Introduction to Algebraic Patching

Béranger Seguin*

Abstract: Using the language and the tools of rigid analytic geometry, Harbater (1987) has defined a "patching operation" which can be used to solve the inverse Galois problem over fields like $\mathbb{Q}_p(T)$ or $\mathbb{F}_q(\!(X)\!)(T)$. Later, Haran and Völklein (1996) rephrased this construction in a purely algebraic language, replacing all geometric arguments with (almost entirely) explicit constructions. Our goal is to present their proof.

In the whole document, we fix a field K equipped with a nontrivial ultrametric valuation v for which it is complete. For example: $\mathbb{Q}_p$, any p-adic field, $\mathbb{F}_q(\!(T)\!)$, $K(\!(T)\!)$ for any field K.

The main reference is [1]. I am greatly indebted to Pierre Dèbes for explaining this proof to me. His explanations have directly inspired mine.

1. Statement

To make things simple, we take the following definition of "realization":

Definition 1.1. A *realization* of a finite group G is a field extension $F|K(T)$ such that:
1. $F|K(T)$ is Galois with Galois group isomorphic to G;
2. $F|K(T)$ is *regular*, i.e. $F \cap \overline{K} = K$;
3. F has an unramified prime of degree 1, i.e. for some $t_0 \in K$, the canonical embedding $K(T) \hookrightarrow K(\!(T - t_0)\!)$ extends into an embedding $F \subseteq K(\!(T - t_0)\!)$. The $(T - t_0)$-adic valuation of $K(\!(T - t_0)\!)$ then restricts to a place v of F above $(T - t_0)$, with $F_v \simeq K(\!(T - t_0)\!)$ and residue field K.

(Geometrically:
1. $F = K(Y)$ for a smooth curve Y, and the embedding $K(T) \hookrightarrow F$ corresponds to a connected ramified cover $Y \to \mathbb{P}^1_K$, Galois with automorphism group G;
2. Y is geometrically irreducible, i.e. $Y \times_{\operatorname{Spec} K} \operatorname{Spec} \overline{K}$ is irreducible;
3. Y has a K-point in the unramified fiber above t_0. Since the cover is Galois, the whole fiber then consists of K-points.)

Theorem 1.2. **(Patching)** Let G be a finite group generated by two subgroups G_1, G_2 which have realizations. Then, G admits a realization.

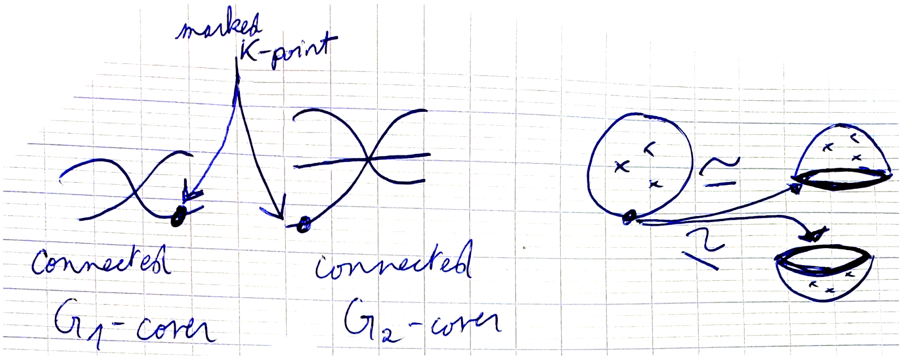
This theorem was first proved by Harbater (1987) using rigid analytic geometry. The proof was later rephrased by Haran and Völklein in a purely algebraic language [1, Proposition 4.3]. Their hope was to get rid of the completeness hypothesis. Instead, they made it very clear at which precise point completeness is used. We make a few remarks:
- Any finite group is generated by its cyclic subgroups. Thus, if all cyclic groups have realizations (see [1, Lemma 4.5]), the inverse Galois problem is solved over $K(T)$, e.g. over $\mathbb{Q}_p(T)$.
- This works over $\mathbb{C}$ (seeing it as abstractly isomorphic to $\mathbb{C}_p$), removing the need to use Riemann's existence theorem to solve the inverse Galois problem over $\mathbb{C}(T)$. See also [2].
- Other consequences if K is algebraically closed:
  - every embedding problem over $K(T)$ is solvable [1, Theorem 4.6];

*Universität Paderborn, Fakultät EIM, Institut für Mathematik, Warburger Str. 100, 33098 Paderborn, Germany. Email: bseguin@math.upb.de.

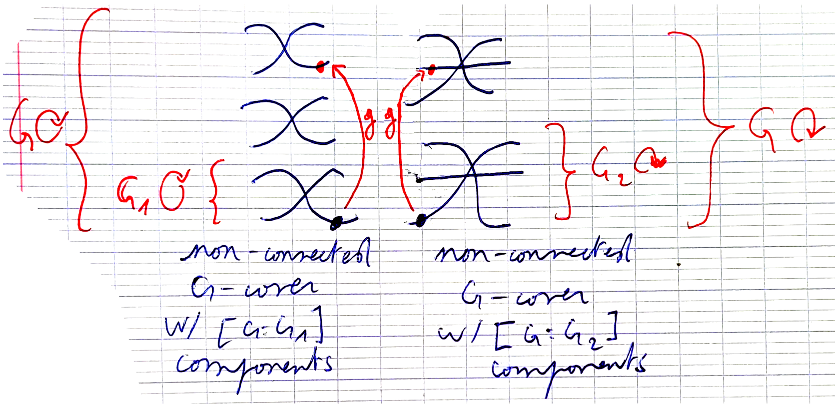
- if K is also countable, then the absolute Galois group of $K(T)$ is profinite free with countably many generators [1, Cororally 4.7].

2. Geometric Intuition

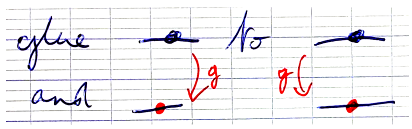
The whole point of algebraic patching is to avoid geometric arguments. However, since it adapts a geometric proof, it is great to have a rough overview of what we are trying to mimic.

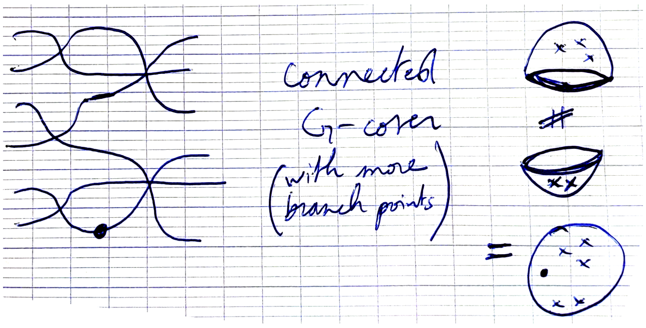


$$\Downarrow$$



$$\Downarrow$$





3. Where geometry hides: convergent power series

Throughout, we use the convention of denoting the fields of fractions of a domain R by $\hat{R}$.

We define the ring:

$$K\{T\} := \left\{ \sum_{n\geq 0} a_n T^n \in K[[T]] \,\middle|\, a_n \to 0 \right\}.$$

(Geometrically: ring of "holomorphic functions" on a disk of radius 1 around 0)

Similarly, we obtain rings $K\{T^{-1}\}$ ("holomorphic functions on the disk around ∞") and $K\{T, T^{-1}\}$ ("holomorphic functions on the unit circle"; here, $a_n \to 0$ when $|n| \to \infty$). Note that $K\{T\} \cap K\{T^{-1}\} = K$ in $K\{T, T^{-1}\}$ ("holomorphic functions on $\mathbb{P}^1$ are constant", an ultrametric form of Liouville's theorem). We are going to use the corresponding fields of fractions ("meromorphic functions") $\widehat{K\{T\}}, \widehat{K\{T^{-1}\}}$ and $\widehat{K\{T, T^{-1}\}}$.

Lemma 3.1. $\widehat{K\{T\}} \cap \widehat{K\{T^{-1}\}} = K(T)$ in $\widehat{K\{T, T^{-1}\}}$.

(Proved using Weierstrass' division theorem, which is a form of Euclidean division in rings of convergent power series) (Geometrically: "meromorphic functions on $\mathbb{P}^1$ are rational", an ultrametric form of Riemann's existence theorem.)

Lemma 3.2. [**3, Theorem 2.14**] If $\sum a_n T^n \in K(\!(T)\!)$ is algebraic over $K(T)$, then there is a $r \in K^\times$ such that $\sum a_n (rT)^n \in \widehat{K\{T\}}$.

(**Idea:** if the coefficients a_n grow faster than any exponential, then no polynomial can cause the required cancellations; the correct proof requires careful estimations and Newton polygons)

Lemma 3.3. [**1, Corollary 2.3**] **(Cartan's lemma)** Let $P \in \mathrm{GL}_n\left(\widehat{K\{T, T^{-1}\}}\right)$. Then, there are matrices $P_1 \in \mathrm{GL}_n\left(\widehat{K\{T\}}\right), P_2 \in \mathrm{GL}_n\left(\widehat{K\{T^{-1}\}}\right)$ such that $P = P_1 P_2$.

(The proof is quite computational, relying on a simple induction. Arbitrarily good approximations may be computed with a simple algorithm.)

4. Patching two extensions

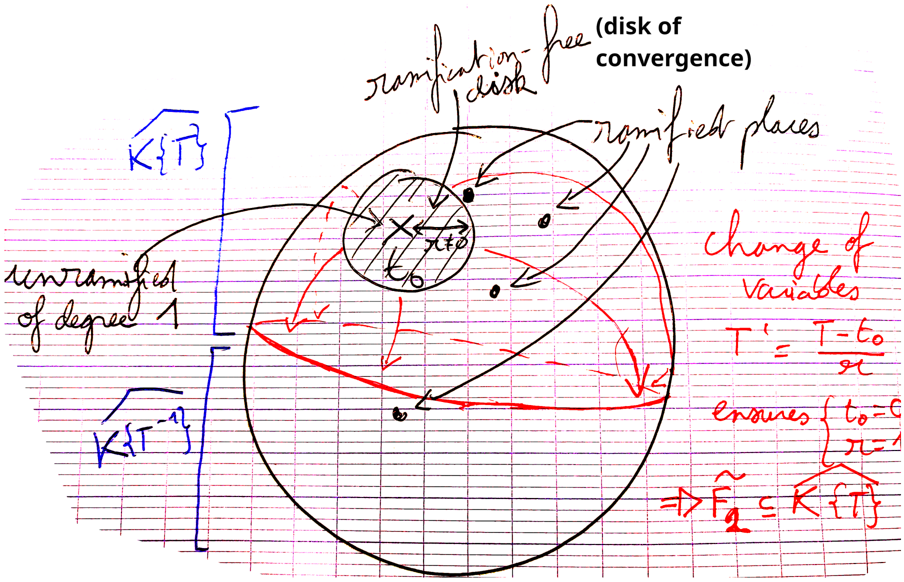
Let G_1, G_2 be two subgroups of G generating G. Let $F_1 | K(T)$ be a realization of G_1, $F_2 | K(T)$ be a realization of G_2.

4.1. Embedding the extensions in rings of power series

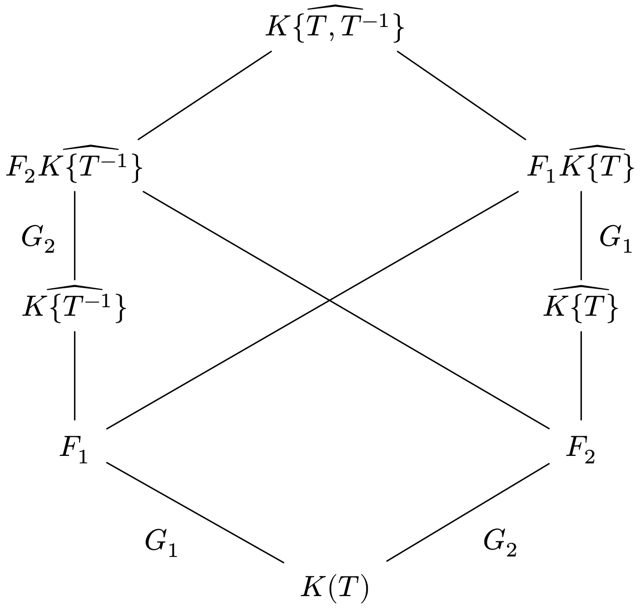
We reduce to the case where we have embeddings $F_1 \hookrightarrow \widehat{K\{T^{-1}\}}$ and $F_2 \hookrightarrow \widehat{K\{T\}}$. As both cases are symmetrical, we focus on proving that we can replace F_2 with a subfield of $\widehat{K\{T\}}$.

By hypothesis, there is an prime of degree 1 unramified in F_2, so $F_2 \subseteq K(\!(T - t_0)\!)$. Consider a primitive element β_2 of F_2, which we see as an element $\sum a_n (T - t_0)^n \in K(\!(T - t_0)\!)$, algebraic over $K(T)$. By Lemma 3.2, there is a $r \in K^\times$ such that $\sum a_n r^n (T - t_0)^n \in \widehat{K\{T - t_0\}}$. Making the change of variables $T' = \frac{T - t_0}{r}$, we have $\beta_2 = \sum a_n (T - t_0)^n = \sum a_n r^n \left(\frac{T - t_0}{r}\right)^n = \sum a_n r^n (T')^n \in \widehat{K\{T'\}}$. Thus F_2 embeds in $\widehat{K\{T'\}}$.

(Equivalently, replace F_2 by $\widetilde{F_2} = K(T)\left(\widetilde{\beta_2}\right)$ where $\widetilde{\beta_2} := \sum a_n r^n T^n \in \widehat{K\{T\}}$.)



We now assume $F_1 \subseteq \widehat{K\{T^{-1}\}}$ and $F_2 \subseteq \widehat{K\{T\}}$. Note that F_2 and $\widehat{K\{T^{-1}\}}$ are linearly disjoint as F_2 is Galois over $K(T)$, included in $\widehat{K\{T\}}$ and $\widehat{K\{T^{-1}\}} \cap \widehat{K\{T\}} = K(T)$. Hence, $F_2\widehat{K\{T^{-1}\}}$ is a Galois field extension of $\widehat{K\{T^{-1}\}}$ with Galois group G_2, and symmetrically $F_1\widehat{K\{T\}}|\widehat{K\{T\}}$ is Galois with group G_1. The situation is summed up by the field diagram:



In what follows, we denote by i_1 the isomorphism $G_1 \xrightarrow{\sim} \mathrm{Gal}\left(F_1\widehat{K\{T\}}|\widehat{K\{T\}}\right)$ and by i_2 the isomorphism $G_2 \xrightarrow{\sim} \mathrm{Gal}\left(F_2\widehat{K\{T^{-1}\}}|\widehat{K\{T^{-1}\}}\right)$.

4.2. Turning the G_i-realizations into étale G-algebras

We define the following $F_1\widehat{K\{T\}}$-algebra (where both sum and multiplication are pointwise):

$$F_1' := \left\{ \text{maps } \psi : G \to F_1\widehat{K\{T\}} \,\middle|\, \psi(g\alpha) = i_1(\alpha^{-1})(\psi(g)) \text{ for all } g \in G, \alpha \in G_1 \right\}.$$

The condition defining F_1' implies that the elements $\psi(g)$ determine each other when they belong to a same orbit under right multiplication by an element of G_1. For instance, if one chooses representatives $\omega_1, ..., \omega_r$ of G/G_1, then an element of F_1' is determined by the elements $\psi(\omega_1), ..., \psi(\omega_r) \in F_1\widehat{K\{T\}}$, as $\psi(\omega_i\alpha) = i_1(\alpha^{-1})(\psi(\omega_i))$. So, F_1' is abstractly isomorphic to a product of $[G : G_1]$ copies of $F_1\widehat{K\{T\}}$. Its dimension over $\widehat{K\{T\}}$ is $[G : G_1]|G_1| = |G|$.

Note that G acts on F_1' via the left action $(h.\psi)(g) = \psi(h^{-1}g)$. The fixed subalgebra ${F_1'}^G$ of F_1' under G corresponds to constant maps $\psi : G \to F_1\widehat{K\{T\}}$, identified with their value at 1, and satisfying the relation $\psi = i_1(\alpha^{-1})(\psi)$ for all $\alpha \in G_1$. Since $F_1\widehat{K\{T\}}|\widehat{K\{T\}}$ is Galois with group $i_1(G_1)$, it follows that ${F_1'}^{G_1}$ can be identified with $\widehat{K\{T\}}$.

We define symmetrically the following $F_2\widehat{K\{T^{-1}\}}$-algebra:

$$F_2' := \left\{ \text{maps } \psi : G \to F_2\widehat{K\{T^{-1}\}} \,\middle|\, \psi(g\beta) = i_2(\beta^{-1})(\psi(g)) \text{ for all } g \in G, \beta \in G_2 \right\}.$$

4.3. The actual patching step

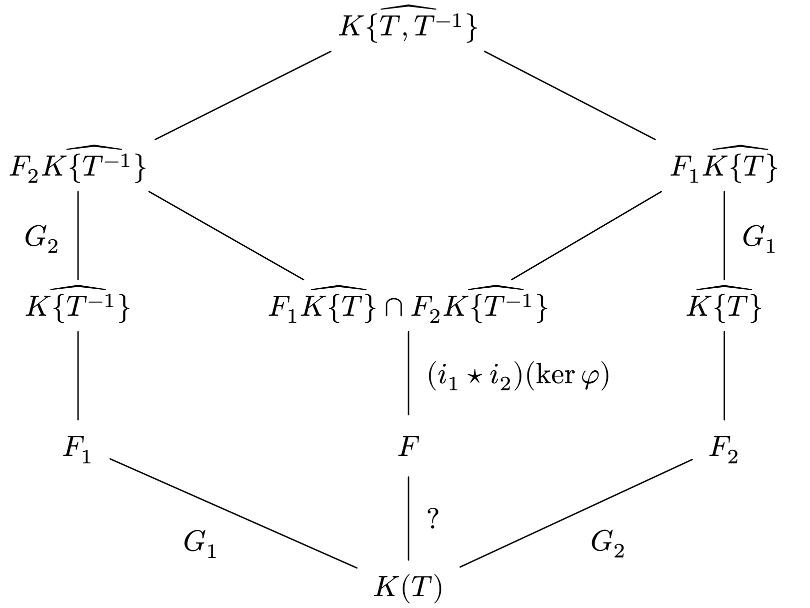
Finally, we define the algebra $F := F_1' \cap F_2'$, where the intersection is taken in the algebra of all maps $G \to \widehat{K\{T, T^{-1}\}}$:

$$F = \left\{ \text{maps } \psi : G \to F_1\widehat{K\{T\}} \cap F_2\widehat{K\{T^{-1}\}} \,\middle|\, \begin{array}{l} \psi(g\alpha) = i_1(\alpha^{-1})(\psi(g)) \text{ for all } g \in G, \alpha \in G_1 \\ \psi(g\beta) = i_2(\beta^{-1})(\psi(g)) \text{ for all } g \in G, \beta \in G_2 \end{array} \right\}.$$

Since G_1 and G_2 generate G, such a map is determined by the image of 1: this lets us see F as a subalgebra of $F_1\widehat{K\{T\}} \cap F_2\widehat{K\{T^{-1}\}}$, specifically the fixed subfield of $F_1\widehat{K\{T\}} \cap F_2\widehat{K\{T^{-1}\}}$ under the set of all automorphisms $i_1(\alpha_1) \circ i_2(\beta_1) \circ i_1(\alpha_2) \circ i_2(\beta_2) \circ \ldots \circ i_1(\alpha_n) \circ i_2(\beta_n)$ where $\alpha_i \in G_1$, $\beta_i \in G_2$, and the product $\alpha_1\beta_1 \ldots \alpha_n\beta_n$ evaluates to 1 in G.[2] In particular, F is a field.

The action of G on maps $\psi : G \to \widehat{K\{T, T^{-1}\}}$ (defined by $(h.\psi)(g) = \psi(h^{-1}g)$) restricts to $F = F_1' \cap F_2'$. The fixed subfield is $F^G = {F_1'}^G \cap {F_2'}^G = \widehat{K\{T\}} \cap \widehat{K\{T^{-1}\}} = K(T)$. In particular, F is a finite Galois extension of $K(T)$, whose Galois group is a quotient of G.

Remark 4.3.1. As of now, we did not use completeness!



4.4. Constructing a basis of F

The only thing which is missing is a "lower bound" on F, i.e., an equality of dimensions $[F : K(T)] = |G|$. To prove this equality, we are going to construct a basis of F over $K(T)$.

[2]This can be written in terms of the free product $G_1 \star G_2$, which has a surjective "product" morphism φ to G induced by the inclusions in G, and a morphism $i_1 \star i_2$ to $\mathrm{Aut}\left(F_1\widehat{K\{T\}} \cap F_2\widehat{K\{T^{-1}\}}\right)$. Then, F is the fixed subfield of $F_1\widehat{K\{T\}} \cap F_2\widehat{K\{T^{-1}\}}$ under $(i_1 \star i_2)(\ker\varphi)$.

(**Small tool:** If L is a field and V is a L-vector space of dimension n, there is a (fully coordinate-free) simply transitive left action of $\mathrm{GL}_n(L)$ on the set of L-bases of V, given by $(M.\mathcal{B})_i = \sum_j M_{ij}\mathcal{B}_j$, i.e. $M.\mathcal{B}$ is the unique basis of V such that the transition matrix between $\mathcal{B}$ and $M.\mathcal{B}$ is M.)

Choose a $\widehat{K\{T\}}$-basis $\mathcal{B}_1$ of F_1' and a $\widehat{K\{T^{-1}\}}$-basis $\mathcal{B}_2$ of F_2'.[3] Since these spaces have dimension $|G|$, both $\mathcal{B}_1$ and $\mathcal{B}_2$ are bases (after extension of scalars to $K\{\widehat{T,T^{-1}}\}$) of the $K\{\widehat{T,T^{-1}}\}$-vector space of all maps $G \to K\{\widehat{T,T^{-1}}\}$, of dimension $|G|$. Form the transition matrix $P \in \mathrm{GL}_{|G|}\left(K\{\widehat{T,T^{-1}}\}\right)$ between these two bases, so that $\mathcal{B}_1 = P.\mathcal{B}_2$, and use Lemma 3.3 (this uses completeness!) to decompose P as a product P_1P_2 with $P_1 \in \mathrm{GL}_{|G|}\left(\widehat{K\{T\}}\right)$, $P_2 \in \mathrm{GL}_{|G|}\left(\widehat{K\{T^{-1}\}}\right)$. Now, define the basis $\mathcal{B} = P_2.\mathcal{B}_2$ of F_2'. Note that $\mathcal{B}$ is also a basis of F_1' since $\mathcal{B} = P_1^{-1}.\mathcal{B}_1$ (over $K\{\widehat{T,T^{-1}}\}$, this simply follows from $P_1.\mathcal{B} = P_1P_2.\mathcal{B}_2 = P.\mathcal{B}_2 = \mathcal{B}_1$). Therefore, the basis $\mathcal{B}$ is contained in $F = F_1' \cap F_2'$, which proves that $[F : K(T)] = |\mathcal{B}| = |G|$.

4.5. **Ramification in the patched extension**

4.5.1. Ramified primes of the patched extension.

Assume F_1, F_2 are unramified above some place $(T - t_0)$, i.e. they embed into $\overline{K}(\!(T - t_0)\!)$. The cases $v(t_0) \geq 0$ and $v(t_0) \leq 0$ are symmetrical, thus we assume $v(t_0) \geq 0$. Then, the ultrametric inequality implies $\widehat{K\{T\}} = \widehat{K\{T - t_0\}} \subseteq \overline{K}(\!(T - t_0)\!)$, and thus $F_1\widehat{K\{T\}}$ embeds into $\overline{K}(\!(T - t_0)\!)$ and finally $F \subseteq F_1\widehat{K\{T\}}$ embeds into $\overline{K}(\!(T - t_0)\!)$. Thus, $F|K(T)$ is unramified above t_0.

Remark 4.5.1.1. More generally, $F\widehat{K\{T\}} = F_1\widehat{K\{T\}}$ and $F\widehat{K\{T^{-1}\}} = F_2\widehat{K\{T^{-1}\}}$. The decomposition subgroups of G at a given place $(T - x)$ are those of F_1 or F_2 (depending on the sign of $v(x)$).

4.5.2. Existence of an unramified prime of degree 1.

Let $x \in K$ with $v(x) = 0$ and such that $(T - x)$ is unramified in F (this is the case for all but finitely many choices of x). The evaluation morphism: $e_x : \begin{cases} K\{T,T^{-1}\} \to K \\ \sum a_n T^n \to \sum a_n x^n \end{cases}$ is well-defined, surjective, and has kernel $(T - x)K\{T, T^{-1}\}$ (Weierstrass' division theorem). So, the (discrete) $(T - x)$-adic valuation on $K\{\widehat{T,T^{-1}}\}$ has residue field K. The ring of elements of nonnegative valuation is the localization $K\{T, T^{-1}\}_{(T-x)}$.

The restriction of the $(T - x)$-adic valuation to F is a discrete valuation v' lying above the unramified prime $(T - x)$ of $K(T)$. The ring $F_{(v')}$ of elements $x \in F$ with $v'(x) \geq 0$ is contained in $K\{T, T^{-1}\}_{(T-x)}$, and we get a composite map:

$$F_{(v')} \hookrightarrow K\{T, T^{-1}\}_{(T-x)} \twoheadrightarrow K\{T, T^{-1}\}_{(T-x)}/(T - x)K\{T, T^{-1}\}_{(T-x)} \simeq K.$$

This map is surjective as its restriction to $K[T]_{(T-x)}$ is $K[T]_{(T-x)} \twoheadrightarrow K[T]/(T - x)K[T] \simeq K$. This means that v' is an unramified place of F with residue field K.

Bibliography

[1] D. Haran and H. Völklein, "Galois groups over complete valued fields," *Israel Journal of Mathematics*, vol. 93, pp. 9–27, 1996, doi: 10.1007/BF02761092.

[2] A. Fehm, D. Haran, and E. Paran, "The Inverse Galois Problem over $\mathbb{C}(z)$", *Contemporary Mathematics*, vol. 767, pp. 115–123, 2021, doi: 10.1090/conm/767/15401.

[3] E. Artin, *Algebraic Numbers and Algebraic Functions*. 1967.

[3] Let $i \in \{1, 2\}$. Choosing a system of representatives of G/G_i and a primitive element β_i of F_i, we can write very explicit bases, for which the transition matrix in the canonical basis $(\mathbb{1}_g)_{g\in G}$ is a block-diagonal matrix of size $|G|$ with $[G : G_i]$ diagonal blocks which are Vandermonde matrices of size $|G_i|$ involving the conjugates of β_i.