G_i$. Next observe that the sum and the product of two expansions is again an expension. Hence, Statement (b) follows from the uniqueness of the expansions and from the observations $(f_{a+b})(1) = a + b = f_a(1) + f_b(1) = (f_a + f_b)(1)$ and $f_{ab}(1) = (f_a f_b)(1)$.

Next we consider a nonzero $a \in F$ and let $\tau \in G$. Using the notation of Definition 4.2, we have $f_a(\tau) = \big((a^{\tau_1})^{\tau_2\cdots}\big)^{\tau_r} \neq 0$. Since taking the inverse in $\bigcap_{i\in I} Q_i$ commutes with the action of G, the map $\zeta \mapsto f_a(\zeta)^{-1}$ is the expansion of a^{-1}. This proves (c).

Finally, we check that the map $\zeta \to f_a(\sigma\zeta)$ has the value $f_a(\sigma)$ at $\zeta = 1$ and it satisfies (2b). Hence, that map is an expansion of $f_a(\sigma)$, as claimed in (d). ∎

Definition 4.4: G-action on F. For $a \in F$ and $\sigma \in G$ put

$$a^\sigma = f_a(\sigma), \tag{3}$$

where f_a is the expansion of a. ∎

LEMMA 4.5: *The compound F of the patching data $\mathcal{E}$ is a field on which G acts by (6) such that $F^G = E$. Moreover, for each $i \in I$, the restriction of this action to G_i coincides with the action of $G_i = \mathrm{Gal}(Q_i/P_i)$ on F as a subset of Q_i.*

Proof: By Lemma 4.3(a),(b),(c), F is a field containing E. Furthermore, (6) defines an action of $\bar{G}$ on F. Indeed, $a^1 = f_a(1) = a$. Moreover, if ζ is another element of G, then by (3) and Lemma 4.3(d), $(a^\sigma)^\zeta = f_a(\sigma)^\zeta = f_{f_a(\sigma)}(\zeta) = f_a(\sigma\zeta) = a^{(\sigma\zeta)}$.

CLAIM: $F^G = E$. Indeed, by Lemma 4.3(a), elements of E have constant expansions, hence are fixed by G. Conversely, let $a \in F^G$. Then for each $i \in I$ we have $a \in Q_i^{G_i} = P_i$. Hence, by (1c), $a \in E$.

The action of G on F maps G onto a subgroup $\bar{G}$ of $\mathrm{Aut}(F)$. It follows from Galois theory that F/E is a Galois extension with Galois group $\bar{G}$. In particular, $[F : E] = |\bar{G}| \leq |G|$.

Finally, let $\tau \in G_i$ and $a \in F$. Then, $f_a(\tau) = f_a(1)^\tau = a^\tau$, where τ acts as an element of $G_i = \mathrm{Gal}(Q_i/P_i)$. Thus, that action coincides with the action given by (6).

∎

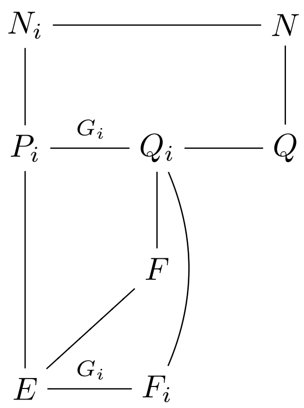
The next goal is to prove that $|\bar{G}| = G$, i.e $\mathrm{Gal}(F/E) \cong G$. To achieve this goal we introduce more objects and invoke Cartan's decomposition. Let

$$N = \Big\{ \sum_{\zeta \in G} a_\zeta \zeta \mid a_\zeta \in Q \Big\} \tag{3}$$

be the vector space over Q with basis $(\zeta \mid \zeta \in G)$, where G is given some fixed ordering. Thus, $\dim_Q N = |G|$. For each $i \in I$ we consider the following subset of N:

$$N_i = \Big\{ \sum_{\zeta \in G} a_\zeta \zeta \in N \mid a_\zeta \in Q_i,\ a_\zeta^\eta = a_{\zeta\eta} \text{ for all } \zeta \in G,\ \eta \in G_i \Big\}. \tag{4}$$

It is a vector space over P_i.



LEMMA 4.6: *For each $i \in I$. the Q-vector space N has a basis which is contained in N_i.*

Proof: Let $\Lambda = \{\lambda_1, \ldots, \lambda_m\}$ be a system of representatives of G/G_i and let $\eta_1, \ldots, \eta_r$ be a listing of the elements of G_i. Thus, $G = \{\lambda_k \eta_\nu \mid k = 1, \ldots, m;\ \nu = 1, \ldots, r\}$. Let z be a primitive element for Q_i/P_i. The following sequence of $|G|$ elements of N_i

$$\Big(\sum_{\nu=1}^{r} (z^{j-1})^{\eta_\nu}\ \lambda_k \eta_\nu \mid j = 1, \ldots, r;\ k = 1, \ldots, m \Big)$$

(in some order) is linearly independent over Q, hence it forms a basis of N over Q.

Indeed, let $a_{jk} \in Q$ such that $\sum_{j=1}^{r}\sum_{k=1}^{m} a_{jk}\big(\sum_{\nu=1}^{r}(z^{j-1})^{\eta_\nu}\ \lambda_k\eta_\nu\big) = 0$. Then

$$\sum_{k=1}^{m}\sum_{\nu=1}^{r}\big(\sum_{j=1}^{r} a_{jk}(z^{j-1})^{\eta_\nu}\ \big)\lambda_k\eta_\nu = 0.$$

This gives $\sum_{j=1}^{r} a_{jk}(z^{j-1})^{\eta_\nu} = 0$ for all k, ν. Thus, for each k, $(a_{1k},\ldots,a_{rk})$ is a solution of the homogeneous system of equations with the Vandermonde matrix $\big((z^{j-1})^{\eta_\nu}\big)$. Since this matrix is invertible, $a_{jk} = 0$ for all j, k. ∎

Lemma 4.7 (Common lemma): *N has a Q-basis in $\bigcap_{i\in I} N_i$.*

Proof: Consider a nonempty subset J of I. Using induction on $|J|$, we find a Q-basis in $\bigcap_{j\in J} N_j$. For $J = I$ this gives the assertion of the lemma.

For each $i \in I$, Lemma 4.6 gives a Q-basis $\mathbf{v}_i$ of N in N_i, so the result follows when $|J| = 1$. Assume $|J| \geq 2$ and fix $i \in J$. By induction N has a Q-basis $\mathbf{u}$ in $\bigcap_{j\in J\smallsetminus\{i\}} N_j$. The transition matrix $B \in \mathrm{GL}_n(Q)$ between $\mathbf{v}_i$ and $\mathbf{u}$ satisfies

$$\mathbf{u} = \mathbf{v}_i B. \tag{3}$$

By (1e), there exist $B_1 \in \mathrm{GL}_n(P_i)$ and $B_2 \in \mathrm{GL}_n(P_i') \subseteq \bigcap_{j\in J\smallsetminus\{i\}} \mathrm{GL}_n(P_j)$. such that $B = B_1B_2$. Then $\mathbf{u}B_2^{-1} = \mathbf{v}_iB_1$ is a Q-basis of N in $\bigcap_{j\in J} N_j$. This finishes the induction. ∎

Lemma 4.8: *Let G be a finite group that acts on a field F and set $E = F^G$. If $[F:E] \geq |G|$, then F/E is a Galois extension whose Galois group is G.*

Proof: Denote the quotient of G by the kernel of the action of G on F. Then $\bar{G}$ is a finite group of automorphisms of F with fixed field E. By a lemma of Artin [Lang, Algebra, Lemma VI.1.8], F/E is a Galois extension with $\mathrm{Gal}(F/E) = \bar{G}$. By assumption, $|G| \geq |\bar{G}| = |\mathrm{Gal}(F/E)| = [F:E] \geq |G|$. Hence, $G = \bar{G} = \mathrm{Gal}(F/E)$. ∎

Now we are in a position to improve Lemma 4.5.

Proposition 4.9: *The compound F of the patching data $\mathcal{E}$ is a Galois extension of E with Galois group G acting by (3). Moreover, $Q_i = P_iF$ for each $i \in I$.*

Proof: We define a map $T\colon F \to N$ by

$$T(a) = \sum_{\zeta \in G} f_a(\zeta)\zeta.$$

By Lemma 4.3(a),(b), T is an E-linear map. By (2b), $f_a(\zeta)^\tau = f_a(\zeta\tau)$ for all $\zeta \in G$ and $\tau \in \bigcup_{i\in I} G_i$, so $\mathrm{Im}(T) = \bigcap_{i\in I} N_i$. By Lemma 4.7, $\mathrm{Im}(T)$ contains $|G|$ linearly independent elements over Q, hence over E. Therefore, $[F : E] = \dim_E F \geq \dim_E \mathrm{Im}(T) \geq |G|$. By Lemma 4.5, F/E is a Galois group and $E = F^G$. Hence, by Lemma 4.8, $\mathrm{Gal}(F/F) = G$.

Finally, by what we have just proved and by Lemma 4.5, the restriction $\mathrm{Gal}(Q_i/P_i) \to \mathrm{Gal}(F/E)$ is injective. Hence, $Q_i = P_iF$. ∎

5. Galois Action on Patching Data

Knowledge of the finite groups that can be realized over a field K does not determine $\mathrm{Gal}(K)$. For that we need control on the finite embedding problems that can be solved over K. Unfortunately, our methods can handle only "finite split embedding problems". However, in some cases (like those that appear in our main results), being able to solve all finite embedding problem suffices.

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

$$\mathrm{pr}\colon \Gamma \ltimes G \to \Gamma \tag{1}$$

of finite groups, where $\Gamma = \mathrm{Gal}(E/E_0)$ is the Galois group of a Galois extension E/E_0, G is a finite group on which Γ acts from the right, $\Gamma \ltimes G$ is the corresponding semidirect product, and pr is the projection on Γ. Each element of $\Gamma \ltimes G$ has a unique representation as a product $\gamma\zeta$ with $\gamma \in \Gamma$ and $\zeta \in G$. The product and the inverse operation are given in $\Gamma \ltimes G$ by the formulas $\gamma\zeta\cdot\delta\eta = \gamma\delta\cdot\zeta^\delta\eta$ and $(\gamma\zeta)^{-1} = \gamma^{-1}(\zeta^{\gamma^{-1}})^{-1}$. A **solution** of (1) is a Galois extension F of E_0 that contains E and an isomorphism $\psi\colon \mathrm{Gal}(F/E_0) \to \Gamma \ltimes G$ such that $\mathrm{pr} \circ \psi = \mathrm{res}_E$. We call F a **solution field** of (1).

Suppose the compound F of patching data $\mathcal{E}$ (§4) realizes G over E. A 'proper' action of Γ on $\mathcal{E}$ will then ensure that F is even a solution field for the embedding problem (1).

Definition 5.1: Let E/E_0 be a finite Galois extension with Galois group Γ. Let

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

be patching data (Definition 4.1). A **proper action** of Γ on $\mathcal{E}$ is a triple that consists of an action of Γ on the group G, an action of Γ on the field Q, and an action of Γ on the set I such that the following conditions hold:

(2a) The action of Γ on Q extends the action of Γ on E.

(2b) $F_i^\gamma = F_{i^\gamma}$, $P_i^\gamma = P_{i^\gamma}$, and $G_i^\gamma = G_{i^\gamma}$, for all $i \in I$ and $\gamma \in \Gamma$.

(2c) $(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma}$ for all $i \in I$, $a \in F_i$, $\tau \in G_i$, and $\gamma \in \Gamma$.

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

Proposition 5.2: *In the notation of Definition 5.1 suppose that* $\Gamma = \mathrm{Gal}(E/E_0)$ *acts properly on the patching data* $\mathcal{E}$ *given in Definition 5.1. Let* F *be the compound of* $\mathcal{E}$*. Then* Γ *acts on* F *via the restriction from its action on* Q *and the actions of* Γ *and* G *on* F *combine to an action of* $\Gamma \ltimes G$ *on* F *with fixed field* E_0*. This gives an identification* $\mathrm{Gal}(F/E_0) = \Gamma \ltimes G$ *such that the following diagram of short exact sequences commutes:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G & \longrightarrow & \Gamma \ltimes G & \xrightarrow{\mathrm{pr}} & \Gamma & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \\ 1 & \longrightarrow & \mathrm{Gal}(F/E) & \longrightarrow & \mathrm{Gal}(F/E_0) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(E/E_0) & \longrightarrow & 1 \end{array}$$

Thus, F *is a solution field of the embedding problem (1).*

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

Part A: *The action of* Γ *on* F.

Let $i \in I$ and $\gamma \in \Gamma$. Then $Q_i = P_iF_i$, so by (2b), $Q_i^\gamma = Q_{i^\gamma}$. Moreover, we have identified $\mathrm{Gal}(Q_i/P_i)$ with $G_i = \mathrm{Gal}(F_i/E)$ via restriction. Hence, by (2b), for all

$a \in P_i$ and $\tau \in G_i$ we have $\tau^\gamma \in G_{i^\gamma}$ and $a^\gamma \in P_{i^\gamma}$, so $(a^\tau)^\gamma = a^\gamma = (a^\gamma)^{\tau^\gamma}$. Together with (2c), this gives

(3) $$(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma} \qquad \text{for all } a \in Q_i \text{ and } \tau \in G_i.$$

Consider an $a \in F$ and let f_a be the expansion of a (Definition). Define $f_a^\gamma\colon G \to \bigcap_{i\in I} Q_i$ by $f_a^\gamma(\zeta) = f_a(\zeta^{\gamma^{-1}})^\gamma$. Then f_a^γ is the expansion f_{a^γ} of a^γ. Indeed, $f_a^\gamma(1) = f_a(1^{\gamma^{-1}})^\gamma = a^\gamma$ and if $\zeta \in G$ and $\tau \in G_i$, then $\tau^{\gamma^{-1}} \in G_{i^{\gamma^{-1}}}$. Hence, by (4) with $i^{\gamma^{-1}}, f_a(\zeta^{\gamma^{-1}}), \tau^{\gamma^{-1}}$, respectively, replacing i, a, τ, we have

$$\begin{aligned} f_a^\gamma(\zeta\tau) = f_a(\zeta^{\gamma^{-1}}\tau^{\gamma^{-1}})^\gamma &= \big(f_a(\zeta^{\gamma^{-1}})^{\tau^{\gamma^{-1}}}\big)^\gamma \\ &= \big(f_a(\zeta^{\gamma^{-1}})^\gamma\big)^{\tau^{\gamma^{-1}\gamma}} = \big(f_a(\zeta^{\gamma^{-1}})^\gamma\big)^\tau = f_a^\gamma(\zeta)^\tau. \end{aligned}$$

Thus $a^\gamma \in F$. It follows that the action of Γ on Q restricts to an action of Γ on F.

Part B: *The action of* $\Gamma \ltimes G$ *on* F. Let $a \in F$ and $\gamma \in \Gamma$. We claim that

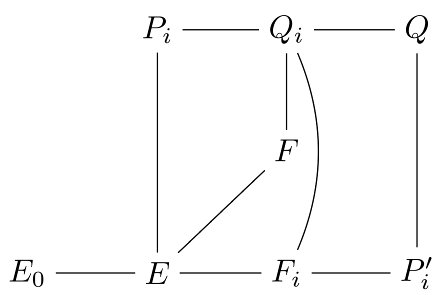
(4) $$(a^\sigma)^\gamma = (a^\gamma)^{\sigma^\gamma} \qquad \text{for all } \sigma \in G,$$

where $a^\sigma = f_a(\sigma)$ (Definition 4.4). Indeed, write σ as a word in $\bigcup_{i\in I} G_i$. Then (4) follows from (4) by induction on the length of the word. If $\sigma = 1$, then (4) is an identity. Suppose (4) holds for some $\sigma \in G$ and let $\tau \in \bigcup_{i\in I} G_i$. Using the identification of the action of each $\tau \in G_i$ on F as an element of G_i with its action as an element of G (Lemma 4.5(a)) and (4) for a^σ rather that a, we have

$$(a^{\sigma\tau})^\gamma = \big((a^\sigma)^\tau\big)^\gamma = \big((a^\sigma)^\gamma\big)^{\tau^\gamma} = \big((a^\gamma)^{\sigma^\gamma}\big)^{\tau^\gamma} = (a^\gamma)^{\sigma^\gamma\tau^\gamma} = (a^\gamma)^{(\sigma\tau)^\gamma}.$$

Now we apply (4) to $a^{\gamma^{-1}}$ instead of a to find that $\Big(\big(a^{\gamma^{-1}}\big)^\sigma\Big)^\gamma = a^{\sigma^\gamma}$. It follows that the actions of Γ and G on F combine to an action of $\Gamma \ltimes G$ on F.

(5)



Part C: *Conclusion of the proof.* Since $F^G = E$ (Lemma 4.5) and $E^\Gamma = E_0$, we have $F^{\Gamma \ltimes G} = E_0$. Furthermore, $[F : E_0] = [F : E] \cdot [E : E_0] = |G| \cdot |\Gamma| = |\Gamma \ltimes G|$. By Galois theory, $\mathrm{Gal}(F/E_0) = \Gamma \ltimes G$ and the map res: $\mathrm{Gal}(F/E_0) \to \mathrm{Gal}(E/E_0)$ coincides with the canonical map pr: $\Gamma \ltimes G \to \Gamma$. ∎

6. Normed Rings

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

Let A be a commutative ring with 1. An **ultrametric absolute value** of A is a function $|\ |: A \to \mathbb{R}$ satisfying the following conditions:

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

(1b) There exists $a \in A$ such that $0 < |a| < 1$.

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

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

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

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

Denote the ordered additive group of the real numbers by $\mathbb{R}^+$. The function v: $\mathrm{Quot}(A) \to \mathbb{R}^+ \cup \{\infty\}$ defined by $v(a) = -\log |a|$ satisfies the following conditions:

(2a) $v(a) = \infty$ if and only if $a = 0$.

(2b) There exists $a \in \mathrm{Quot}(A)$ such that $0 < v(a) < \infty$.

(2c) $v(ab) = v(a) + v(b)$.

(2d) $v(a + b) \geq \min\{v(a), v(b)\}$ (and $v(a + b) = v(b)$ if $v(b) < v(a)$).

In other words, v is a **real valuation** of $\mathrm{Quot}(A)$. Conversely, every real valuation

v: Quot$(A) \to \mathbb{R}^+ \cup \{\infty\}$ gives rise to a nontrivial ultrametric absolute value $|\cdot|$ of Quot(A): $|a| = \varepsilon^{v(a)}$, where ε is a fixed real number between 0 and 1.

An attempt to extend an absolute value from A to a larger ring A' may result in relaxing Condition (1c), replacing the equality by an inequality. This leads to the more general notion of a 'norm'.

Definition 6.1: Normed rings. Let R be an associative ring with 1. A **norm** on R is a function $\| \ \|$: $R \to \mathbb{R}$ that satisfies the following conditions for all $a, b \in R$:

(3a) $\|a\| \geq 0$, and $\|a\| = 0$ if and only if $a = 0$; further $\|1\| = \|-1\| = 1$.

(3b) There is an $x \in R$ with $0 < \|x\| < 1$.

(3c) $\|ab\| \leq \|a\| \cdot \|b\|$.

(3d) $\|a + b\| \leq \max(\|a\|, \|b\|)$.

The norm $\| \ \|$ naturally defines a topology on R whose basis is the collection of all sets $U(a_0, r) = \{a \in R \mid \|a - a_0\| < r\}$ with $a_0 \in R$ and $r > 0$. Both addition and multiplication are continuous under that topology. Thus, R is a **topological ring**.

∎

Definition 6.2: Complete rings. Let R be a normed ring. A sequence $a_1, a_2, a_3, \ldots$ of elements of R is **Cauchy** if for each $\varepsilon > 0$ there exists m_0 such that $\|a_n - a_m\| < \varepsilon$ for all $m, n \geq m_0$. We say that R is **complete** if every Cauchy sequence converges. ∎

Lemma 6.3: 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 sequence $a_1, a_2, a_3, \ldots$ of elements of R is Cauchy if for each $\varepsilon > 0$ there exists m_0 such that $\|a_{m+1} - a_m\| < \varepsilon$ for all $m \geq m_0$.

(d) The map $x \mapsto \|x\|$ from R to $\mathbb{R}$ is continuous.

(e) If R is complete, then a series $\sum_{n=0}^{\infty} a_n$ of elements of R converges if and only if $a_n \to 0$.

(f) If R is complete and $\|a\| < 1$, then $1 - a \in R^\times$. Moreover, $(1 - a)^{-1} = 1 + b$ with $\|b\| < 1$.

Proof of (a): Observe that $\|-a\| \le \|-1\| \cdot \|a\| = \|a\|$. Replacing a by $-a$, we get $\|a\| \le \|-a\|$, hence the claimed equality.

Proof of (b): Assume $\|a+b\| < \|b\|$. Then, by (a), $\|b\| = \|(-a)+(a+b)\| \le \max(\|-a\|, \|a+b\|) < \|b\|$, which is a contradiction.

Proof of (c): With m_0 as above let $n > m \ge m_0$. Then

$$\|a_n - a_m\| \le \max(\|a_n - a_{n-1}\|, \ldots, \|a_{m+1} - a_m\|) < \varepsilon.$$

Proof of (d): By (3d), $\|x\| = \|(x-y)+y\| \le \max(\|x-y\|, \|y\|) \le \|x-y\| + \|y\|$. Hence, $\|x\| - \|y\| \le \|x-y\|$. Symmetrically, $\|y\| - \|x\| \le \|y-x\| = \|x-y\|$. Therefore, $|\,\|x\| - \|y\|\,| \le \|x-y\|$. Consequently, the map $x \mapsto \|x\|$ is continuous.

Proof of (e): Let $s_n = \sum_{i=0}^n a_i$. Then $s_{n+1} - s_n = a_{n+1}$. Thus, by (c), $s_1, s_2, s_3, \ldots$ is a Cauchy sequence if and only if $a_n \to 0$. Hence, the series $\sum_{n=0}^\infty a_n$ converges if and only if $a_n \to 0$.

Proof of (f): The elements a^i tend to 0 as i approaches ∞. Hence, by (e), $\sum_{i=0}^\infty a^i$ converges. The identities $(1-a)\sum_{i=0}^n a^i = 1 - a^{n+1}$ and $\sum_{i=0}^n a^i(1-a) = 1 - a^{n+1}$ imply that $\sum_{i=0}^\infty a^i$ is both the right and the left inverse of $1-a$. Moreover, $\sum_{i=0}^\infty a^i = 1 + b$ with $b = \sum_{i=1}^\infty a^i$ and $\|b\| \le \max_{i \ge 1} \|a\|^i < 1$. ∎

Example 6.4:

(a) Every field K with an ultrametric absolute value is a normed ring. For example, for each prime number p, $\mathbb{Q}$ has a p-adic absolute value $|\cdot|_p$ which is defined by $|x|_p = p^{-m}$ if $x = \frac{a}{b}p^m$ with $a, b, m \in \mathbb{Z}$ and $p \nmid a, b$.

(b) The ring $\mathbb{Z}_p$ of p-adic integers and the field $\mathbb{Q}_p$ of p-adic numbers are complete with respect to the p-adic absolute value.

(c) Let K_0 be a field and let $0 < \varepsilon < 1$. The ring $K_0[[t]]$ (resp. field $K_0((t))$) of formal power series $\sum_{i=0}^\infty a_i t^i$ (resp. $\sum_{i=m}^\infty a_i t^i$ with $m \in \mathbb{Z}$) with coefficients in K_0 is complete with respect to the absolute value $|\sum_{i=m}^\infty a_i t^i| = \varepsilon^{\min(i \mid a_i \ne 0)}$.

(d) Let $\|\cdot\|$ be a norm of a commutative ring A. For each positive integer n we extend the norm to the associative (but usually not commutative) ring $\mathrm{M}_n(A)$ of all

$n \times n$ matrices with entries in A by

$$\|(a_{ij})_{1\le i,j\le n}\| = \max(\|a_{ij}\|_{1\le i,j\le n}).$$

If $b = (b_{jk})_{1\le j,k\le n}$ is another matrix and $c = ab$, then $c_{ik} = \sum_{j=1}^n a_{ij}b_{jk}$ and $\|c_{ik}\| \le \max(\|a_{ij}\| \cdot \|b_{jk}\|) \le \|a\| \cdot \|b\|$. Hence, $\|c\| \le \|a\|\|b\|$. This verifies Condition (3c). The verification of (3a), (3b), and (3d) is straightforward. Note that when $n \ge 2$, even if the initial norm of A is an absolute value, the extended norm satisfies only the weak condition (3c) and not the stronger condition (1c), so it is not an absolute value.

If A is complete, then so is $\mathrm{M}_n(A)$. Indeed, let $a_i = (a_{i,rs})_{1\le r,s\le n}$ be a Cauchy sequence in $\mathrm{M}_n(A)$. Since $\|a_{i,rs} - a_{j,rs}\| \le \|a_i - a_j\|$, each of the sequences $a_{1,rs}, a_{2,rs}, a_{3,rs}, \ldots$ is Cauchy, hence converges to an element b_{rs} of A. Set $b = (b_{rs})_{1\le r,s\le n}$. Then $a_i \to b$. Consequently, $\mathrm{M}_n(A)$ is complete. ∎

Like absolute valued rings, every normed ring has a completion:

LEMMA 6.5: *Every normed ring $(R, \| \,\|)$ can be embedded into a complete normed ring $(\hat{R}, \| \,\|)$ such that R is dense in $\hat{R}$ and the following universal condition holds:*

(4) *Each continuous homomorphism f of R into a complete ring S uniquely extends to a continuous homomorphism $\hat{f}\colon \hat{R} \to S$.*

The normed ring $(\hat{R}, \| \,\|)$ is called the **completion** *of $(R, \| \,\|)$.*

Proof: We consider the set A of all Cauchy sequences $\mathbf{a} = (a_n)_{n=1}^\infty$ with $a_n \in R$. For each $\mathbf{a} \in A$, the values $\|a_n\|$ of its components are bounded. Hence, A is closed under componentwise addition and multiplication and contains all constant sequences. Thus, A is a ring. Let $\mathfrak{n}$ be the ideal of all sequences that converge to 0. We set $\hat{R} = A/\mathfrak{n}$ and identify each $x \in R$ with the coset $(x)_{n=1}^\infty + \mathfrak{n}$.

If $\mathbf{a} \in A \smallsetminus \mathfrak{n}$, then $\|a_n\|$ eventually becomes constant. Indeed, there exists $\beta > 0$ such that $\|a_n\| \ge \beta$ for all sufficiently large n. Choose n_0 large such that $\|a_n - a_m\| < \beta$ for all $n, m \ge n_0$. Then, $\|a_n - a_{n_0}\| < \beta \le \|a_{n_0}\|$, so $\|a_n\| = \|(a_n - a_{n_0}) + a_{n_0}\| = \|a_{n_0}\|$. We define $\|\mathbf{a}\|$ to be the eventual absolute value of a_n and note that $\|\mathbf{a}\| \ne 0$. If $\mathbf{b} \in \mathfrak{n}$, we set $\|\mathbf{b}\| = 0$ and observe that $\|\mathbf{a} + \mathbf{b}\| = \|\mathbf{a}\|$. It follows that $\|\mathbf{a} + \mathfrak{n}\| = \|\mathbf{a}\|$ is a well defined function on $\hat{R}$ which extends the norm of R.

One checks that $\| \ \|$ is a norm on $\hat{R}$ and that R is dense in $\hat{R}$. Indeed, if $\mathbf{a} = (a_n)_{n=1}^\infty \in A$, then $a_n + \mathfrak{n} \to \mathbf{a} + \mathfrak{n}$. To prove that $\hat{R}$ is complete under $\| \ \|$ we consider a Cauchy sequence $(a_k)_{k=1}^\infty$ of elements of $\hat{R}$. For each k we choose an element $b_k \in R$ such that $\|b_k - a_k\| < \frac{1}{k}$. Then $(b_k)_{k=1}^\infty$ is a Cauchy sequence of R and the sequence $(\mathbf{a}_k)_{k=1}^\infty$ converges to the element $(b_k)_{k=1}^\infty + \mathfrak{n}$ of $\hat{R}$.

Finally, let S be a complete normed ring and $f\colon R \to S$ a continuous homomorphism. Then, for each $\mathbf{a} = (a_n)_{n=1}^\infty \in A$, the sequence $(f(a_n))_{n=1}^\infty$ of S is Cauchy, hence it converges to an element s. Define $\hat{f}(\mathbf{a} + \mathfrak{n}) = s$ and check that $\hat{f}$ has the desired properties. ∎

7. Rings of Convergent Powere Series

Let A be a complete normed commutative ring and x a variable. Consider the following subset of $A[[x]]$:

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

For each $f = \sum_{n=0}^\infty a_n x^n \in A\{x\}$ we define $\|f\| = \max(\|a_n\|)_{n=0,1,2,\ldots}$. This definition makes sense because $a_n \to 0$, hence $\|a_n\|$ is bounded.

We prove the Weierstrass division and the Weierstrass preparation theorems for $A\{x\}$ in analogy to the corresponding theorems for the ring of formal power series in one variable over a local ring.

LEMMA 7.1:

(a) *$A\{x\}$ is a subring of $A[[x]]$ containing A.*

(b) *The function $\| \ \|\colon A\{x\} \to \mathbb{R}$ is a norm.*

(c) *The ring $A\{x\}$ is complete under that norm.*

(d) *Let B be a complete normed ring extension of A. Then each $b \in B$ with $\|b\| \le 1$ defines an* **evaluation homomorphism** *$A\{x\} \to B$ given by*

$$f = \sum_{n=0}^\infty a_n x^n \mapsto f(b) = \sum_{n=0}^\infty a_n b^n.$$

Proof of (a): We prove only that $A\{x\}$ is closed under multiplication. To that end let $f = \sum_{i=0}^{\infty} a_i x^i$ and $g = \sum_{j=0}^{\infty} b_j x^j$ be elements of $A\{x\}$. Consider $\varepsilon > 0$ and let n_0 be a positive number such that $\|a_i\| < \varepsilon$ if $i \geq \frac{n_0}{2}$ and $\|b_j\| < \varepsilon$ if $j \geq \frac{n_0}{2}$. Now let $n \geq n_0$ and $i + j = n$. Then $i \geq \frac{n_0}{2}$ or $j \geq \frac{n_0}{2}$. It follows that $\|\sum_{i+j=n} a_i b_j\| \leq \max(\|a_i\| \cdot \|b_j\|)_{i+j=n} \leq \varepsilon \cdot \max(\|f\|, \|g\|)$. Thus, $fg = \sum_{n=0}^{\infty} \sum_{i+j=n} a_i b_j x^n$ belongs to $A\{x\}$, as claimed.

Proof of (b): Standard checking.

Proof of (c): Let $f_i = \sum_{n=0}^{\infty} a_{in} x^n$, $i = 1, 2, 3, \ldots$, be a Cauchy sequence in $A\{x\}$. For each $\varepsilon > 0$ there exists i_0 such that $\|a_{in} - a_{jn}\| \leq \|f_i - f_j\| < \varepsilon$ for all $i, j \geq i_0$ and for all n. Thus, for each n, the sequence $a_{1n}, a_{2n}, a_{3n}, \ldots$ is Cauchy, hence converges to an element $a_n \in A$. If we let j tend to infinity in the latter inequality, we get that $\|a_{in} - a_n\| < \varepsilon$ for all $i \geq i_0$ and all n. Set $f = \sum_{i=0}^{\infty} a_n x^n$. Then $a_n \to 0$ and $\|f_i - f\| = \max(\|a_{in} - a_n\|)_{n=0,1,2,\ldots} < \varepsilon$ if $i \geq i_0$. Consequently, the f_i's converge in $A\{x\}$.

Proof of (d): Note that $\|a_n b^n\| \leq \|a_n\| \to 0$, so $\sum_{n=0}^{\infty} a_n b^n$ is an element of B. ∎

Definition 7.2: Let $f = \sum_{n=0}^{\infty} a_n x^n$ be a nonzero element of $A\{x\}$. We define the **pseudo degree** of f to be the integer $d = \max\{n \geq 0 \mid \|a_n\| = \|f\|\}$ and set

$$\text{pseudo.deg}(f) = d.$$

The element a_d is the **pseudo leading coefficient** of f. Thus, $\|a_d\| = \|f\|$ and $\|a_n\| < \|f\|$ for each $n > d$. If $f \in A[x]$ is a polynomial, then $\text{pseudo.deg}(f) \leq \deg(f)$. If a_d is invertible in A and satisfies $\|ca_d\| = \|c\| \cdot \|a_d\|$ for all $c \in A$, we call f **regular**. In particular, if A is a field and $\| \ \|$ is an ultrametric absolute value, then each $0 \neq f \in A\{x\}$ is regular. The next lemma implies that in this case $\| \ \|$ is an absolute value of $A\{x\}$. ∎

Lemma 7.3 (Gauss' Lemma): *Let $f, g \in A\{x\}$. Suppose f is regular of pseudo degree d and $f, g \neq 0$. Then $\|fg\| = \|f\| \cdot \|g\|$ and* $\text{pseudo.deg}(fg) = \text{pseudo.deg}(f) + \text{pseudo.deg}(g)$.

Proof: Let $f = \sum_{i=0}^{\infty} a_i x^i$ and $g = \sum_{j=0}^{\infty} b_j x^j$. Let a_d (resp. b_e) be the pseudo leading coefficient of f (resp. g). Then $fg = \sum_{n=0}^{\infty} c_n x^n$ with $c_n = \sum_{i+j=n} a_i b_j$.

If $i+j = d+e$ and $(i,j) \neq (d,e)$, then either $i > d$ or $j > e$. In each case, $\|a_i b_j\| \leq \|a_i\|\|b_j\| < \|f\| \cdot \|g\|$. By our assumption on a_d, we have $\|a_d b_e\| = \|a_d\| \cdot \|b_e\| = \|f\| \cdot \|g\|$. By Lemma 6.3(b), this implies $\|c_{d+e}\| = \|f\| \cdot \|g\|$.

If $i + j > d + e$, then either $i > d$ and $\|a_i\| < \|f\|$ or $j > e$ and $\|b_j\| < \|g\|$. In each case $\|a_i b_j\| \leq \|a_i\| \cdot \|b_j\| < \|f\| \cdot \|g\|$. Hence, $\|c_n\| < \|c_{d+e}\|$ for each $n > d + e$. Therefore, c_{d+e} is the pseudo leading coefficient of fg, and the lemma is proved. ∎

Proposition 7.4 (Weierstrass division theorem): *Let $f \in A\{x\}$ and let $g \in A\{x\}$ be regular of pseudo degree d. Then there are unique $q \in A\{x\}$ and $r \in A[x]$ such that $f = qg + r$ and $\deg(r) < d$. Moreover,*

$$\|qg\| = \|q\| \cdot \|g\| \leq \|f\| \qquad \textit{and} \qquad \|r\| \leq \|f\| \tag{1}$$

Proof: We break the proof into several parts.

Part A: *Proof of (1).* First we assume that there exist $q \in A\{x\}$ and $r \in A[x]$ such that $f = qg + r$ with $\deg(r) < d$. If $q = 0$, then (1) is clear. Otherwise, $q \neq 0$ and we let $e = \text{pseudo.deg}(q)$. By Lemma 7.3, $\|qg\| = \|q\| \cdot \|g\|$ and $\text{pseudo.deg}(qg) = e + d > \deg(r)$. Hence, the coefficient c_{d+e} of x^{d+e} in qg is also the coefficient of x^{d+e} in f. It follows that $\|qg\| = \|c_{d+e}\| \leq \|f\|$. Consequently, $\|r\| = \|f - qg\| \leq \|f\|$.

Part B: *Uniqueness.* Suppose $f = qg+r = q'g+r'$, where $q, q' \in A\{x\}$ and $r, r' \in A[x]$ are of degrees less than d. Then $0 = (q - q')g + (r - r')$. By Part A, applied to 0 rather than to f, $\|q - q'\| \cdot \|g\| = \|r - r'\| = 0$. Hence, $q = q'$ and $r = r'$.

Part C: *Existence if g is a polynomial of degree d.* Write $f = \sum_{n=0}^{\infty} b_n x^n$ with $b_n \in A$ converging to 0. For each $m \geq 0$ let $f_m = \sum_{n=0}^{m} b_n x^n \in A[x]$. Then the $f_1, f_2, f_3, \ldots$ converge to f, in particular they form a Cauchy sequence. Since g is regular of pseudo degree d, its leading coefficient is invertible. Euclid's algorithm for polynomials over A produces $q_m, r_m \in A[x]$ with $f_m = q_m g + r_m$ 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 A, $\|q_m - q_k\| \cdot \|g\|, \|r_m - r_k\| \leq \|f_m - f_k\|$. Thus, $\{q_m\}_{m=0}^{\infty}$ and $\{r_m\}_{m=0}^{\infty}$ are Cauchy sequences in $A\{x\}$. Since $A\{x\}$ is complete

(Lemma 7.1), the q_m's converge to some $q \in A\{x\}$. Since A is complete, the r_m's converge to an $r \in A[x]$ of degree less than d. It follows that $f = qg + r$

Part D: *Existence for arbitrary g.* Let $g = \sum_{n=0}^{\infty} a_n x^n$ and set $g_0 = \sum_{n=0}^{d} a_n x^n \in A[x]$. Then $\|g - g_0\| < \|g\|$. By Part C, there are $q_0 \in A\{x\}$ and $r_0 \in A[x]$ such that $f = q_0 g_0 + r_0$ and $\deg(r_0) < d$. By Part A, $\|q_0\| \leq \frac{\|f\|}{\|g\|}$ and $\|r_0\| \leq \|f\|$. Thus, $f = q_0 g + r_0 + f_1$, where $f_1 = -q_0(g - g_0)$, and $\|f_1\| \leq \frac{\|g-g_0\|}{\|g\|} \cdot \|f\|$.

Set $f_0 = f$. By induction we get, for each $k \geq 0$, elements $f_k, q_k \in A\{x\}$ and $r_k \in A[x]$ such that $\deg(r_k) < d$ and

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

It follows that $\|f_k\| \leq \left(\frac{\|g-g_0\|}{\|g\|}\right)^k \|f\|$, so $\|f_k\| \to 0$. Hence, also $\|q_k\|, \|r_k\| \to 0$. Therefore, $q = \sum_{k=0}^{\infty} q_k \in A\{x\}$ and $r = \sum_{k=0}^{\infty} r_k \in A[x]$. By construction, $f = \sum_{n=0}^{k} q_n g + \sum_{n=0}^{k} r_n + f_{k+1}$ for each k. Taking k to infinity, we get $f = qg + r$ and $\deg(r) < d$. ∎

Corollary 7.5 (Weierstrass preparation theorem): *Let $f \in A\{x\}$ be regular of pseudo degree d. Then $f = qg$, where q is a unit of $A\{x\}$ and $g \in A[x]$ is a monic polynomial of degree d with $\|g\| = 1$. Moreover, q and g are uniquely determined by these conditions.*

Proof: By Proposition 7.4 there are $q' \in A\{x\}$ and $r' \in A[x]$ of degree $< d$ such that $x^d = q'f + r'$ and $\|r'\| \leq \|x^d\| = 1$. Set $g = x^d - r'$. Then g is monic of degree d, $g = q'f$, and $\|g\| = 1$. It remains to show that $q' \in A\{x\}^\times$.

Note that g is regular of pseudo degree d. By Proposition 7.4, there are $q \in A\{x\}$ and $r \in A[x]$ such that $f = qg + r$ and $\deg(r) < d$. Thus, $f = qq'f + r$. Since $f = 1 \cdot f + 0$, the uniqueness part of Proposition 7.4 implies that $qq' = 1$. Hence, $q' \in A\{x\}^\times$.

Finally suppose $f = q_1 g_1$, where $q_1 \in A\{x\}^\times$ and $g_1 \in A[x]$ is monic of degree d with $\|g_1\| = 1$. Then $g_1 = (q_1^{-1} q) g + 0$ and $g_1 = 1 \cdot g + (g_1 - g)$, where $g_1 - g$ is a polynomial of degree at most $d - 1$. By the uniqueness part of Proposition 7.4, $q_1^{-1} q_2 = 1$, so $q_1 = q_2$ and $g_1 = g$. ∎

Corollary 7.6: *Let* $f = \sum_{n=0}^{\infty} a_n x^n$ *be a regular element of* $A\{x\}$ *such that* $\|a_0 b\| = \|a_0\| \cdot \|b\|$ *for each* $b \in A$*. Then* $f \in A\{x\}^\times$ *if and only if* $\text{pseudo.deg}(f) = 0$ *and* $a_0 \in A^\times$*.*

Proof: If there exists $g \in \sum_{n=0}^{\infty} b_n x^n$ in $A\{x\}$ such that $fg = 1$, then $\text{pseudo.deg}(f) + \text{pseudo.deg}(g) = 0$, so $\text{pseudo.deg}(f) = 0$. In addition, $a_0 b_0 = 1$, so $a_0 \in A^\times$.

Conversely, suppose $\text{pseudo.deg}(f) = 0$ and $a_0 \in A^\times$. Then f is regular. Hence, by Corollary 7.5, $f = q \cdot 1$ where $q \in A\{x\}^\times$. ∎

Corollary 7.7: *Let* K *be a complete field with respect to an absolute value* $|\ |$ *and let* $O = \{a \in K \mid |a| \le 1\}$ *be its valuation ring. Then* $K\{x\}$ *is a principal ideal domain, hence a unique factorization domain. Moreover, every ideal of* $K\{x\}$ *is generated by an element of* $O[x]$*.*

Proof: By the Weierstass preparation theorem (Corollary 7.5), every nonzero ideal $\mathfrak{a}$ of $K\{x\}$ is generated by the ideal $\mathfrak{a} \cap K[x]$ of $K[x]$. Since $K[x]$ is a principal ideal domain, $\mathfrak{a} \cap K[x] = fK[x]$ for some $f \in K[x]$. Consequenctky, $\mathfrak{a} = K\{x\}$ is a principal ideal. Moreover, dividing f by one of its coefficients with highest absolute value, we may assume that $f \in O[x]$. ∎

8. Convergent Power Series

Let K be a complete field with respect to an ultrametric absolute value $|\ |$. We say that a formal power series $f = \sum_{n=m}^{\infty} a_n x^n$ in $K((x))$ **converges** at an element $c \in K$, if $f(c) = \sum_{n=m}^{\infty} a_n c^n$ converges, i.e. $a_n c^n \to 0$. In this case f converges at each $b \in K$ with $|b| \le |c|$. For example, each $f \in K\{x\}$ converges at 1. We say that f **converges** if f converges at some $c \in K^\times$.

We denote the set of all convergent power series in $K((x))$ by $K((x))_0$ and prove that $K((x))_0$ is a field that contains $K\{x\}$ and is algebraically closed in $K((x))$.

Lemma 8.1: *A power series* $f = \sum_{n=m}^{\infty} a_n x^n$ *in* $K((x))$ *converges if and only if there exists a positive real number* γ *such that* $|a_n| \le \gamma^n$ *for each* $n \ge 0$*.*

Proof: First suppose f converges at $c \in K^\times$. Then $a_n c^n \to 0$, so there exists $n_0 \ge 1$

such that $|a_n c^n| \le 1$ for each $n \ge n_0$. Choose

$$\gamma = \max\{|c|^{-1}, |a_k|^{1/k} \mid k = 0, \dots, n_0 - 1\}.$$

Then $|a_n| \le \gamma^n$ for each $n \ge 0$.

Conversely, suppose $\gamma > 0$ and $|a_n| \le \gamma^n$ for all $n \ge 0$. Increase γ, if necessary, to assume that $\gamma > 1$. Then choose $c \in K^\times$ such that $|c| \le \gamma^{-1.5}$ and observe that $|a_n c^n| \le \gamma^{-0.5n}$ for each $n \ge 0$. Therefore, $a_n c^n \to 0$, hence f converges at c. ∎

LEMMA 8.2: *$K((x))_0$ is a field that contains $\mathrm{Quot}(K\{x\})$, hence also $K(x)$.*

Proof: The only difficulty is to prove that if $f = 1 + \sum_{n=1}^\infty a_n x^n$ converges, then also $f^{-1} = 1 + \sum_{n=1}^\infty a'_n x^n$ converges.

Indeed, for $n \ge 1$, a'_n satisfies the recursive relation $a'_n = -a_n - \sum_{i=1}^{n-1} a_i a'_{n-i}$. By Lemma 8.1, there exists $\gamma > 1$ such that $|a_i| \le \gamma^i$ for each $i \ge 1$. Set $a'_0 = 1$. Suppose, by induction, that $|a'_j| \le \gamma^j$ for $j = 1, \dots, n-1$. Then $|a'_n| \le \max_i(|a_i| \cdot |a'_{n-i}|) \le \gamma^n$. Hence, f^{-1} converges. ∎

Let v be the valuation of $K((x))$ defined by

$$v(\sum_{n=m}^\infty a_n x^n) = m \qquad \text{for } a_m, a_{m+1}, a_{m+2}, \ldots \in K \text{ with } a_m \ne 0.$$

It is discrete, complete, its valuation ring is $K[[x]]$, and $v(x) = 1$. The residue of an element $f = \sum_{n=0}^\infty a_n x^n$ of $K[[x]]$ at v is a_0, and we denote it by $\bar{f}$. We also consider the valuation ring $O = K[[x]] \cap K((x))_0$ of $K((x))_0$ and denote the restriction of v to $K((x))_0$ also by v. Since $K((x))_0$ contains $K(x)$, it is v-dense in $K((x))$. Finally, we also denote the unique extension of v to the algebraic closure of $K((x))$ by v.

Remark 8.3: $K((x))_0$ is not complete. Indeed, choose $a \in K$ such that $|a| > 1$. Then there exists no $\gamma > 0$ such that $|a^{n^2}| \le \gamma^n$ for all $n \ge 1$. By Lemma 8.1, the power series $f = \sum_{n=0}^\infty a^{n^2} x^n$ does not belong to $K((x))_0$. Therefore, the valued field $(K((x))_0, v)$ is not complete. ∎

LEMMA 8.4: *The field $K((x))_0$ is separably algebraically closed in $K((x))$.*

Proof: Let $y = \sum_{n=m}^\infty a_n x^n$, with $a_n \in K$, be an element of $K((x))$ which is separably algebraic of degree d over $K((x))_0$. We have to prove that $y \in K((x))_0$.

PART A: *A shift of y.* Assume that $d > 1$ and let $y_1, \ldots, y_d$, with $y = y_1$, be the (distinct) conjugates of y over $K((x))_0$. In particular $r = \max(v(y - y_i) \mid i = 2, \ldots, d)$ is an integer. Choose $s \geq r + 1$ and let

$$y_i' = \frac{1}{x^s}\big(y_i - \sum_{n=m}^{s} a_n x^n\big), \qquad i = 1, \ldots, d.$$

Then $y_1', \ldots, y_d'$ are the distinct conjugates of y_1' over $K((x))_0$. Also, $v(y_1') \geq 1$ and $y_i' = \frac{1}{x^s}(y_i - y) + y_1'$, so $v(y_i') \leq -1$, $i = 2, \ldots, d$. If y_1' belongs to $K((x))_0$, then so does y, and conversely. Therefore, we replace y_i by y_i', if necessary, to assume that

$$v(y) \geq 1 \text{ and } v(y_i) \leq -1,\ i = 2, \ldots, d. \tag{1}$$

In particular $y = \sum_{n=0}^{\infty} a_n x^n$ with $a_0 = 0$. The elements $y_1, \ldots, y_d$ are the roots of an irreducible separable polynomial

$$h(Y) = p_d Y^d + p_{d-1} Y^{d-1} + \cdots + p_1 Y + p_0$$

with coefficients $p_i \in O$. Let $e = \min(v(p_0), \ldots, v(p_d))$. Divide the p_i, if necessary, by x^e, to assume that $v(p_i) \geq 0$ for each i between 0 and d and that $v(p_j) = 0$ for at least one j between 0 and d.

PART B: *We prove that* $v(p_0), v(p_d) > 0,\ v(p_k) > v(p_1)$ *if* $2 \leq k \leq d-1$ *and* $v(p_1) = 0$. Indeed, since $v(y) > 0$ and $h(y) = 0$, we have $v(p_0) > 0$. Since $v(y_2) < 0$ and $h(y_2) = 0$, we have $v(p_d) > 0$. Next observe that

$$\frac{p_1}{p_d} = \pm y_2 \cdots y_d \pm \sum_{i=2}^{d} \frac{y_1 \cdots y_d}{y_i}.$$

If $2 \leq i \leq d$, then $v(y_i) < v(y_1)$, so $v(y_2 \cdots y_d) < v(\frac{y_1}{y_i}) + v(y_2 \cdots y_d) = v(\frac{y_1 \cdots y_d}{y_i})$. Hence,

$$v\Big(\frac{p_1}{p_d}\Big) = v(y_2 \cdots y_d). \tag{2}$$

For k between 1 and $d-2$ we have

$$\frac{p_{d-k}}{p_d} = \pm \sum_{\sigma} \prod_{i=1}^{k} y_{\sigma(i)}, \tag{3}$$

where σ ranges over all monotonically increasing maps from $\{1,\dots,k\}$ to $\{1,\dots,d\}$. If $\sigma(1)\neq 1$, then $\{y_{\sigma(1)},\dots,y_{\sigma(k)}\}$ is properly contained in $\{y_2,\dots,y_d\}$. Hence, $v(\prod_{i=1}^k y_{\sigma(i)}) > v(y_2\cdots y_d)$. If $\sigma(1)=1$, then

$$v\Big(\prod_{i=1}^k y_{\sigma(i)}\Big) > v\Big(\prod_{i=2}^k y_{\sigma(i)}\Big) > v(y_2\cdots y_d).$$

Hence, by (2) and (3), $v(\frac{p_{d-k}}{p_d}) > v(\frac{p_1}{p_d})$, so $v(p_{d-k}) > v(p_1)$. Since $v(p_j)=0$ for some j between 0 and d, since $v(p_i)\geq 0$ for every i between 0 and d, and since $v(p_0), v(p_d)>0$, we conclude that $v(p_1)=0$ and $v(p_i)>0$ for all $i\neq 1$. Therefore,

$$p_k=\sum_{n=0}^\infty b_{kn}x^n, \qquad k=0,\dots,d \tag{4}$$

with $b_{kn}\in K$ such that $b_{1,0}\neq 0$ and $b_{k,0}=0$ for each $k\neq 1$. In particular, $|b_{1,0}|\neq 0$ but unfortunately, $|b_{1,0}|$ may be smaller than 1.

Part C: *Making* $|b_{1,0}|$ *large.* We choose $c\in K$ such that $|c^{d-1}b_{1,0}|\geq 1$ and let $z=cy$. Then z is a zero of the polynomial $g(Z)=p_dZ^d+cp_{d-1}Z^{d-1}+\cdots+c^{d-1}p_1Z+c^dp_0$ with coefficients in O. Relation (4) remains valid except that the zero term of the coefficient of Z in g becomes $c^{d-1}b_{1,0}$. By the choice of c, its absolute value is at least 1. So, without loss, we may assume that

$$|b_{1,0}|\geq 1. \tag{5}$$

Part D: *An estimate for* $|a_n|$. By Lemma 8.1, there exists $\gamma>0$ such that $|b_{kn}|\leq\gamma^n$ for all $0\leq k\leq d$ and $n\geq 1$. By induction we prove that $|a_n|\leq\gamma^n$ for each $n\geq 0$. This will prove that $y\in O$ and will conclude the proof of the lemma.

Indeed, $|a_0|=0<1=\gamma^0$. Now assume that $|a_m|\leq\gamma^m$ for each $0\leq m\leq n-1$. For each k between 0 and d we have that $p_ky^k=\sum_{n=0}^\infty c_{kn}x^n$, where

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

and

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

It follows that

$$c_{0n} = b_{0n} \text{ and } c_{1n} = b_{1,0}a_n + b_{11}a_{n-1} + \cdots + b_{1,n-1}a_1. \tag{6}$$

For $k \geq 2$ we have $b_{k,0} = 0$. Hence, if a term $b_{k,\sigma(0)} \prod_{j=1}^k a_{\sigma(j)}$ in c_{kn} contains a_n, then $\sigma(0) = 0$, so $b_{k,\sigma(0)} = 0$. Thus,

$$c_{kn} = \text{sum of products of the form } b_{k,\sigma(0)} \prod_{j=1}^k a_{\sigma(j)}, \qquad \text{with } \sigma(j) < n,\ j = 1, \ldots, k. \tag{7}$$

From the relation $\sum_{k=0}^d p_k y^k = h(y) = 0$ we conclude that $\sum_{k=0}^d c_{kn} = 0$ for all n. Hence, by (6),

$$b_{1,0}a_n = -b_{0n} - b_{11}a_{n-1} - \cdots - b_{1,n-1}a_1 - c_{2n} - \cdots - c_{dn}.$$

Therefore, by (7),

$$\begin{gathered} b_{1,0}a_n = \text{sum of products of the form } -b_{k,\sigma(0)} \prod_{j=1}^k a_{\sigma(j)}, \\ \text{with } \sigma \in S_{kn},\ 0 \leq k \leq d, \text{ and } \sigma(j) < n,\ j = 1, \ldots, k. \end{gathered} \tag{8}$$

Note that $b_{k,0} = 0$ for each $k \neq 1$ (by (4)), while $b_{1,0}$ does not occur on the right hand side of (8). Hence, for a summand in the right hand side of (8) indexed by σ we have

$$|b_{k,\sigma(0)} \prod_{j=1}^k a_{\sigma(j)}| \leq \gamma^{\sum_{j=0}^k \sigma(j)} = \gamma^n.$$

We conclude from $|b_{1,0}| \geq 1$ that $|a_n| \leq \gamma^n$, as contended. ∎

PROPOSITION 8.5: *The field $K((x))_0$ is algebraically closed in $K((x))$. Thus, each $f \in K((x))$ which is algebraic over $K(x)$ converges at some $c \in K^\times$. Moreover, there exists a positive integer m such that f converges at each $b \in K^\times$ with $|b| \leq \frac{1}{m}$.*

Proof: In view of Lemma 8.4, we have to prove the proposition only for $\mathrm{char}(K) > 0$. Let $f = \sum_{n=m}^\infty a_n x^n \in K((x))$ be algebraic over $K((x))_0$. Then $K((x))_0(f)$ is a purely inseparable extension of a separable algebraic extension of $K((x))_0$. By Lemma 8.4, the latter coincides with $K((x))_0$. Hence, $K((x))_0(f)$ is a purely inseparable extension of $K((x))_0$.

Thus, there exists a power q of char(K) such that $\sum_{n=m}^{\infty} a_n^q x^{nq} = f^q \in K((x))_0$. By Lemma 8.1, there exists $\gamma > 0$ such that $|a_n^q| \le \gamma^{nq}$ for all $n \ge 1$. It follows that $|a_n| \le \gamma^n$ for all $n \ge 1$. By Lemma 8.1, $f \in K((x))_0$, so there exists $c \in K^\times$ such that f converges at c. If $\frac{1}{m} \le |c|$, then f converges at each $b \in K^\times$ with $|b| \le \frac{1}{m}$. ∎

9. Several Variables

Starting from a complete valued field $(K, |\ |)$, we choose an element $r \in K^\times$, a finite set I, and for each $i \in I$ an element $c_i \in K$ such that $|r| \le |c_i - c_j|$ if $i \ne j$. Then we set $w_i = \frac{r}{x - c_i}$, with an indeterminate x, and consider the ring $R = K\{w_i \mid i \in I\}$ of all series

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

with $a_0, a_{in} \in K$ such that for each i the element a_{in} tends to 0 as $n \to \infty$. The ring R is complete under the norm defined by $\|f\| = \max_{i,n}(|a_0|, |a_{in}|)$ (Lemma 11.1). We prove that R is a principal ideal domain (Proposition 11.9) and denote its quotient field by Q. More generally for each subset J of I, we denote the quotient field of $K\{w_i \mid i \in J\}$ by P_J. We deduce (Proposition 12.1) that $P_J \cap P_{J'} = P_{J \cap J'}$ if $J, J' \subseteq I$ have a nonempty intersection and $P_J \cap P_{J'} = K(x)$ if $J \cap J' = \emptyset$. Thus, setting $P_i = P_{I \smallsetminus \{i\}}$ for $i \in I$, we conclude that $\bigcap_{i \in I} P_i = K(x)$. The fields $E = K(x)$ and P_i are the first objects of patching data (Definition 4.1) that we start to assemble.

10. A Normed Subring of $K(x)$

Let $E = K(x)$ be the field of rational functions in the variable x over a field K. Let I be a finite set and r an element of $K^\times$. For each $i \in I$ let c_i be an element of K. Suppose $c_i \ne c_j$ if $i \ne j$. For each $i \in I$ let $w_i = \frac{r}{x - c_i} \in K(x)$. We consider the subring $R_0 = K[w_i \mid i \in I]$ of $K(x)$, prove that each of its elements is a linear combination of the powers w_i^n with coefficients in K, and define a norm on R_0.

Lemma 10.1:

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

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

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

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

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

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

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

(d) *Let $i \neq j$ be elements of I. Then $\frac{w_i}{w_j} = 1 + \frac{c_i - c_j}{r} w_i \in K[w_i]$ is invertible in $K[w_i, w_j]$.*

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

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

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

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

Proof of (d): Multiplying $\frac{r}{w_j} - \frac{r}{w_i} = c_i - c_j$ by $\frac{w_i}{r}$ we get that

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

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

Now we make an assumption for the rest of this chapter:

Assumption 10.2: The field K is complete with respect to a nontrivial ultrametric absolute value $| \ |$ and

$$|r| \le |c_i - c_j| \quad \text{for all } i \ne j. \tag{5}$$ □

Geometrically, Condition (5) means that the open disks $\{a \in K \mid |a - c_i| < r\}$, $i \in I$, of K are disjoint.

Let $E = K(x)$ be the field of rational functions over K in the variable x. We define a function $\| \ \|$ on $R_0 = K[w_i \mid i \in I]$ using the unique presentation (3):

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

Then $\|f\| \ge 0$ for each $f \in R_0$, $\|f\| = 0$ if and only if $f = 0$ (Lemma 10.1(c)), and $\|f + g\| \le \max(\|f\|, \|g\|)$ for all $f, g \in R_0$. Moreover, $\|w_i\| = 1$ for each $i \in I$ but $\|w_iw_j\| = \frac{|r|}{|c_i-c_j|}$ (by (4)) is less than 1 if $|r| < |c_i - c_j|$. Thus, $\| \ \|$ is in general not an absolute value. However, by (1) and (5)

$$\|w_iw_j^m\| \le \max_{1\le k\le m}\Big(\Big|\frac{r}{c_i - c_j}\Big|^m, \Big|\frac{r}{c_i - c_j}\Big|^{m+1-k}\Big) \le 1.$$

By induction, $\|w_i^kw_j^m\| \le 1$ for each k, so $\|fg\| \le \|f\| \cdot \|g\|$ for all $f, g \in R_0$. Moreover, if $a \in K$ and $f \in R_0$, then $\|af\| = \|a\|\|f\|$. Therefore, $\| \ \|$ is a norm on R_0 in the sense of Definition 6.1.

11. Mittag-Leffler Series

We keep the notation of Section 10 and Assumption 10.2 and proceed to define rings of convergent power series of several variables over K. In the language of rigid geometry, these are the rings of holomorphic functions on the complements of finitely many open discs of the projective line $\mathbb{P}^1(K)$.

Let $R = K\{w_i \mid i \in I\}$ be the completion of $R_0 = K[w_i \mid i \in I]$ with respect to $\| \ \|$ (Lemma 6.5). Our first result gives a Mittag-Leffler decomposition of each $f \in R$. It generalizes Lemma 10.1(c):

LEMMA 11.1: *Each element f of R has a unique presentation as a* **Mittag-Leffler series**

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

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

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

Proof: Each f as in (1) is the limit of the sequence $(f_d)_{d\geq 1}$ of its partial sums $f_d = a_0 + \sum_{i\in I}\sum_{n=1}^{d} a_{in} w_i^n \in R_0$, so $f \in R$. Since $\|f_d\| = \max_{i,n}(|a_0|, |a_{in}|)$ for each sufficiently large d, we have $\|f\| = \max_{i,n}(|a_0|, |a_{in}|)$. If $f = 0$ in (1), then $0 = \max_{i,n}(|a_0|, |a_{in}|)$, so $a_0 = a_{in} = 0$ for all i and n. It follows that the presentation (1) is unique.

On the other hand, let $g \in R$. Then there exists a sequence of elements $g_k = a_{k,0} + \sum_{i\in I}\sum_{n=1}^{\infty} a_{k,in} w_i^n$, $k = 1, 2, 3, \ldots$, in R_0, that converges to g. In particular, for each pair (k, i) we have $a_{k,in} = 0$ if n is sufficiently large. Also, the sequence $(g_k)_{k=1}^{\infty}$ is Cauchy. Hence, each of the sequences $\{a_{k,0} \mid k = 1, 2, 3, \ldots\}$ and $\{a_{k,in} \mid k = 1, 2, 3, \ldots\}$ is Cauchy. Since K is complete, $a_{k,0} \to a_0$ and $a_{k,in} \to a_{in}$ for some $a_0, a_{in} \in K$. 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 (1). Then $f \in R$ and $g_k \to f$ in R. Consequently, $g = f$. ∎

If $I = \emptyset$, then $R = R_0 = K$.

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

Remark 11.2: Let $i \in I$. Then $K\{w_i\} = \{\sum_{n=0}^{\infty} a_n w_i^n \mid a_n \to 0\}$ is a subring of R, the completion of $K[w_i]$ with respect to the norm. Consider the ring $K\{x\}$ of converging power series over K. By Lemma 7.1(d), there is a homomorphism $K\{x\} \to K\{w_i\}$ given by $\sum_{n=0}^{\infty} a_n x^n \mapsto \sum_{n=0}^{\infty} a_n w_i^n$. By Lemma 11.1, this is an isomorphism of normed rings. ∎

LEMMA 11.3: *Let $i, j \in I$ be distinct, let $p \in K[w_i] \subseteq R$ be a polynomial of degree $\leq d$ in w_i, and let $f \in K\{w_j\} \subseteq R$. Then $pf \in K\{w_i, w_j\}$ and the i-component of pf is a polynomial of degree $\leq d$ in w_i.*

Proof: Presenting p as the sum of its monomials we may assume that p is a power of w_i, say, $p = w_i^d$.

The assertion is obvious, if $d = 0$.

Let $d \geq 1$ and assume, by induction, that $w_i^{d-1} f = p' + f'$, where $p' \in K[w_i]$ is of degree $\leq d-1$ and $f' \in K\{w_j\}$. Then $w_i^d f = w_i p' + w_i f'$. Here $w_i p' \in K[w_i]$ is of degree $\leq d$ and the i-component of $w_i f'$ is, by (1) of Section 10, a polynomial of degree ≤ 1. Thus, the i-component of $w_i^d f$ is of degree $\leq d$. ∎

Remark 11.4: Let $(L, |\ |)$ be a complete valued field extending $(K, |\ |)$. Each $c \in L$ with $|c - c_i| \geq |r|$, for all $i \in I$, defines a continuous **evaluation homomorphism** $R \to L$ given by $f = a_0 + \sum_{i\in I}\sum_n a_{in} w_i^n \mapsto f(c) = a_0 + \sum_{i\in I}\sum_n a_{in}(\frac{r}{c-c_i})^n$. Indeed, $x \mapsto c$ defines a K-homomorphism $\varphi\colon K[x] \to L$. Let P be its kernel. Then φ extends to the localization $K[x]_P$. Since $\varphi(x - c_i) = c - c_i \neq 0$, we have $w_i \in K[x]_P$, for each $i \in I$. Thus, φ restricts to a homomorphism $R_0 \to L$, given by the above formula. Since $\left|\frac{r}{c-c_i}\right| \leq 1$ for each i, we have $|f(c)| \leq \|f\|$ for each $f \in R_0$. Hence, φ uniquely extends to a continuous homomorphism $\varphi\colon R \to L$. ∎

LEMMA 11.5 (Degree shifting): *Let $f \in R$ be given by (1). Fix $i \neq j$ in I. Let $\sum_{n=1}^\infty a'_{in} w_i^n$ be the i-component of $\frac{w_j}{w_i} f \in R$. Then*

$$a'_{in} = -\sum_{\nu=n+1}^\infty \frac{a_{i\nu} r^{\nu-n}}{(c_j - c_i)^{\nu-n}} \tag{2}$$

$$= \frac{-r}{c_j - c_i} \sum_{\nu=n+1}^\infty a_{i\nu}\Big(\frac{r}{c_j - c_i}\Big)^{\nu-(n+1)}, \quad n = 1, 2, 3, \ldots.$$

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

(a) *If $|a_{in}| \leq \varepsilon$ for each $n \geq d+1$, then $|b_{in}| \leq |\frac{r}{c_j - c_i}|^m \varepsilon$ for each $n \geq d+1-m$.*

(b) *Suppose $d > m$. If $|a_{in}| < \varepsilon$ for each $n \geq d+1$ and $|a_{id}| = \varepsilon$, then $|b_{in}| < |\frac{r}{c_j - c_i}|^m \varepsilon$ for each $n \geq d+1-m$ and $|b_{i,d-m}| = |\frac{r}{c_j - c_i}|^m \varepsilon$.*

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

Proof: By Lemma 10.1(d), $\frac{w_j}{w_i} \in R^\times$, so $(\frac{w_j}{w_i})^m f \in R$ for each m and the above statements make sense.

Proof of (2): We may assume that $a_0 = a_{i1} = 0$ and $a_{k\nu} = 0$ for each $k \neq i$ and each ν. Indeed, $\frac{w_j}{w_i} = 1 + (c_j - c_i)\frac{w_j}{r} \in K\{w_j\}$. Hence, $\frac{w_j}{w_i} \cdot w_k^\nu \in K\{w_l \mid l \neq i\}$. Furthermore, $\frac{w_j}{w_i} \cdot w_i = w_j \in K\{w_l \mid l \neq i\}$. Hence, by (1), 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 (1) of Section 10,

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

from which (2) 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 Condition (5) of Section 10, $|\frac{r}{c_i - c_j}| \le 1$. Hence, (a) follows from (2) with $n = d, d+1, d+2, \ldots$ and (b) follows from (2) 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 (2) that $a'_{i,n} = 0$ for all large n. Hence, $\sum_{n=1}^\infty a'_{in} w_i^n$ is a polynomial.

If $\sum_{n=1}^\infty a_{in} w_i^n$ is not a polynomial, then for each d_0 there exists $d > d_0$ such that $a_{id} \neq 0$. Since $|a_{in}| \to 0$ as $n \to \infty$, there are only finitely many $n \ge d$ with $|a_{in}| \ge |a_{id}|$. Replacing d with the largest of those n's, if necessary, we may assume that $|a_{in}| < |a_{id}|$ for each $n \ge d+1$. By (b), $a'_{i,d-1} \neq 0$. Consequently, $\sum_{n=1}^\infty a'_{in} w_i^n$ is not a polynomial. ∎

We apply degree shifting (albeit not yet Lemma 11.5) to generalize the Weierstrass preparation theorem (Corollary 7.5) to Mittag-Leffler series.

LEMMA 11.6: *Suppose $I \neq \emptyset$ and let $0 \neq f \in R$. Then there is an $l \in I$ such that $f = pu$ with $p \in K[w_l]$ and $u \in R^\times$.*

Proof: Write f in the form (1). Then, 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 $a_0 = 1$. Then $\|1 - f\| < 1$. By Lemma 6.3(f), $f \in R^\times$, so $p = 1$ and $u = f$ satisfy the claim of the lemma for each $l \in I$.

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 $A = K\{w_k \mid k \neq i\}$. This is a complete subring of R. We introduce a new variable z, and consider the ring $A\{z\}$ of convergent power series in z over A (Lemma 7.1(c)). Since $a_{id} \in K^\times \subseteq A^\times$, the element

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

of $A\{z\}$ is regular of pseudo degree d. By Corollary 7.5, 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 7.1(d), the evaluation homomorphism $\theta\colon A\{z\} \to R$ 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 $A[w_i]$. Replacing f by p and using Lemma 10.1, we may assume that $f \in A[w_i] = A + K[w_i]$ is a polynomial of degree d in w_i, that is,

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

If $I = \{i\}$, then $A[w_i] = K[w_i]$, and we are done. If $|I| \geq 2$, we choose a $j \in I$ distinct from i. By Lemma 10.1(d), $\frac{w_j}{w_i} = 1 + \frac{c_j - c_i}{r} w_j$ is invertible in R_0, hence in R. Since $\frac{w_j}{w_i} \in A$, we have $\frac{w_j}{w_i}(\sum_{k \neq i} \sum_{n=1}^{\infty} a_{kn} w_k^n) \in A$. In addition, by Lemma 10.1,

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

is a polynomial in $A[w_i]$ of degree $\le d-1$. Using induction on d, we may assume that $f \in A$. Finally, we apply the induction hypothesis (on $|I|$) to conclude the proof. ∎

Lemma 11.7: *Let $j \in I$. Then each $f \in R$ can be written as $f = pu$ with $p \in K[w_j]$, $\|p\| = 1$, and $u \in R^\times$.*

Proof: Lemma 11.6 gives a decomposition $f = p_1 u_1$ with $u_1 \in R^\times$ and $p_1 \in K[w_i]$ for some $i \in I$. If $i = j$, we set $p = p_1$ and $u = u_1$. If $i \ne j$, we may assume that $f \in K[w_i]$. Thus, $f = \sum_{n=0}^d a_n w_i^n$ with $a_d \ne 0$. By Lemma 10.1(d), $\frac{w_i}{w_j}$ is invertible in R_0, hence in R. Multiplying f by $\left(\frac{w_j}{w_i}\right)^d$ gives

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

Thus, $f = pu$ with $p \in K[w_j]$ and $u \in R^\times$. Finally, we may divide p by a coefficient with the highest absolute value to get that $\|p\| = 1$. ∎

Corollary 11.8: *Let $0 \ne g \in R$. Then $R_0 + gR = R$.*

Proof: Since $R = \sum_{i\in I} K\{w_i\}$ and $R_0 = K[w_i \mid i \in I] = \sum_{i \in I} K[w_i]$ (Lemma 10.1), it suffices to prove for each $i \in I$ and for every $f \in K\{w_i\}$ that there is $h \in K[w_i]$ such that $f - h \in gR$. By Lemma 11.7, we may assume that $g \in K[w_i]$. By Remark 11.2, there is a K-isomorphism $K\{z\} \to K\{w_i\}$ that maps $K[z]$ onto $K[w_i]$. Therefore the assertion follows from the Weierstrass Division Theorem (Proposition 7.4) for the ring $K\{z\}$. ∎

The next result generalizes Proposition 7.7 to Mittag-Leffler series.

Proposition 11.9: *The ring $R = K\{w_i \mid i \in I\}$ is a principal ideal domain, hence a unique factorization domain. Moreover, for each $i \in I$, each 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 $f_1, f_2 \in R$ with $f_1 f_2 = 0$. Choose an $i \in I$. By Lemma 11.7, $f_1 = p_1 u_1$ 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 $p_1 p_2 = f_1 f_2 (u_1 u_2)^{-1} = 0$, and hence either $p_1 = 0$ or $p_2 = 0$. Therefore, either $f_1 = 0$ or $f_2 = 0$. Consequently, R is an integral domain.

By Lemma 11.7, each ideal $\mathfrak{a}$ of R is generated by the ideal $\mathfrak{a} \cap K[w_i]$ of $K[w_i]$. Since $K[w_i]$ is a principal ideal domain, $\mathfrak{a} \cap K[w_i] = pK[w_i]$ for some $p \in K[w_i]$. Consequently, $\mathfrak{a} = pR$ is a principal ideal. ∎

12. Fields of Mittag-Leffler Series

In the notation of Sections 10 and 11 we consider for each nonempty subset J of I the integral domain $R_J = K\{w_i \mid i \in J\}$ (Proposition 11.9) and let $P_J = \mathrm{Quot}(R_J)$. For $J = \emptyset$, we set $P_J = K(x)$. All of these fields are contained in the field $Q = P_I$. The fields $P_i = P_{I \smallsetminus \{i\}}$, $i \in I$, will be our 'analytic' fields in the patching data over $E = K(x)$ that we start to assemble. As in Definition 4.1, the fields $P_i' = \bigcap_{j \neq i} P_j$ will be useful auxiliary fields.

PROPOSITION 12.1: *Let J and J' be subsets of I. Then $P_J \cap P_{J'} = P_{J \cap J'}$.*

Proof: If either $J = \emptyset$ or $J' = \emptyset$, then $P_J \cap P_{J'} = K(x)$, by definition. We therefore assume that $J, J' \neq \emptyset$. Let $j \in J$. Then $K[w_j] \subseteq R_J$, hence $K(x) = K(w_j) \subseteq P_J$. Similarly $K(x) \subseteq P_{J'}$. Hence $K(x) \subseteq P_J \cap P_{J'}$. If $J \cap J' \neq \emptyset$, then, by the unique representation for the elements of R appearing in (1) of Lemma 11.1, we have $R_{J \cap J'} = R_J \cap R_{J'}$, so $P_{J \cap J'} \subseteq P_J \cap P_{J'}$.

For the converse inclusion, let $0 \neq f \in P_J \cap P_{J'}$. Fix $j \in J$ and $j' \in J'$; if $J \cap J' \neq \emptyset$, take $j, j' \in J \cap J'$. Write f as f_1/g_1 with $f_1, g_1 \in R_J$. By Lemma 11.7, $g_1 = p_1 u_1$, where $0 \neq p_1 \in K[w_j]$ and $u_1 \in R_J^\times$. Replace f_1 by $f_1 u_1^{-1}$ to assume that $g_1 \in K[w_j]$. Similarly $f = f_2/g_2$ with $f_2 \in R_{J'}$ and $g_2 \in K[w_{j'}]$.

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

Now suppose $J \cap J' = \emptyset$. Let $g_1 = \sum_{n=0}^{d_1} b_n w_j^n$ with $b_n \in K$. Put $h_1 = (\frac{w_{j'}}{w_j})^{d_1} g_1$. Since $\frac{w_{j'}}{w_j} \in K[w_{j'}]$ (Lemma 10.1(d)), we have $h_1 = \sum_{n=0}^{d_1} b_n (\frac{w_{j'}}{w_j})^{d_1 - n} w_{j'}^n \in K[w_{j'}]$. Similarly there is an integer $d_2 \geq 0$ such that $h_2 = (\frac{w_j}{w_{j'}})^{d_2} g_2 \in K[w_j]$. Let $d = d_1 + d_2$. Then, for each $k \in J$

$$f_1 h_2 \cdot \left(\frac{w_{j'}}{w_k}\right)^d = f_2 h_1 \cdot \left(\frac{w_j}{w_k}\right)^d. \tag{1}$$

Note that $f_1h_2 \in R_J$ while $f_2h_1 \in R_{J'}$. In particular, the k-component of f_2h_1 is zero. By Lemma 11.5(c), the k-component of $f_2h_1 \cdot \big(\frac{w_j}{w_k}\big)^d$ is a polynomial in w_k. By (1), the k-component of $f_1h_2 \cdot \big(\frac{w_{j'}}{w_k}\big)^d$ is a polynomial in w_k. Hence, again by Lemma 11.5(c), the k-component of f_1h_2 is a polynomial in w_k.

We conclude that $f_1h_2 \in K[w_k \mid k \in J]$, so $f = \frac{f_1h_2}{g_1h_2} \in K(x)$. ∎

Corollary 12.2: *For each $i \in I$ we have $P_i' = P_{\{i\}}$. Also, $\bigcap_{j\in I} P_j = K(x)$.*

Proof: We apply Proposition 12.1 several times:

$$P_i' = \bigcap_{j\neq i} P_j = \bigcap_{j\neq i} P_{I\smallsetminus\{j\}} = P_{\bigcap_{j\neq i} I\smallsetminus\{j\}} = P_{\{i\}}.$$

For the second equality we choose an $i \in I$. Then

$$\bigcap_{j\in I} P_j = P_{I\smallsetminus\{i\}} \cap \bigcap_{j\neq i} P_{I\smallsetminus\{j\}} = P_{I\smallsetminus\{i\}} \cap P_{\{i\}} = K(x),$$

as claimed. ∎

13. Factorization of Matrices over Complete Rings

We show in this section how to decompose a matrix over a complete ring into a product of matrices over certain complete subrings. This will establish the decomposition condition in the definition of the patching data (Definition 4.1) in our setup.

Lemma 13.1: *Let $(M, \|\ \|)$ be a complete normed ring and let $0 < \varepsilon < 1$. Consider elements $a_1, a_2, a_3, \ldots \in M$ such that $\|a_i\| \le \varepsilon$ for each i and $\|a_i\| \to 0$. Let*

$$p_i = (1-a_1)\cdots(1-a_i), \qquad i = 1, 2, 3, \ldots \quad .$$

Then the sequence $(p_i)_{i=1}^\infty$ converges to an element of $M^\times$.

Proof: For each $i \ge 1$ we have $\|p_i\| \le \|1-a_1\|\cdots\|1-a_i\| \le 1$. Setting $p_0 = 1$, we also have $p_i = p_{i-1}(1-a_i)$. Hence,

$$\|p_i - p_{i-1}\| \le \|p_{i-1}\| \cdot \|a_i\| \le \|a_i\| \to 0.$$

Thus, $(p_i)_{i=1}^\infty$ is a Cauchy sequence, so it converges to some $p \in M$. Furthermore,

$$\|p_k - 1\| = \|\sum_{i=1}^k (p_i - p_{i-1})\| \le \max \|a_i\| \le \varepsilon.$$

Consequently, $\|p-1\| < 1$. By Lemma 6.3(f), $p \in M^\times$. ∎

Lemma 13.2 (Cartan's Lemma): *Let $(M, \| \ \|)$ be a complete normed ring. Let M_1 and M_2 be complete subrings of M. Suppose*

(1) *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 exist $b_1 \in M_1^\times$ and $b_2 \in M_2^\times$ such that $b = b_1 b_2$.

Proof: Let $a_1 = b - 1$ and $\varepsilon = \|a_1\|$. Then $0 \le \varepsilon < 1$. The condition

$$1 + a_{j+1} = (1 - a_j^+)(1 + a_j)(1 - a_j^-), \tag{2}$$

with a_j^+, a_j^- associated to a_j by (1), recursively defines a sequence $(a_j)_{j=1}^\infty$ in M. Use the relation $a_j = a_j^+ + a_j^-$ to rewrite (2):

$$a_{j+1} = a_j^+ a_j^- - a_j^+ a_j - a_j a_j^- + a_j^+ a_j a_j^-. \tag{3}$$

Inductively assume that $\|a_j\| \le \varepsilon^{2^{j-1}}$. Since $\|a_j^+\|, \|a_j^-\| \le \|a_j\|$, (3) implies that $\|a_{j+1}\| \le \max(\|a_j\|^2, \|a_j\|^3) = \|a_j\|^2 \le \varepsilon^{2^j}$. Therefore, $a_j \to 0$, $a_j^- \to 0$, and $a_j^+ \to 0$. Further, by (2),

$$1 + a_{j+1} = (1 - a_j^+) \cdots (1 - a_1^+) \ b \ (1 - a_1^-) \cdots (1 - a_j^-). \tag{4}$$

By Lemma 13.1, the partial products $(1 - a_1^-) \cdots (1 - a_j^-)$ converge to some $b_2' \in M_2^\times$. Similarly, the partial products $(1 - a_j^+) \cdots (1 - a_1^+)$ converge to some $b_1' \in M_1^\times$. Passing to the limit in (4), we get $1 = b_1' b b_2'$. Therefore, $b = (b_1')^{-1}(b_2')^{-1}$, as desired. ∎

Lemma 13.3: *Let A be a complete integral domain with respect to an absolute value $| \ |$, A_1, A_2 complete subrings of A, and A_0 a dense subring of A. Set $E_i = \mathrm{Quot}(A_i)$ for $i = 0, 1, 2$ and $E = \mathrm{Quot}(A)$. Suppose these objects satisfy the following conditions:*

(5a) *For each* $a \in A$ *there are* $a^+ \in A_1$ *and* $a^- \in A_2$ *with* $|a^+|, |a^-| \leq |a|$ *such that* $a = a^+ + a^-$.

(5b) $A = A_0 + gA$ *for each nonzero* $g \in A_0$.

(5c) *For every* $f \in A$ *there are* $p \in A_0$ *and* $u \in A^\times$ *such that* $f = pu$.

(5d) $E_0 \subseteq E_2$.

Then, for every positive integer n *and for each* $b \in \mathrm{GL}_n(E)$ *there are* $b_1 \in \mathrm{GL}_n(E_1)$ *and* $b_2 \in \mathrm{GL}_n(E_2)$ *such that* $b = b_1 b_2$.

Proof: As in Example 6.4(d), we define the norm of a matrix $a = (a_{ij}) \in \mathrm{M}_n(A)$ by $\|a\| = \max_{ij} |a_{ij}|$ and note that $\mathrm{M}_n(A)$ is a complete normed ring, $\mathrm{M}_n(A_1), \mathrm{M}_n(A_2)$ are complete normed subrings of $\mathrm{M}_n(A)$, and $\mathrm{M}_n(A_0)$ is a dense subring of $\mathrm{M}_n(A)$. Moreover, by (5a), for each $a \in \mathrm{M}_n(A)$ there are $a^+ \in \mathrm{M}_n(A_1)$ and $a^- \in \mathrm{M}_n(A_2)$ with $\|a^+\|, \|a^-\| \leq \|a\|$ such that $a = a^+ + a^-$.

By Condition (5c) each element of E is of the form $\frac{1}{h} f$, where $f \in A$ and $h \in A_0$, $h \neq 0$. Hence, there is $h \in A_0$ such that $hb \in \mathrm{M}_n(A)$ and $h \neq 0$. If $hb = b_1 b_2'$, where $b_1 \in \mathrm{GL}_n(E_1)$ and $b_2' \in \mathrm{GL}_n(E_2)$, then $b = b_1 b_2$ with $b_2 = \frac{1}{h} b_2' \in \mathrm{GL}_n(E_2)$. Thus, we may assume that $b \in \mathrm{M}_n(A)$.

Let $d \in A$ be the determinant of b. By Condition (5c) there are $g \in A_0$ and $u \in A^\times$ such that $d = gu$. Let $b'' \in \mathrm{M}_n(A)$ be the adjoint matrix of b, so that $bb'' = d \cdot 1$, where 1 is here the unit of $M_n(A)$. Let $b' = u^{-1} b''$. Then $b' \in \mathrm{M}_n(A)$ and $bb' = g \cdot 1$.

We set

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

Then V is an additive subgroup of $\mathrm{M}_n(A)$ and $g\mathrm{M}_n(A) \leq V$. By (5b), $\mathrm{M}_n(A) = \mathrm{M}_n(A_0) + g\mathrm{M}_n(A)$. Hence $V = V_0 + g\mathrm{M}_n(A)$. Since $\mathrm{M}_n(A_0)$ is dense in $\mathrm{M}_n(A)$, and therefore $g\mathrm{M}_n(A_0)$ is dense in $g\mathrm{M}_n(A)$, it follows that $V_0 = V_0 + g\mathrm{M}_n(A_0)$ is dense in $V = V_0 + g\mathrm{M}_n(A)$. Since $b' \in V$, there is $a_0 \in V_0$ such that $||b' - a_0|| < \frac{|g|}{||b||}$. In particular, $a_0 \in \mathrm{M}_n(A_0)$ and $ba_0 \in g\mathrm{M}_n(A)$.

Put $a = \frac{1}{g} a_0 \in \mathrm{M}_n(E_0)$. Then $ba \in \mathrm{M}_n(A)$ and $||1 - ba|| = ||\frac{1}{g} b(b' - a_0)|| \leq \frac{1}{|g|} ||b|| \cdot ||b' - a_0|| < 1$. It follows from Lemma 6.3(f) that $ba \in \mathrm{GL}_n(A)$. In particular

$\det(a) \neq 0$ and therefore $a \in \mathrm{GL}_n(E_0) \leq \mathrm{GL}(E_2)$. By Lemma 13.2, there are $b_1 \in \mathrm{GL}_n(A_1)$ and $b_2' \in \mathrm{GL}_n(A_2) \leq \mathrm{GL}_n(E_2)$ such that $ba = b_1 b_2'$. Thus $b = b_1 b_2$, where $b_1 \in \mathrm{GL}_n(A_1) \leq \mathrm{GL}_n(E_1)$ and $b_2 = b_2' a^{-1} \in \mathrm{GL}_n(E_2)$. ∎

We apply Corollary 13.3 to the rings and fields of Section 12.

COROLLARY 13.4: *Let $B \in \mathrm{GL}_n(Q)$.*

(a) *For each partition $I = J \cup J'$ there exist $B_1 \in \mathrm{GL}_n(P_J)$ and $B_2 \in \mathrm{GL}_n(P_{J'})$ such that $B = B_1 B_2$.*
(b) *For each $i \in I$ there exist $B_1 \in \mathrm{GL}_n(P_i)$ and $B_2 \in \mathrm{GL}_n(P_i')$ such that $B = B_1 B_2$.*

Proof: We may assume without loss that both J and J' are nonempty and apply Lemma 13.3 to the rings $R, R_J, R_{J'}, R_0$ rather than A, A_1, A_2, A_0, where $R_0 = K[w_i \mid i \in I]$.

By definition, R, R_J, and $R_{J'}$ are complete rings (Second paragraph of Section 11). Given $f \in R$, say, $f = a_0 + \sum_{i\in I}\sum_{k=1}^{\infty} a_{ik} w_i^k$ (Lemma 11.1), we let $f_1 = a_0 + \sum_{i\in J}\sum_{k=1}^{\infty} a_{ik} w_i^k$ and $f_2 = \sum_{i\in J'}\sum_{k=1}^{\infty} a_{ik} w_i^k$. Then $|f_i| \leq |f|$, $i = 1, 2$ and $f = f_1 + f_2$. This proves condition (5a) in our context.

By definition, R is the completion of R_0, so R_0 is dense in R and $K(x) = \mathrm{Quot}(R_0)$ is contained in both $P_J = \mathrm{Quot}(R_j)$ and $P_{J'} = \mathrm{Quot}(R_{J'})$. Conditions (5b) and (5c) are Corollary 11.8 and Lemma 11.7, respectively. Our Corollary is therefore a special case of Lemma 13.3. ∎

We apply Corollary 12.2 and Corollary 13.4 to put together patching data whose analytic fields are the fields P_i introduced above.

PROPOSITION 13.5: *Let K be a complete field with respect to an ultrametric absolute value $|\ |$. Let x be an indeterminate, G a finite group, r an element of $K^\times$, and I a finite set with $|I| \geq 2$. For each $i \in I$ let G_i be a subgroup of G, F_i a finite Galois extension of $E = K(x)$ with $\mathrm{Gal}(F_i/K) \cong G_i$, and $c_i \in K^\times$ such that $|r| \leq |c_i - c_j|$ if $i \neq j$. Set $w_i = \frac{r}{x - c_i}$, $P_i = \mathrm{Quot}(K\{w_j \mid j \in I \smallsetminus \{i\}\})$, $P_i' = \mathrm{Quot}(K\{w_i\})$, and $Q = \mathrm{Quot}(K\{w_i \mid i \in I\})$. Suppose $G = \langle G_i \mid i \in I\rangle$ and $F_i \subseteq P_i'$ for each $i \in I$. Then $\mathcal{E} = (E, F_i, P_i, Q, G_i, G)_{i\in I}$ is patching data.*

Proof: Our assumptions imply conditions (1a) and (1d) of Definition 4.1. By Corollary 12.2, $P'_i = P_{\{i\}} = \bigcap_{j\neq i} P_{I\smallsetminus\{j\}} = \bigcap_{j\neq i} P_j$ and $\bigcap_{i\in I} P_i = E$. Thus, Conditions (1b) and (1c) of Definition 4.1 hold. Finally, Condition (1e) of Definition 4.1 holds by Corollary 13.4. It follows that $\mathcal{E}$ is patching data. ∎

14. Cyclic Extensions

Every finite group is generated by cyclic groups whose orders are powers of prime numbers. Given a field K, a variable x, and a power q of a prime number, we construct a Galois extension F of $K(x)$ with $\mathrm{Gal}(F/K(x)) \cong \mathbb{Z}/n\mathbb{Z}$. If in addition K is complete with respect to a non-archimedean norm, we show how to embed F into $K\{x\}$.

LEMMA 14.1: *Let K be a field, n a positive integer with $\mathrm{char}(K)\nmid n$, and x a variable. Then $K(x)$ has a cyclic extension F of degree n which is contained in $K((x))$.*

Proof: Choose a root of unity ζ_n of order n in K_s. Let $L = K(\zeta_n)$ and $G = \mathrm{Gal}(L/K)$. Then there is a map $\chi\colon G \to \{1,\ldots,n-1\}$ such that $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$. Then $\gcd(\chi(\sigma), n) = 1$ and

$$\chi(\sigma\tau) \equiv \chi(\sigma)\chi(\tau) \mod n \tag{1}$$

for all $\sigma,\tau \in G$. By Example 3.5.1, $K((x))$ is a regular extension of K and $L((x)) = K((x))(\zeta_n)$. Thus, we may identify G with $\mathrm{Gal}(L((x))/K((x)))$.

Choose a primitive element c of L/K. Consider the element

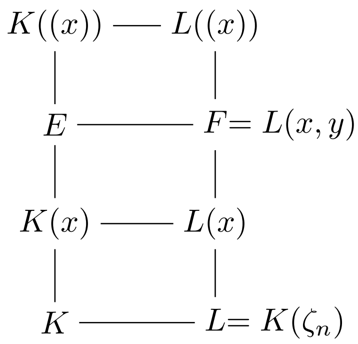
$$g(x) = \prod_{\sigma\in G} \big(1+\sigma(c)x\big)^{\chi(\sigma^{-1})}$$

of $L[x]$. Since $\mathrm{char}(K)\nmid n$, Hensel's lemma (Proposition 3.5.2) gives a $z \in L[[x]]$ with $z^n = 1+cx$. Then $y = \prod_{\sigma\in G}\sigma(z)^{\chi(\sigma^{-1})} \in L[[x]]$ and $y^n = \prod_{\sigma\in G}\sigma(z^n)^{\chi(\sigma^{-1})} = \prod_{\sigma\in G}(1+\sigma(c)x)^{\chi(\sigma^{-1})} = g(x)$. Since $\zeta_n \in L$, $F = L(x,y)$ is a cyclic extension of degree d of $L(x)$, where $d|n$ and $y^d \in L(x)$ [Lang7, p. 289, Thm. 6.2(ii)]. Since $\chi(\sigma^{-1})$ is relatively prime to n, we must have $d = n$. The Galois group $\mathrm{Gal}(F/L(x))$ is generated by an element ω satisfying $\omega(y) = \zeta_n y$.

By (1) there exist for each $\tau, \rho \in G$ a positive integer $k(\tau, \rho)$ and a polynomial $f_\tau(x) \in L[x]$ such that

$$\tau(y) = \prod_{\sigma \in G} \tau\sigma(z)^{\chi(\sigma^{-1})} = \prod_{\rho \in G} \rho(z)^{\chi(\rho^{-1}\tau)} = \prod_{\rho \in G} \rho(z)^{\chi(\rho^{-1})\chi(\tau) + k(\tau,\rho)n}$$
$$= y^{\chi(\tau)} \prod_{\rho \in G} (1 + \rho(c)x)^{k(\tau,\rho)} = y^{\chi(\tau)} f_\tau(x).$$

It follows that G leaves F invariant. Let E be the fixed field of G in F.



Denote the subgroup of $\mathrm{Aut}(F/K(x))$ generated by G and $\mathrm{Gal}(F/L(x))$ by H. Then the fixed field of H is $K(x)$, so $F/K(x)$ is a Galois extension with $\mathrm{Gal}(F/K(x)) = G \cdot \mathrm{Gal}(F/L(x))$. Moreover, given $\tau \in G$, put $m = \chi(\tau)$. Then $\tau\omega(y) = \tau(\zeta_n y) = \zeta_n^m y^m f_\tau(x) = \omega(y)^m f_\tau(x) = \omega(y^m f_\tau(x)) = \omega\tau(y)$. Thus, $\tau\omega = \omega\tau$, so G commutes with $\mathrm{Gal}(F/L(x))$. Therefore, $E/K(x)$ is a Galois extension with $\mathrm{Gal}(E/K(x)) \cong \mathrm{Gal}(F/L(x)) \cong \mathbb{Z}/n\mathbb{Z}$. ∎

Lemma 14.2: *Let E be a field of positive characteristic p. Let F be a cyclic extension of degree p^n, $n \geq 1$, of E. Then E has a $\mathbb{Z}/p^{n+1}\mathbb{Z}$-extension F' which contains F.*

Proof: Define F' to be $F(z)$ where z is a zero of $Z^p - Z - a$ with $a \in F$. The three parts of the proof produce a, and then show F' has the desired properties.

Part A: *Construction of a.* Since F/E is separable, there is a $b_1 \in F$ with $c = \mathrm{trace}_{F/E}(b_1) \neq 0$ [Lang7, p. 286, Thm. 5.2]. Put $b = \frac{b_1}{c}$. Then $\mathrm{trace}_{F/E}(b) = 1$ and $\mathrm{trace}_{F/E}(b^p - b) = (\mathrm{trace}_{F/E}(b))^p - \mathrm{trace}_{F/E}(b) = 0$. With σ a generator of $\mathrm{Gal}(F/E)$, the additive form of Hilbert's Theorem 90 [Lang7, p. 290, Thm. 6.3] gives $a \in F$ with

$$\sigma a - a = b^p - b. \tag{2}$$

PART B: *Irreducibility of $Z^p - Z - a$.* Assume $Z^p - Z - a$ is reducible over F. Then $z \in F$ [Lang7, p. 290, Thm. 6.4(b)]. Thus

$$(3) \qquad (\sigma z - z)^p - (\sigma z - z) - (b^p - b) = (\sigma z - z)^p - (\sigma z - z) - (\sigma a - a)$$
$$= (\sigma z^p - \sigma z - \sigma a) - (z^p - z - a) = 0$$

Since b is a root of $Z^p - Z - (b^p - b)$, there is an i with $\sigma z - z = b + i$ [Lang7, p. 290, Thm. 6.4(b)]. Apply $\mathrm{trace}_{F/E}$ to both sides to get 0 on the left and 1 on the right. This contradiction proves $Z^p - Z - a$ is irreducible.

PART C: *Extension of σ to σ' that maps z to $z + b$.* Equality (2) implies $z + b$ is a zero of $Z^p - Z - \sigma a$. Thus, by Part B, σ extends to an automorphism σ' of F' with $\sigma'(z) = z + b$. We need only prove that σ' has order p^{n+1}. Induction shows $(\sigma')^j(z) = z + b + \sigma b + \cdots + \sigma^{j-1} b$. In particular,

$$(4) \qquad (\sigma')^{p^n}(z) = z + \mathrm{trace}_{F/E}(b) = z + 1.$$

Hence, $(\sigma')^{ip^n}(z) = z + i$, $i = 1, \ldots, p$. Therefore, the order of σ' is p^{n+1}, as contended. ∎

LEMMA 14.3: *Let K be a field, x a variable, and A a finite abelian group. Then $K(x)$ has a Galois extension F such that $\mathrm{Gal}(F/K(x)) \cong A$ and F/K is regular.*

Proof: We put $p = \mathrm{char}(K)$ and divide the proof into two parts:

PART A: *$A \cong \mathbb{Z}/m\mathbb{Z}$ and $p \nmid m$.* By Lemma 16.3.1, $K(x)$ has a cyclic extension E_m of degree m which is contained in $K((x))$. By Example 3.5.1, $K((x))$ is a regular extension of K. Hence, so is E_m (Corollary 2.6.5(b)).

PART B: *$A \cong \mathbb{Z}/p^k\mathbb{Z}$.* Assume without loss that $k \geq 1$. By Eisenstein's criterion and Gauss' lemma, the polynomial $Z^p - Z - x$ is irreducible over $\tilde{K}(x)$. Let z be a root of $Z^p - Z - x$ in $K(x)_s$. Then, by Artin-Schreier, [Lang7, p. 290, Thm. 6.4(b)], $K(z)$ is a cyclic extension of degree p of $K(x)$. Lemma 16.3.2 gives a cyclic extension E_{p^k} of $K(x)$ of degree p^k which contains $K(z)$.

By the preceding paragraph, $K(z) \cap \tilde{K}(x) = K(x)$. Since $\mathrm{Gal}(E_{p^k}/K(x))$ is a cyclic group of order p^k, each subextension of E_{p^k} which properly contains $K(x)$ must contain $K(z)$. Hence, $E_{p^k} \cap \tilde{K}(x) = K(x)$. Thus, E_{p^k} is linearly disjoint from $\tilde{K}(x)$ over $K(x)$. By the tower property (Lemma 2.5.3), E_{p^k} is linearly disjoint from $\tilde{K}$ over K; that is, E_{p^k}/K is regular.

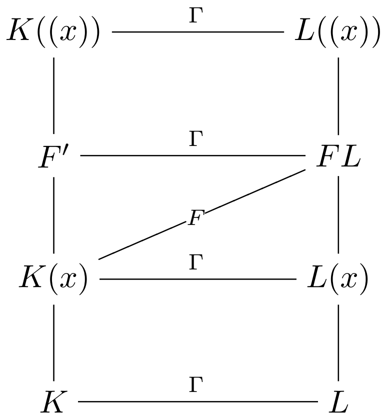
PART C: *$A \cong \mathbb{Z}/n\mathbb{Z}$, $n = mp^k$, $p \nmid m$.* The compositum $E_n = E_m E_{p^k}$ is a cyclic extension of $K(x)$ of degree n. Moreover, $E_n \cap \tilde{K}(x)$ decomposes into a cyclic extension of $K(x)$ of degree which divides m and a cyclic extension of $K(x)$ degree dividing p^k. By Parts A and B, both subextensions must be $K(x)$. It follows that E_n is a regular extension of K. ∎

The following result, due to Helmut Völklein, improves Lemma 14.3. Its proof applies the field crossing argument.

LEMMA 14.4: *Let K be an infinite field, x a variable, and A a finite abelian group. Then $K(x)$ has a finite Galois extension in $K((x))$ with Galois group isomorphic to A.*

Proof: Lemma 14.3 gives a Galois extension F of $K(x)$ such that $\mathrm{Gal}(F/K(x)) \cong A$ and F/K is regular. We choose a primitive element y for $F/K(x)$ integral over $K[x]$ and let $g = \mathrm{irr}(y, K(x))$. Then $g(Y) = f(X, Y)$, where $f \in K[X, Y]$ is irreducible. Since F/K is regular, f is absolutely irreducible. Replacing x by $x - a$ for an appropriate $a \in K$, we may assume that $f(0, Y)$ is separable. Let L be the splitting field of $f(0, Y)$ over K. By Hensel's lemma, $g(Y)$ has a root y' in $L((x))$. Since $F/K(x)$ is Galois, $F = K(x, y') \subseteq L((x))$. Hence FL is a Galois extension of $K(x)$ in $L((x))$. Since F, as a regular extension of K, is linearly disjoint from L over K, we have $\mathrm{Gal}(FL/K(x)) = \mathrm{Gal}(FL/F) \times \mathrm{Gal}(FL/L(x)$. Morover, $\mathrm{Gal}(FL/L(x))$ is isomorphic via restriction to $\mathrm{Gal}(F/K(x)) \cong A$, hence $\mathrm{Gal}(FL/L(x))$ is abelian. It follows that $\mathrm{Gal}(FL/L(x))$ lies in the center of $\mathrm{Gal}(FL/K(x))$.

The action of $\Gamma = \mathrm{Gal}(L/K)$ on the coefficients of the power series belonging to $L((x))$ extends to a faithful action of Γ on $L((x))$ with fixed field $K((x))$. Since F is a Galois extension of $K(x)$ in $L((x))$, it is invariant under Γ. Hence, the action of Γ on $L((x))$ restricts to an action of Γ on FL fixing each element of $K(x)$. We denote the fixed field of Γ in FL by F'.



It follows that $F' \cap L(x) = K(x)$ and $F' \cdot L(x) = FL$. Hence, $\Gamma \cdot \mathrm{Gal}(FL/L(x)) = \mathrm{Gal}(FL/K(x))$. Since, by the preceding paragraph, $\mathrm{Gal}(FL/L(x))$ lies in the center of $\mathrm{Gal}(FL/K(x))$, we conclude that $\mathrm{Gal}(FL/F')$ is a normal subgroup of $\mathrm{Gal}(FL/K(x))$. Therefore, F' is a Galois extension of $K(x)$ and $\mathrm{Gal}(F'/K(x)) \cong \mathrm{Gal}(FL/L(x)) \cong \mathrm{Gal}(F/K(x)) \cong A$, as desired. ∎

We can do even better, if K is a complete field under an absolute value $|\ |$.

LEMMA 14.5: *Let K be a complete field under an absolute value $|\ |$, let x be a variable, and let A be a finite abelian group. Then $K(x)$ has a Galois extension in $K\{x\}$ with Galois group A.*

Proof: By Lemma 14.4, $K(x)$ has a Galois extension F in $K((x))$ with Galois group isomorphic to A. We choose a primitive element y for $F/K(x)$ integral over $K[x]$. Then $y \in K[[x]]$, so $y = \sum_{n=0}^{\infty} a_n x^n$ with $a_n \in K$ for each $n \geq 0$. By Proposition 8.5, y converges at some $c \in K^{\times}$. Thus, the series $\sum_{n=0}^{\infty} a_n c^n$ converges in K, which means that $y' = \sum_{n=0}^{\infty} a_n c^n x^n \in K\{x\}$. Now, the map $x \to cx$ extends to an automorphism φ of $K((x))$ that leaves $K(x)$ invariant. It maps $K(x,y)$ onto the subfield $K(x,y')$ of $K\{x\}$. Since $K(x,y)/K$ is Galois with Galois group A, so is the extension $K(x,y')/K$, as desired. ∎

15. Embedding Problems over Complete Fields

Let K/K_0 be a finite Galois extension of fields with Galois group Γ acting on a finite group G. Consider a variable x and set $E_0 = K_0(x)$ and $E = K(x)$. Then E/E_0 is a

Galois extension and we identify $\mathrm{Gal}(E/E_0)$ with $\Gamma = \mathrm{Gal}(K/K_0)$ via restriction. We refer to

$$(1) \qquad \mathrm{pr}\colon \Gamma \ltimes G \to \Gamma$$

as a **constant finite split embedding problem over** E_0. We prove that if K_0 is complete under an ultrametric absolute value, then (1) has a solution field (Section 5) equipped with a K-rational place.

PROPOSITION 15.1: *Let K_0 be a complete field with respect to an ultrametric absolute value $|\;|$. Let K/K_0 be a finite Galois extension with Galois group Γ acting on a finite group G from the right. Then E has a Galois extension F such that*

(3a) *F/E_0 is Galois;*

(3b) *there is an isomorphism $\psi\colon \mathrm{Gal}(F/E_0) \to \Gamma \ltimes G$ such that $\mathrm{pr} \circ \psi = \mathrm{res}_E$; and*

(3c) *F has a set of cardinality $|K_0|$ of K-rational place φ (so F/K is regular) such that $\varphi(x) \in K_0$ and $\bar{F}_\varphi = K$.*

Proof: Our strategy is to attach patching data $\mathcal{E}$ to the embedding problem and to define a proper action of Γ on $\mathcal{E}$. Then we apply Proposition 5.2 to conclude that the compound F of $\mathcal{E}$ gives a solution to the embedding problem.

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

(4a) $\{\gamma \in \Gamma \mid i^\gamma = i\} = \{1\}$;

(4b) the order of the group $G_i = \langle \tau_i \rangle$ is a power of a prime number;

(4c) $\tau_i^\gamma = \tau_{i^\gamma}$, for every $\gamma \in \Gamma$; and

(4d) $|I| \geq 2$.

(E.g. assuming $G \neq 1$, let G_0 be the set of all elements of G whose order is a power of a prime number and note that Γ leaves G_0 invariant. Let $I = G_0 \times \Gamma$ and for each $(\sigma, \gamma) \in I$ and $\gamma' \in \Gamma$ let $(\sigma, \gamma)^{\gamma'} = (\sigma, \gamma\gamma')$ and $\tau_{(\sigma,\gamma)} = \sigma^\gamma$.)

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

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

Indeed, it suffices to find $\{c_j \mid j \in J\} \subseteq K$ (and then define c_i, for $i = j^\gamma \in I$, as c_j^γ) such that $c_j^\delta \neq c_j^\varepsilon$ for all $j \in J$ and all distinct $\delta, \varepsilon \in \Gamma$, and $c_j^\delta \neq c_k$ for all distinct $j, k \in J$ and all $\delta \in \Gamma$.

The first condition says that c_j is a primitive element for K/K_0; the second condition means that distinct c_j and c_k are not conjugate over K_0. Thus it suffices to show that there are infinitely many primitive elements for K/K_0. But if $c \in K^\times$ is primitive, then so is $c + a$, for each $a \in K_0$. Since K_0 is complete, hence infinite, the claim follows.

Construction B: *Patching data.*

We choose $r \in K_0^\times$ such that $|r| \leq |c_i - c_j|$ for all distinct $i, j \in I$. For each $i \in I$ we set $w_i = \frac{r}{x - c_i} \in K(x)$. As in Section 11, we consider the ring $R = K\{w_i \mid i \in I\}$ and let $Q = \mathrm{Quot}(R)$. For each $i \in I$ let

$$P_i = P_{I \smallsetminus \{i\}} = \mathrm{Quot}(K\{w_j \mid j \neq i\}) \quad \text{and} \quad P_i' = P_{\{i\}} = \mathrm{Quot}(K\{w_i\})$$

(we use the notation of Section 12).

Let $\gamma \in \Gamma$. By our definition, $w_i^\gamma = \frac{r}{x - c_i^\gamma} = w_{i^\gamma}$, $i \in I$. Hence, γ leaves $R_0 = K[w_i \mid i \in I]$ invariant. Since $|\ |$ is complete on K_0, it has a unique extension to K, so $|a^\gamma| = |a|$ for each $a \in K$. Moreover, for each $f = a_0 + \sum_{i \in I} \sum_{n=1}^\infty a_{in} w_i^n \in R_0$, we have

$$f^\gamma = a_0^\gamma + \sum_{i \in I} \sum_{n=1}^\infty a_{in}^\gamma (w_i^\gamma)^n \tag{5}$$

and

$$\begin{aligned} \|f^\gamma\| &= \|a_0^\gamma + \sum_{i \in I} \sum_{n=1}^\infty a_{in}^\gamma (w_i^\gamma)^n\| = \|a_0^\gamma + \sum_{i \in I} \sum_{n=1}^\infty a_{in}^\gamma w_{i^\gamma}^n\| \\ &= \max(|a_0^\gamma|, |a_{in}^\gamma|)_{i,n} = \max(|a_0|, |a_{in}|)_{i,n} = \|f\|. \end{aligned}$$

By Lemma 6.5, γ uniquely extends to a continuous automorphism of the completion R of R_0, by formula (5) for $f \in R$. Hence, Γ lifts to a group of continuous automorphisms of R. Therefore, Γ extends to a group of automorphisms of $Q = \mathrm{Quot}(R)$. In addition, $P_i^\gamma = P_{i^\gamma}$ and $(P_i')^\gamma = P_{i^\gamma}'$.

For each $j \in J$, Lemma 14.5 gives a cyclic extension F_j of E in $P'_j = K\{w_j\}$ with Galois group $G_j = \langle \tau_j \rangle$.

For an arbitrary $i \in I$ there exist unique $j \in J$ and $\gamma \in \Gamma$ such that $i = j^\gamma$ (by (4a)). Since γ acts on Q and leaves E invariant, $F_i = F_j^\gamma$ is a Galois extension of E in Q in P'_i.

The isomorphism $\gamma\colon F_j \to F_i$ gives an isomorphism

$$\mathrm{Gal}(F_j/E) \cong \mathrm{Gal}(F_i/E)$$

that maps each $\tau \in \mathrm{Gal}(F_j/E)$ onto $\gamma^{-1} \circ \tau \circ \gamma \in \mathrm{Gal}(F_i/E)$ (notice that the elements of the Galois groups act from the right). In particular, it maps τ_j onto $\gamma^{-1} \circ \tau_j \circ \gamma$. We can therefore identify G_i with $\mathrm{Gal}(F_i/E)$ such that τ_i coincides with $\gamma^{-1} \circ \tau_j \circ \gamma$. This means that $(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma}$ for all $a \in F_j$ and $\tau \in G_j$. In particular, $F_i \subseteq P'_i$ for each $i \in I$. It follows from Proposition 13.5 that $\mathcal{E} = (E, F_i, P_i, Q; G_i, G)_{i \in I}$ is patching data. By construction, Γ acts properly on $\mathcal{E}$ (Definition 5.1). By Propositions 4.5 and 5.2, the compound F of $\mathcal{E}$ satisfies (3a) and (3b). Now we verify (3c).

Claim C: *F/K has many prime divisor of degree 1.* Each $b \in K_0$ with

$$(6) \qquad |b| > \max_{i \in I}(|r|, |c_i|)$$

satisfies $\left|\frac{r}{b - c_i}\right| < 1$ for each $i \in I$, hence, the map $x \mapsto b$ extends to a homomorphism from R to K that maps w_i onto $\frac{r}{b - c_i}$. Since R is a principal ideal domain (Proposition 11.9), this homomorphism extends to a K-rational place $\varphi_b\colon Q \to K \cup \{\infty\}$. Thus, $\varphi_b|_F$ is a K-rational place of F with $\varphi_b(x) = b \in K_0$, so it corresponds to a prime divisor of F/K of degree 1. If $b' \in K_0$ and $b' \neq b$, then $\varphi_b \neq \varphi_{b'}$, so also the prime divisors that φ_b and $\varphi_{b'}$ define are distinct. Consequently, the cardinality of the prime divisors of F/K of degree 1 is that of K_0.

Finally, the regularity of F/K follows from the fact that $\varphi_b(F) = K \cup \{\infty\}$ [FrJ08, Lemma 2.6.9]. ∎

16. Embedding Problems over Ample Fields

In this section K/K_0 is an arbitrary finite Galois extension with Galois group Γ and x is a variable. Suppose Γ acts on a finite group G. We look for a rational solution of the constant split embedding problem

$$\text{pr: Gal}(K(x)/K_0(x)) \ltimes G \to \text{Gal}(K(x)/K_0(x)) \tag{1}$$

over $K_0(x)$. When K_0 is complete under an ultrametric absolute value, this problem reduces to the special case solved in Section .

Consider also a regular extension $\hat{K}_0$ of K_0 such that x is transcendental over $\hat{K}_0$ and let $\hat{K} = K\hat{K}_0$. Then $\hat{K}_0(x)$ is a regular extension of $K_0(x)$ [FrJ08, Lemma 2.6.8(a)], so $\hat{K}_0(x)$ is linearly disjoint from $K(x)$ over $K_0(x)$. Hence, res: $\text{Gal}(\hat{K}(x)/\hat{K}_0(x)) \to \text{Gal}(K(x)/K_0(x))$ is an isomorphism. This gives rise to a finite split embedding problem over $\hat{K}_0(x)$,

$$\text{pr: Gal}(\hat{K}(x)/\hat{K}_0(x)) \ltimes G \to \text{Gal}(\hat{K}(x)/\hat{K}_0(x)) \tag{2}$$

such that $\text{pr} \circ (\text{res}_{K(x)} \times \text{id}_G) = \text{res}_{K(x)} \circ \text{pr}$.

We identify each of the groups $\text{Gal}(\hat{K}(x)/\hat{K}_0(x))$, $\text{Gal}(K(x)/K_0(x))$, and $\text{Gal}(\hat{K}/\hat{K}_0)$ with $\Gamma = \text{Gal}(K/K_0)$ via restriction. Moreover, if F (resp. $\hat{F}$) is a solution field of embedding problem (1) (resp. (2)), then we identify $\text{Gal}(F/K_0(x))$ (resp. $\text{Gal}(\hat{F}/\hat{K}_0(x))$) with $\Gamma \ltimes G$ via an isomorphism θ (resp. $\hat{\theta}$) satisfying $\text{pr} \circ \theta = \text{res}$ (resp. $\text{pr} \circ \hat{\theta} = \text{res}$). We say that (F, θ) is a **split rational solution** of (1) if F has a K-rational place φ such that $\Gamma = D_\varphi$. We say that (F, θ) is **unramified** if φ can be chosen to be unramified over $K_0(x)$.

LEMMA 16.1: *In the above notation suppose K_0 is ample and existentially closed in $\hat{K}_0$. Let $\hat{F}$ be a solution field to embedding problem (2) with a $\hat{K}$-rational place $\hat{\varphi}$, unramified over $\hat{K}_0(x)$, such that $\hat{\varphi}(x) \in \hat{K}_0$. Then embedding problem (1) has a solution field F with a K-rational place φ unramified over $K_0(x)$ such that $\varphi(x) \in K_0$.*

Proof: We break up the proof into several parts. First we solve embedding problem (1) over $\hat{K}_0(x)$, then we push the solution down to a solution over a function field $K_0(\mathbf{u}, x)$

which is regular over K_0, and finally we specialize the latter solution to a solution over $K_0(x)$ with a place satisfying all of the prescribed conditions.

PART A: *A solution of (1) over $\hat{K}_0(x)$.* By assumption, there exists an isomorphism

$$\hat{\theta}\colon \mathrm{Gal}(\hat{F}/\hat{K}_0(x)) \to \mathrm{Gal}(\hat{K}(x)/\hat{K}_0(x)) \ltimes G$$

such that $\mathrm{pr}\circ\hat{\theta} = \mathrm{res}_{\hat{K}(x)}$. Let $\hat{F}_0$ be the fixed field in $\hat{F}$ of $D_{\hat{\varphi}}$ $(= \Gamma)$. Then, $\hat{F}_0 \cap \hat{K}(x) = \hat{K}_0(x)$ and $\hat{F}_0 \cdot \hat{K}(x) = \hat{F}$, so $m = [\hat{F}_0 : \hat{K}_0(x)] = [\hat{F} : \hat{K}(x)]$. Then, $\hat{\varphi}(\hat{F}_0) = \hat{K}_0 \cup \{\infty\}$. Hence, $\hat{F}_0/\hat{K}_0$ is regular [FrJ08, Lemma 2.6.9(b)].

We choose a primitive element y for the extension $\hat{F}_0/\hat{K}_0(x)$ integral over $\hat{K}_0[x]$. By the preceding paragraph, $\hat{F} = \hat{K}(x, y)$.

By [Jar11, Lemma 5.1.2], there exists an absolutely irreducible polynomial $h \in \hat{K}_0[V, W]$ and elements $v, w \in \hat{F}_0$ such that $\hat{K}_0(v, w) = \hat{F}_0$, $h(v, w) = 0$, $h(0, 0) = 0$, and $\frac{\partial h}{\partial W}(0, 0) \neq 0$.

We also choose a primitive element c for K over K_0, a primitive element z for $\hat{F}$ over $\hat{K}_0(x)$ integral over $\hat{K}_0[x]$, and note that $\hat{F} = \hat{K}_0(c, x, y)$. Then there exist polynomials $f, p_0, p_1 \in \hat{K}_0[X, Z]$, $g, r_0, r_1, r_2 \in \hat{K}_0[X, Y]$, $q_0, q_1 \in \hat{K}_0[T, X, Y]$, and $s_0, s_1, s_2 \in \hat{K}_0[V, W]$ such that the following conditions hold:

(3a) $\hat{F} = \hat{K}_0(x, z)$ and $f(x, Z) = \mathrm{irr}(z, \hat{K}_0(x))$; in particular $\mathrm{discr}(f(x, Z)) \in \hat{K}_0(x)^\times$.

(3b) $g(x, Y) = \mathrm{irr}(y, \hat{K}_0(x)) = \mathrm{irr}(y, \hat{K}(x))$; since $\hat{F}_0/\hat{K}_0$ is regular (by the first paragraph of Part A), $g(X, Y)$ is absolutely irreducible [FrJ08, Cor. 10.2.2(b)].

(3c) $y = \frac{p_1(x,z)}{p_0(x,z)}$, $z = \frac{q_1(c,x,y)}{q_0(c,x,y)}$, $p_0(x, z) \neq 0$, and $q_0(c, x, y) \neq 0$.

(3d) $v = \frac{r_1(x,y)}{r_0(x,y)}$, $w = \frac{r_2(x,y)}{r_0(x,y)}$, $x = \frac{s_1(v,w)}{s_0(v,w)}$, $y = \frac{s_2(v,w)}{s_0(v,w)}$, $r_0(x, y) \neq 0$, and $s_0(v, w) \neq 0$.

PART B: *Pushing down.* The polynomials introduced in Part A depend on only finitely many parameters from $\hat{K}_0$. Thus, there are $u_1, \ldots, u_n \in \hat{K}_0$ with the following properties:

(4a) The coefficients of $f, g, h, p_0, p_1, q_0, q_1, r_0, r_1, r_2, s_0, s_1, s_2$ are in $K_0[\mathbf{u}]$.

(4b) $F_{\mathbf{u}} = K_0(\mathbf{u}, x, z)$ is a Galois extension of $K_0(\mathbf{u}, x)$,
$f(x, Z) = \mathrm{irr}(z, K_0(\mathbf{u}, x))$, and $\mathrm{discr}(f(x, Z)) \in K_0(\mathbf{u}, x)^\times$.

(4c) $g(x, Y) = \mathrm{irr}(y, K_0(\mathbf{u}, x)) = \mathrm{irr}(y, K(\mathbf{u}, x))$; we set $F_{0,\mathbf{u}} = K_0(\mathbf{u}, x, y)$.

It follows that restriction maps the groups $\mathrm{Gal}(\hat{F}/\hat{K}_0(x))$, $\mathrm{Gal}(\hat{F}/\hat{F}_0)$, and $\mathrm{Gal}(\hat{F}/\hat{K}(x))$ isomorphically onto the groups $\mathrm{Gal}(F_{\mathbf{u}}/K_0(\mathbf{u},x))$, $\mathrm{Gal}(F_{\mathbf{u}}/F_{0,\mathbf{u}})$, and $\mathrm{Gal}(F_{\mathbf{u}}/K(\mathbf{u},x))$, respectively. Therefore, restriction transfers $\hat{\theta}$ to an isomorphism

$$\theta\colon \mathrm{Gal}(F_{\mathbf{u}}/K_0(\mathbf{u},x)) \to \mathrm{Gal}(K(\mathbf{u},x)/K_0(\mathbf{u},x)) \ltimes G \tag{5}$$

satisfying $\mathrm{pr}\circ\theta = \mathrm{res}_{F_{\mathbf{u}}/K(\mathbf{u},x)}$.

Part C: *Specialization.* Since K_0 is existentially closed in $\hat{K}_0$, the field $\hat{K}_0$ and therefore also $K_0(\mathbf{u})$ are regular extensions of K_0 (Lemma 1.5). Thus, $\mathbf{u}$ generates an absolutely irreducible variety $U = \mathrm{Spec}(K_0[\mathbf{u}])$ over K_0 [FrJ08, Cor. 10.2.2]. The variety U has a nonempty Zariski-open subset U' that contains $\mathbf{u}$ such that for each $\mathbf{u}' \in U'$ the K_0-specialization $\mathbf{u} \to \mathbf{u}'$ extends to a $K(x)$-homomorphism $'\colon K(x)[\mathbf{u},v,w,y,z] \to K(x)[\mathbf{u}',v',w',y',z']$ such that the following conditions, derived from (3) and (4), hold:

(6a) The coefficients of $f',g',h',p_0',p_1',q_0',q_1',r_0',r_1',r_2',s_0',s_1',s_2'$ belong to $K_0[\mathbf{u}']$.

(6b) $F = K_0(\mathbf{u}',x,z')$ is a Galois extension of $K_0(\mathbf{u}',x)$, $f'(x,z') = 0$, and $\mathrm{discr}(f'(x,Z)) \in K_0(\mathbf{u}',x)^\times$.

(6c) $y' = \frac{p_1'(x,z')}{p_0'(x,z')}$, $z' = \frac{q_1'(c,x,y')}{q_0'(c,x,y')}$, $p_0'(x,z') \neq 0$, and $q_0'(c,x,y') \neq 0$; we set $F_0 = K_0(\mathbf{u}',x,y')$ and find that $F = F_0K$.

(6d) $g'(X,Y)$ is absolutely irreducible, $\deg_Y(g'(x,Y)) = \deg_Y(g(x,Y))$, $g'(x,y') = 0$, and so $g'(x,Y) = \mathrm{irr}(y',K_0(\mathbf{u}',x)) = \mathrm{irr}(y',K(\mathbf{u}',x))$;

(6e) $h'(V,W)$ is absolutely irreducible, $h'(0,0) = 0$, and $\frac{\partial h'}{\partial W}(0,0) \neq 0$.

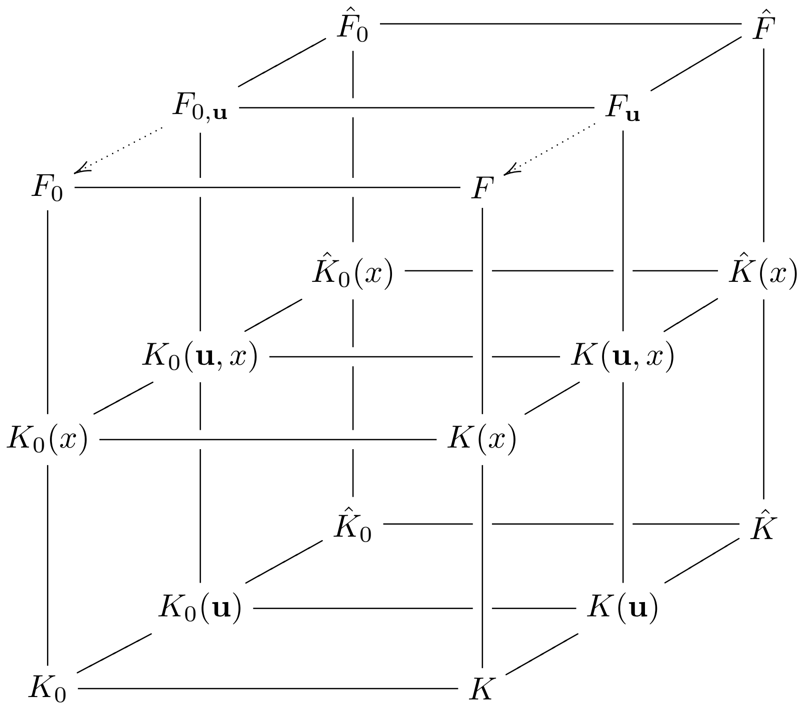
(6f) $v' = \frac{r_1'(x,y')}{r_0'(x,y')}$, $w' = \frac{r_2'(x,y')}{r_0'(x,y')}$, $x = \frac{s_1'(v',w')}{s_0'(v',w')}$, $y' = \frac{s_2'(v',w')}{s_0'(v',w')}$, $r_0'(x,y') \neq 0$, and $s_0'(v',w') \neq 0$; thus $F_0 = K_0(\mathbf{u}',v',w')$.

To achieve the absolute irreducibility of g' and h' we have used the Bertini-Noether theorem [FrJ08, Prop. 9.4.3].

Part D: *Choosing* $\mathbf{u}' \in K_0^n$. Since K_0 is existentially closed in $\hat{K}_0$ and since $\mathbf{u} \in U'(\hat{K}_0)$, we can choose $\mathbf{u}' \in U'(K_0)$. Then $K_0[\mathbf{u}'] = K_0$, $K_0(\mathbf{u}',x) = K_0(x)$, $F_0 = K_0(x,y') = K_0(v',w')$, and $F = K_0(x,z')$. Since $\mathrm{discr}(f'(x,Z)) \neq 0$ (by (6b)) the homomorphism $'$ induces an embedding

$$\psi^*\colon \mathrm{Gal}(F/K_0(x)) \to \mathrm{Gal}(F_{\mathbf{u}}/K_0(\mathbf{u},x)) \tag{7}$$

such that $(\psi^*(\sigma)(s))' = \sigma(s')$ for all $\sigma \in \mathrm{Gal}(F/K_0(x))$ and $s \in F_{\mathbf{u}}$ with $s' \in F$ [Lan93, p. 344, Prop. 2.8]. Each $s \in K(x)$ is fixed by $'$, hence $\psi^*(\sigma)(s) = \sigma(s)$ for each $\sigma \in \mathrm{Gal}(F/K_0(x))$. It follows that ψ^* commutes with restriction to $K(x)$.



By (6c), $F = K(x, y') = F_0K$. By (6d) and [FrJ08, Cor. 10.2.2(b)], F_0/K_0 is a regular extension, so F_0 is linearly disjoint from K over K_0. Therefore, F_0 is linearly disjoint from $K(x)$ over $K_0(x)$, hence $F_0 \cap K(x) = K_0(x)$ and $[F_0 : K_0(x)] = [F : K(x)]$. It follows from (6d) that

$$\begin{aligned}
|\mathrm{Gal}(F/K_0(x))| &= [F : K_0(x)] \\
&= [F : K(x)][K(x) : K_0(x)] \\
&= \deg_Y g'(x, Y)[K : K_0] \\
&= \deg_Y g(x, Y)[K : K_0] \\
&= [F_{\mathbf{u}} : K(\mathbf{u}, x)][K(\mathbf{u}, x) : K_0(\mathbf{u}, x)] \\
&= [F_{\mathbf{u}} : K_0(\mathbf{u}, x)] = |\mathrm{Gal}(F_{\mathbf{u}}/K_0(\mathbf{u}, x))|.
\end{aligned}$$

Therefore ψ^* is an isomorphism. Let

$$\rho\colon \mathrm{Gal}(K(\mathbf{u}, x)/K_0(\mathbf{u}, x)) \ltimes G \to \mathrm{Gal}(K(x)/K_0(x)) \ltimes G$$

be the isomorphism whose restriction to $\mathrm{Gal}(K(\mathbf{u},x)/K_0(\mathbf{u},x))$ is the restriction map and to G is the identity map. Then, $\theta' = \rho\circ\theta\circ\psi^*$ satisfies $\mathrm{pr}\circ\theta' = \mathrm{res}_{F/K(x)}$ (by (5)). This means that θ' is a solution of embedding problem (1).

PART E: *Rational place.* Finally, by (6e) and (6f), the curve defined by $h'(X,Y)=0$ is a model of F_0/K_0 and $(0,0)$ is a K_0-rational simple point of it. Therefore, by [Jar11, Lemma 5.1.4(b)], F_0 has a K_0-rational place $\varphi_0\colon F_0\to K_0\cup\{\infty\}$. Since K_0 is ample, F_0 has infinitely many K_0-places (Lemma 1.1). Only finitely many of them are ramified over $K_0(x)$. Hence, we may choose φ_0 to be unramified over $K_0(x)$. Using the linear disjointness of F_0 and K over K_0, we extend φ_0 to a K-rational place $\varphi\colon F\to K\cup\{\infty\}$ unramified over $K_0(x)$. ∎

THEOREM 16.2: *Let K_0 be an ample field. Then each constant finite split embedding problem over $K_0(x)$ has a split unramified rational solution.*

Proof: Consider a constant finite split embedding problem (1) over $K_0(x)$. Let $\hat K_0 = K_0((t))$. Then $\hat K_0$ is complete under a nontrivial discrete ultrametric absolute value with prime element t. Consequently, by Proposition 15.1, (2) has a split unramified rational solution. By Lemma , K_0 is existentially closed in $\hat K_0$. Hence, by Lemma 16.1, (1) has a split unramified rational solution. ∎

17. PAC Hilbertian Fields are ω-Free

The statement of the title was a major open problem of Field Arithmetic. Theorem 17.3 settles that problem.

Recall that the **rank** of a profinite group G is the least cardinality of a system of generators of G that converges to 1. If G is not finitely generated, then $\mathrm{rank}(G)$ is also the cardinality of the set of all open normal subgroups of G [FrJ08, Prop. 17.1.2]. We denote the free profinite group of rank m by $\hat F_m$.

An **embedding problem** for a profinite group G is a couple

$$(1)\qquad (\varphi\colon G\to A,\ \alpha\colon B\to A),$$

of homomorphisms of profinite groups with φ and α surjective. The embedding problem is said to be **finite** if B is finite. If there exists a homomorphism $\alpha'\colon A\to B$ such that

$\alpha \circ \alpha' = \mathrm{id}_A$, we say that (1) **splits**. A **weak solution** to (1) is a homomorphism $\gamma: G \to B$ such that $\alpha \circ \gamma = \varphi$. If γ is surjective, we say that γ is a **solution** to (1). We say that G is **projective** if every finite embedding problem for G has a weak solution.

An **embedding problem** over a field K is an embedding problem (1), where $G = \mathrm{Gal}(K)$. If L is the fixed field of $\mathrm{Ker}(\varphi)$, we may identify A with $\mathrm{Gal}(L/K)$ and φ with $\mathrm{res}_{K_s/L}$ and then consider $\alpha: B \to \mathrm{Gal}(L/K)$ as the given embedding problem. This shows that our present definition generalizes the one given in Section 5. Note that if $\gamma: \mathrm{Gal}(K) \to B$ is a solution of (1) and F is the fixed field in K_s of $\mathrm{Ker}(\gamma)$, then F is a solution field of the embedding problem $\alpha: B \to \mathrm{Gal}(L/K)$ and γ induces an isomorphism $\bar{\gamma}: \mathrm{Gal}(F/K) \to B$ such that $\alpha \circ \bar{\gamma} = \mathrm{res}_{F/L}$.

The first statement of the following proposition is due to Gruenberg [FrJ08, Lemma 22.3.2], the second one is a result of Iwasawa [FrJ08, Cor. 24.8.2].

PROPOSITION 17.1: *Let G be a projective group. If each finite split embedding problem for G is solvable, then every finite embedding problem for G is solvable. If in addition* $\mathrm{rank}(G) \le \aleph_0$, *then* $G \cong \hat{F}_\omega$.

We say that a field K is **ω-free** if every finite embedding problem over K (that is, finite embedding problem for $\mathrm{Gal}(K)$) is solvable.

THEOREM 17.2: *Let K be an ample field.*

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

(b) *If in addition,* $\mathrm{Gal}(K)$ *is projective, then K is ω-free.*

(c) *If in addition,* $\mathrm{Gal}(K)$ *has countably many generators, and in particular, if K is countable, then* $\mathrm{Gal}(K) \cong \hat{F}_\omega$.

Proof of (a): Every finite split embedding problem over K gives a finite split constant embedding problem over $K(x)$. The latter is solvable by Theorem 16.2. Now use the Hilbertianity and specialize to get a solution of the original embedding problem over K [FrJ08, Lemma 13.1.1].

Proof of (b): By (a), every finite split embedding problem over K is solvable. Hence, by Proposition 17.1, every finite embedding problem over K is solvable.

Proof of (c): Use (b) and Proposition 17.1. ∎

The following special case of Theorem 17.2 is a solution of [FrJ86, Prob. 24.41].

THEOREM 17.3: *Let K be a PAC field. Then K is ω-free if and only if K is Hilbertian.*

Proof: That 'K is ω-free' implies 'K is Hilbertian' is a result of Roquette [FrJ08, Cor. 27.3.3]. Conversely, if K is PAC, then $\mathrm{Gal}(K)$ is projective [FrJ08, Thm. 11.6.2]. By Example (a) of 2, K is ample. Hence, if K is Hilbertian, then by Theorem 17.2(b), K is ω-free. ∎

References

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic, Third Edition, revised by Moshe Jarden*, Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008.

[Jar11] M. Jarden, *Algebraic Patching*, Springer Monographs in Mathematics, Springer 2011