THE INVERSE GALOIS PROBLEM OVER $\mathbb{C}(z)$

ARNO FEHM, DAN HARAN AND ELAD PARAN

Abstract. We give a self-contained elementary solution for the inverse Galois problem over the field of rational functions over the complex numbers.

1. Introduction

Since the 19th century one of the foundational open questions of Galois theory is the *inverse Galois problem*, which asks whether every finite group occurs as the Galois group of a Galois extension of the field $\mathbb{Q}$ of rational numbers. In 1892 Hilbert proved his celebrated *irreducibility theorem* and deduced that the inverse Galois problem has a positive answer provided that every finite group occurs as the Galois group of a Galois extension of the field $\mathbb{Q}(z)$ of rational functions over $\mathbb{Q}$. It was known already back then that the analogous problem for the field $\mathbb{C}(z)$ of rational functions over the complex numbers indeed has a positive answer: *Every finite group occurs as the Galois group of a Galois extension of* $\mathbb{C}(z)$. The aim of this work is to give a new and elementary proof of this result which uses only basic complex analysis and field theory. The value of such a proof becomes clear when compared to the previously known ones:

1.1. **Classical proof using Riemann's existence theorem.** The classical proof (likely the one known to Hilbert) uses the fact that the finite extensions of $\mathbb{C}(z)$ correspond to compact Riemann surfaces realized as branched covers of the Riemann sphere $\hat{\mathbb{C}}$, which in turn are described by the fundamental group $\pi_1(D)$ of domains $D = \hat{\mathbb{C}} \smallsetminus \{z_1, \dots, z_d\}$, where $z_1, \dots, z_d$ are the branch points. This correspondence follows from Riemann's existence theorem, which states that every compact Riemann surface admits meromorphic functions with prescribed values at finitely many points. This is a deep theorem proven using potential theory [Lam09, Ch. X] or the theory of Hilbert spaces and cohomology [Voe96, Ch. 6].

1.2. **Modern proofs via ultrametric analysis.** Various "patching" approaches that appeared in recent years allow the study of the Galois theory of $K(z)$ for fields K that are complete with respect to an *ultrametric* absolute value, like the field $\mathbb{Q}_p$ of p-adic numbers or the field $F((t))$ of formal power series over a base field F. Such approaches can be used to give, somewhat artificially, a proof of the inverse Galois problem over $\mathbb{C}(z)$: For example, one could prove a strengthening of the inverse Galois problem (the so-called *regular inverse Galois problem*) over $\mathbb{Q}_p(z)$ and then, via an embedding of $\mathbb{Q}_p$ into $\mathbb{C}$ (which cannot be continuous but exists by the axiom of choice), deduce the inverse

2010 *Mathematics Subject Classification.* Primary: 11R32; Secondary: 12E30, 30H50.

Galois problem over $\mathbb{C}(z)$, cf. [DD99, §1]. Alternatively, one could prove the regular inverse Galois problem over $\mathbb{C}((t))(z)$, where $\mathbb{C}((t))$ is the complete field of formal power series over $\mathbb{C}$, and then "push down" this solution to $\mathbb{C}(z)$, cf. [HJ98, §6].

Such a proof has the obvious disadvantage that it invokes constructions and methods from the non-archimedean world that are foreign to the object of study – the field of complex numbers – while at the same time completely ignoring the useful analytic structure of $\mathbb{C}$: Early patching approaches, such as Harbater's *formal patching* [Har87], as well as *rigid patching* [Ser92] [Liu95] build on the heavy machinery of formal schemes, respectively Tate's rigid geometry and formal / rigid GAGA theorems – cf. the survey [Har03]. In more recent approaches, such as Haran-Völklein's *algebraic patching* [Jar11] and Harbater-Hartmann's *field patching* [HH10], which abstain from employing heavy geometric theories, one needs algebraic structure theorems for certain rings of non-archimedean holomorphic functions.

1.3. **A direct proof.** The new proof we propose follows the footsteps of the *algebraic patching* approach of [HV96], though here we work directly over the complex numbers with intrinsic rings of holomorphic functions on discs and annuli on the Riemann sphere. The heart of the proof is a matrix factorization result for our rings (Proposition 2.5), which is a variant of the classical Wiener-Hopf factorization theorem in harmonic analysis, cf. [BS06] or [GF74]. This factorization result allows us to realize groups inductively by "patching" two subgroups at a time (Proposition 3.5), where the "patches" correspond to two discs that intersect in an annulus.

We note that while our approach is inspired by the mentioned lofty methods and ideas, the proof itself is self-contained and elementary, and invokes only undergraduate complex analysis, linear algebra, and field theory. On the other hand, the previously explained approaches, in particular the one using Riemann's existence theorem, allow to prove much stronger statements on the Galois theory of $\mathbb{C}(z)$ than just the inverse Galois problem, and we refer the interested reader to [Har03] and [Voe96] for more details. For results on the inverse Galois problem over other fields see for example [DD99], [Jar11].

2. Rings of holomorphic functions

Let $\emptyset \neq I \subseteq [0,\infty]$ be an open interval, like (r_1, r_2), $[0, r_2)$, $(r_1, \infty]$ with $0 < r_1 < r_2 < \infty$, and denote by

$$A_I = \{z \in \hat{\mathbb{C}} \mid |z| \in I\}$$

the corresponding annulus around the origin (where $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ is the Riemann sphere). For a domain $\emptyset \neq D \subseteq \hat{\mathbb{C}}$ we denote by $\mathcal{H}(D)$ and $\mathcal{M}(D)$ the ring of holomorphic resp. meromorphic functions on D and let $\mathcal{H}_I = \mathcal{H}(A_I)$, $\mathcal{M}_I = \mathcal{M}(A_I)$. Recall that every $f \in \mathcal{H}_I$ has a unique Laurent series expansion

$$f(z) = \sum_{k=-\infty}^{\infty} f_k z^k, \quad f_k \in \mathbb{C}$$

which converges *pointwise* to f on A_I. In particular, $f_k = 0$ for $k < 0$ if $0 \in I$, and $f_k = 0$ for $k > 0$ if $\infty \in I$. We denote by $\mathcal{W}_I$ the set of those such f for which the convergence is even *normal* on A_I, i.e.

$$\mathcal{W}_I = \{f \in \mathcal{H}_I \mid ||f||_I < \infty\},$$

where

$$||f||_I = \sum_{k=-\infty}^{\infty} \sup_{z \in A_I} |f_k z^k| = \sum_{k=-\infty}^{\infty} |f_k| \sup_{z \in A_I} |z|^k.$$

Lemma 2.1. *$(\mathcal{W}_I, ||.||_I)$ is a Banach algebra.*

Proof. For $f, g \in \mathcal{W}_I$, obviously $||f + g||_I \leq ||f||_I + ||g||_I$. Also,

$$||fg||_I = \sum_n \left| \sum_{k+l=n} f_k g_l \right| \sup_{z \in A_I} |z^n| \leq \sum_n \sum_{k+l=n} |f_k| \cdot |g_l| \sup_{z \in A_I} |z|^k \sup_{z \in A_I} |z|^l = ||f||_I \cdot ||g||_I,$$

so $\mathcal{W}_I$ is a $\mathbb{C}$-algebra and $||.||_I$ is a norm on $\mathcal{W}_I$.

If $(f_n)_{n=1}^{\infty}$ is a Cauchy sequence in $\mathcal{W}_I$, then, replacing it with a suitable subsequence, we can assume that $||f_{n+1} - f_n||_I < 2^{-n}$ for all n, hence, writing $f_n = \sum_k f_{n,k} z^k$, we have

$$\sum_{n>N} \sum_k |f_{n+1,k} - f_{n,k}| \sup_{z \in A_I} |z|^k = \sum_{n>N} ||f_{n+1} - f_n||_I < \sum_{n>N} 2^{-n} = 2^{-N}$$

for all N. In particular, $(f_{n,k})_{n=1}^{\infty}$ a Cauchy sequence in $\mathbb{C}$, for every k, hence it converges. Let $g_k = \lim_{n\to\infty} f_{n,k}$. Then $g_k - f_{N,k} = \lim_{n\to\infty} f_{n+1,k} - f_{N,k} = \sum_{n \geq N} f_{n+1,k} - f_{n,k}$, for all N, hence $g = \sum_k g_k z^k$ satisfies

$$||g - f_N||_I = \sum_k |g_k - f_{N,k}| \sup_{z \in A_I} |z|^k = \sum_k \left| \sum_{n \geq N} f_{n+1,k} - f_{n,k} \right| \sup_{z \in A_I} |z|^k < 2^{-N+1} \to 0.$$

From this we see that $f_N \to g$ uniformly on A_I, hence $g \in \mathcal{H}_I$, and that $||g||_I < \infty$, hence $g \in \mathcal{W}_I$. Thus, $\mathcal{W}_I$ is complete. □

Lemma 2.2. *$\mathcal{W}_I$ is an integral domain.*

Proof. We have $\mathcal{W}_I \subseteq \mathcal{H}_I$, and $\mathcal{H}_I$ is an integral domain since a non-zero holomorphic function on A_I has only isolated zeros, and so the product of two such functions is again non-zero. □

From now on we always view $\mathcal{W}_I$ as a Banach algebra equipped with the norm $||.||_I$ and identify its quotient field $\mathrm{Quot}(\mathcal{W}_I)$ with a subfield of $\mathcal{M}_I$.

Lemma 2.3. *Let $0 < r_1 < r_2 < \infty$.*

(a) *The ring of Laurent polynomials $\mathbb{C}[z, z^{-1}]$ is dense in $\mathcal{W}_{(r_1,r_2)}$.*

(b) *The Banach algebras $\mathcal{W}_{[0,r_2)}$ and $\mathcal{W}_{(r_1,\infty]}$ are Banach subalgebras of $\mathcal{W}_{(r_1,r_2)}$.*

(c) *There is a continuous additive homomorphism $\varphi\colon \mathcal{W}_{(r_1,r_2)} \to \mathcal{W}_{[0,r_2)}$ with*

(c1) $\varphi|_{\mathcal{W}_{[0,r_2)}} = \mathrm{id}_{\mathcal{W}_{[0,r_2)}}$,

(c2) $\ker(\varphi) \subseteq \mathcal{W}_{(r_1,\infty]}$, *and*

(c3) $||\varphi(f)||_{[0,r_2)} \leq ||f||_{(r_1,r_2)}$ *for all* $f \in \mathcal{W}_{(r_1,r_2)}$.

(d) $\mathrm{Quot}(\mathcal{W}_{[0,r_2)}) \cap \mathrm{Quot}(\mathcal{W}_{(r_1,\infty]}) = \mathbb{C}(z)$.
(e) $\mathcal{H}_{[0,r_2)} \subseteq \mathcal{W}_{[0,r_1)}$.

Proof. (a): If $f = \sum_k f_k z^k \in \mathcal{W}_{(r_1,r_2)}$, then $g_N := \sum_{k=-N}^{N} f_k z^k \in \mathbb{C}[z, z^{-1}]$ converges to f in $\mathcal{W}_{(r_1,r_2)}$ as $N \to \infty$.

(b): This is clear from the definition of the norms $||.||_{[0,r_2)}$, $||.||_{(r_1,\infty]}$, $||.||_{(r_1,r_2)}$, since

$$\sup_{z \in A_{(r_1,r_2)}} |z|^k = \begin{cases} r_2^k = \sup_{z \in A_{[0,r_2)}} |z|^k, \text{ for } k \geq 0 \\ r_1^k = \sup_{z \in A_{(r_1,\infty]}} |z|^k, \text{ for } k \leq 0 \end{cases}.$$

(c): For $f = \sum_k f_k z^k \in \mathcal{W}_{(r_1,r_2)}$ let $\varphi(f) := \sum_{k=0}^{\infty} f_k z^k \in \mathcal{W}_{[0,r_2)}$. Clearly, φ is an additive homomorphism with $\varphi|_{\mathcal{W}_{[0,r_2)}} = \mathrm{id}_{\mathcal{W}_{[0,r_2)}}$ and $\ker(\varphi) \subseteq \mathcal{W}_{(r_1,\infty]}$. By (b), $||\varphi(f)||_{[0,r_2)} = ||\varphi(f)||_{(r_1,r_2)} \leq ||f||_{(r_1,r_2)}$ for all $f \in \mathcal{W}_{(r_1,r_2)}$. In particular, φ is continuous.

(d): It follows from Liouville's theorem (cf. [Lam09, 1.6.5(3)]) that

$$\mathrm{Quot}(\mathcal{W}_{[0,r_2)}) \cap \mathrm{Quot}(\mathcal{W}_{(r_1,\infty]}) \subseteq \mathcal{M}_{[0,r_2)} \cap \mathcal{M}_{(r_1,\infty]} = \mathcal{M}(\hat{\mathbb{C}}) = \mathbb{C}(z).$$

(e): For $f = \sum_{k=0}^{\infty} f_k z^k \in \mathcal{H}_{[0,r_2)}$ the convergence is absolute on $A_{[0,r_2)}$, in particular at $r_1 \in A_{[0,r_2)}$, hence $||f||_{[0,r_1)} = \sum_{k=0}^{\infty} |f_k| r_1^k < \infty$. □

Let $n \in \mathbb{N}$. Since $\mathcal{W}_I$ is complete, the ring of $n \times n$-matrices $\mathrm{Mat}_n(\mathcal{W}_I)$ is complete with respect to the sub-multiplicative matrix norm defined for $A = (a_{ij})_{i,j=1,\ldots,n}$ by

$$|A| = n \cdot \max_{i,j} ||a_{ij}||_I.$$

Notice that the unit matrix $\mathbb{1}$ in $\mathrm{Mat}_n(\mathcal{W}_I)$ satisfies $|\mathbb{1}| = n$.

Lemma 2.4. *Let $A \in \mathrm{Mat}_n(\mathcal{W}_I)$. If $|\mathbb{1} - A| < 1$, then $A \in \mathrm{GL}_n(\mathcal{W}_I)$.*

Proof. Let $B = \mathbb{1} - A$. Since $\mathrm{Mat}_n(\mathcal{W}_I)$ is complete, the geometric series $\sum_{k=0}^{\infty} B^k$ converges to some $C \in \mathrm{Mat}_n(\mathcal{W}_I)$, and $AC = CA = \mathbb{1}$. □

We now fix $0 < r_1 < r_2 < \infty$ and write $R = \mathcal{W}_{(r_1,r_2)}$, $R_1 = \mathcal{W}_{[0,r_2)}$, $R_2 = \mathcal{W}_{(r_1,\infty]}$. For $M \in \mathrm{Mat}_n(R)$ we denote by $M^+ \in \mathrm{Mat}_n(R_1)$ the matrix obtained by applying the continuous map φ of Lemma 2.3(c) to the entries of M. Thus, $M \mapsto M^+$ is a continuous map.

Proposition 2.5 (Matrix factorization)**.** *For every $A \in \mathrm{GL}_n(R)$ there exist matrices $B_1 \in \mathrm{GL}_n(R_1)$, $B_2 \in \mathrm{GL}_n(R_2)$ and $C \in \mathrm{GL}_n(\mathbb{C}(z))$ with $A = B_1 B_2 C$.*

Proof. By Lemma 2.3(a), applied to the entries of $A^{-1} \in \mathrm{GL}_n(R)$, there exists $D \in \mathrm{Mat}_n(\mathbb{C}[z, z^{-1}])$ with $|D - A^{-1}| < \frac{1}{n+2}|A|^{-1}$, so $|AD - \mathbb{1}| \leq |A| \cdot |D - A^{-1}| < \frac{1}{n+2}$. Let $A_0 = \mathbb{1} - AD$. Since $|A_0| < \frac{1}{n+2} < \frac{1}{2}$, which implies $\frac{|A_0|}{1-|A_0|} < 1$, the infinite sum

$$A_0^+ + (A_0^+ \cdot A_0)^+ + ((A_0^+ \cdot A_0)^+ \cdot A_0)^+ + \ldots$$

converges by Lemma 2.3(c3) to a matrix $A_1 \in \mathrm{Mat}_n(R_1)$ with $|A_1| < \sum_{k=1}^{\infty} |A_0|^k \leq \frac{|A_0|}{1-|A_0|} < 1$. Since the map $M \mapsto M^+$ is additive and continuous,

$$\begin{aligned}((\mathbb{1}+A_1)A_0)^+ &= A_0^+ + (A_1A_0)^+ = \\ &= A_0^+ + \big(A_0^+A_0 + (A_0^+ \cdot A_0)^+A_0 + ((A_0^+ \cdot A_0)^+ \cdot A_0)^+A_0 + \ldots\big)^+ = \\ &= A_0^+ + (A_0^+ \cdot A_0)^+ + ((A_0^+ \cdot A_0)^+ \cdot A_0)^+ + \ldots = A_1.\end{aligned}$$

Put $A_2 = A_1 - (\mathbb{1}+A_1)A_0$. Then the above computation implies that $A_2^+ = A_1^+ - A_1 = 0$, so $A_2 \in \mathrm{Mat}_n(R_2)$. Moreover,

$$|A_2| \leq \frac{|A_0|}{1-|A_0|} + |A_0| \cdot (n + \frac{|A_0|}{1-|A_0|}) = \frac{|A_0|}{1-|A_0|}(n+1-(n-1)|A_0|) \leq \frac{|A_0|}{1-|A_0|}(n+1) < 1,$$

since $|A_0| < \frac{1}{n+2}$. For $i = 1, 2$ we have $\mathbb{1} + A_i \in \mathrm{GL}_n(R_i)$ by Lemma 2.4. Observe that $\mathbb{1} + A_2 = \mathbb{1} + A_1 - (\mathbb{1}+A_1)A_0 = (\mathbb{1}+A_1)(\mathbb{1}-A_0)$ and let $B_2 = \mathbb{1}+A_2$, $B_1 = (\mathbb{1}+A_1)^{-1}$. Then $B_2 = B_1^{-1}AD$, so $D \in \mathrm{GL}_n(\mathbb{C}(z))$ and $A = B_1B_2C$ with $C = D^{-1}$. □

Remark 2.6. The rings $\mathcal{W}_I$ may be seen as a variant of the classical *Wiener algebra* of absolutely convergent Fourier series. They play a role analogous to that of Tate algebras in patching over non-archimedean fields. The construction of the latter rings uses the uniform norm for functions on certain sets. However, it appears that working with the uniform norm over $\mathbb{C}$ as well does not work: It is unclear to the authors whether any of the rings so obtained satisfy the essential properties of the rings $\mathcal{W}_I$ established in this section; some of them obviously do not, for example if the mentioned sets chosen are as in [HV96], see also [GF74, p. 30] for further obstructions.

3. Patching of Galois groups

In this section we show how to "patch" certain Galois extensions of $E := \mathbb{C}(z)$.

Definition 3.1. Let $\emptyset \neq D \subseteq \hat{\mathbb{C}}$ be a domain and F a finite extension of E which is a subfield of $\mathcal{M}(D)$. We say that F/E is **analytic over** D if it is Galois and there exists a primitive element f for F/E such that its $\mathrm{Gal}(F/E)$-conjugates $f_1, \ldots, f_n$, as well as $(f_\nu - f_\mu)^{-1}$, $1 \leq \nu < \mu \leq n$, belong to $\mathcal{H}(D)$. We say that a finite group G is **analytically realizable** if there exists an analytic extension of E over some domain D with Galois group isomorphic to G.

Example 3.2. Every finite *cyclic* group is analytically realizable. Indeed, let n be a positive integer, let $f(z) \in \mathcal{H}_{[0,1)}$ be an n-th root of $z-1$, and let $F = \mathbb{C}(z, f)$. Since f has no zero in the open unit disc, also $f^{-1} \in \mathcal{H}_{[0,1)}$. Since the polynomial

$$p(T) = T^n - (z-1) = \prod_{k=1}^{n} (T - e^{\frac{2\pi i k}{n}} f) \in \mathbb{C}[z][T]$$

completely decomposes over $\mathbb{C}(z, f)$, the extension $\mathbb{C}(z, f)/\mathbb{C}(z)$ is Galois. By Eisenstein's criterion applied to the prime element $z - 1 \in \mathbb{C}[z]$, p is irreducible over $\mathbb{C}(z)$, hence $\mathrm{Gal}(\mathbb{C}(z, f)/\mathbb{C}(z)) \cong \mathbb{Z}/n\mathbb{Z}$ and the conjugates of f are $f_\nu = e^{\frac{2\pi i \nu}{n}} f$, $\nu = 1, \ldots, n$. Thus,

both $f_1, \dots, f_n$ and $(f_\nu - f_\mu)^{-1} = (e^{\frac{2\pi i\nu}{n}} - e^{\frac{2\pi i\mu}{n}})^{-1} f^{-1}$ are in $\mathcal{H}_{[0,1)}$, so $\mathbb{C}(z, f)$ is analytic over the open unit disc.

Lemma 3.3. *If $F = E(f)$ is analytic over D, and $\varphi = \frac{az+b}{cz+d} \in \mathbb{C}(z)$ is a Möbius transformation, then $F' = E(f \circ \varphi)$ is analytic over $\varphi^{-1}(D)$, and* $\mathrm{Gal}(F/E) \cong \mathrm{Gal}(F'/E)$.

Proof. The composition $g \mapsto g \circ \varphi$ induces an isomorphism $\varphi^* \colon \mathcal{M}(D) \to \mathcal{M}(\varphi^{-1}(D))$ which maps $\mathbb{C}(z)$ onto $\mathbb{C}(\varphi(z))$ and $\mathbb{C}(z, f)$ onto $\mathbb{C}(\varphi(z), f(\varphi(z)))$. Since it maps rational functions onto rational functions, and the same holds for φ^{-1}, it follows that $\mathbb{C}(\varphi(z)) = \mathbb{C}(z)$. Thus, φ^* maps F/E onto F'/E. Since $\varphi^*(\mathcal{H}(D)) = \mathcal{H}(\varphi^{-1}(D))$, F' is analytic over $\varphi^{-1}(D)$. □

Remark 3.4. Since any domain contains a disc and all open discs $D \subseteq \hat{\mathbb{C}}$ are isomorphic to each other, Lemma 3.3 implies that every group G that is analytically realizable is realized by a suitable analytic extension F/E over any open disc, for example $A_{[0,2r_2)}$, where $r_2 > 0$. By Lemma 2.3(e), $\mathcal{H}_{[0,2r_2)} \subseteq \mathcal{W}_{[0,r_2)}$, so there exists a primitive element f for F/E such that all conjugates $f_1, \dots, f_n$ of f, as well as the $(f_\nu - f_\mu)^{-1}$, belong to $\mathcal{W}_{[0,r_2)}$.

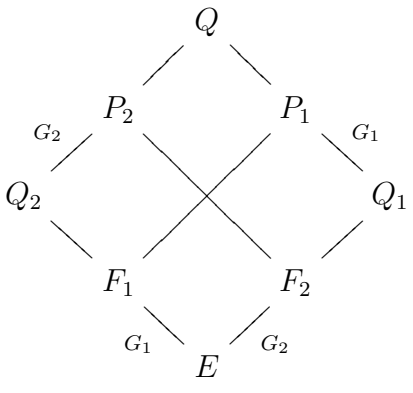
The induction step in our proof of the inverse Galois problem over $\mathbb{C}(z)$ is given by the following proposition:

Proposition 3.5 (Patching)**.** *Let G be a finite group, generated by subgroups G_1, G_2. If both G_1 and G_2 are analytically realizable, then so is G.*

Before proving this proposition, we need some additional constructions and lemmas. Fix $0 < r_1 < r_2 < \infty$ and write $R = \mathcal{W}_{(r_1,r_2)}$, $R_1 = \mathcal{W}_{[0,r_2)}$, $R_2 = \mathcal{W}_{(r_1,\infty]}$, as in the previous section. Put $Q = \mathrm{Quot}(R)$, $Q_1 = \mathrm{Quot}(R_1)$, $Q_2 = \mathrm{Quot}(R_2)$. As $R_1, R_2 \subseteq R$, we have $Q_1, Q_2 \subseteq Q$. Let F_1, F_2 be analytic extensions of E with Galois groups G_1, G_2, respectively. By Remark 3.4 we may assume that F_1 is analytic over $A_{(\frac{1}{2}r_1,\infty]}$ and F_2 is analytic over $A_{[0,2r_2)}$. In particular, $F_1 \subseteq Q_2$ and $F_2 \subseteq Q_1$. By Lemma 2.3(d)

$$Q_1 \cap Q_2 = E, \tag{1}$$

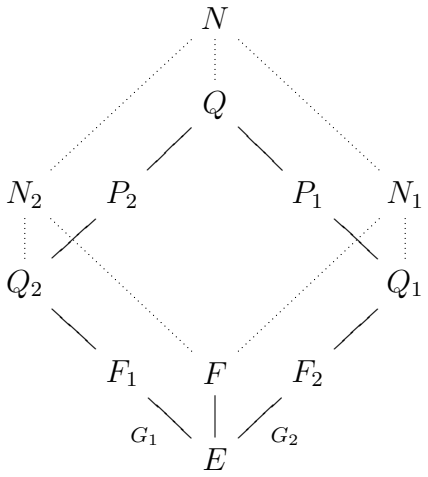
hence for $i = 1, 2$ we have $F_i \cap Q_i = E$. Let $P_i = F_i Q_i$ be the compositum of F_i and Q_i inside Q. Since F_i/E is Galois with group G_i and $F_i \cap Q_i = E$, we deduce that also P_i/Q_i is Galois and we may identify its Galois group with G_i by restriction to F_i.



Let $n = |G|$ be the order of G and consider the commutative Q-algebra $N = Q^n$ with Q embedded diagonally. We label the standard basis $\mathcal{S}$ of N by the elements of G, and thus write $\mathcal{S} = (g \mid g \in G)$ and $N = \{\sum_{g\in G} a_g g \mid a_g \in Q\}$. Let G act on N by $(\sum_g a_g g)^\sigma = \sum_g a_g(\sigma^{-1}g) = \sum_g a_{\sigma g} g$, $\sigma \in G$. Clearly, the fixed ring N^G is Q, where we view Q as a subring of N via the mentioned diagonal embedding. For each $i = 1, 2$ consider the Q_i-subalgebra

$$N_i = \left\{ \sum_{g\in G} a_g g \in N \;\middle|\; a_g \in P_i,\ a_g^\tau = a_{g\tau},\ \text{for all } g \in G,\ \tau \in G_i \right\} \tag{2}$$

of N. Put $F = N_1 \cap N_2$.



Lemma 3.6. *For $i = 1, 2$, the Q_i-algebra N_i is G-invariant and $N_i^G = Q_i$.*

Proof. Let $\sum_{g\in G} a_g g \in N_i$ and $\sigma \in G$. Then $a_g^\tau = a_{g\tau}$ for all $g \in G$ and $\tau \in G_i$, so $a_{\sigma g}^\tau = a_{\sigma g\tau}$. Hence $(\sum_{g\in G} a_g g)^\sigma = \sum_{g\in G} a_{\sigma g} g \in N_i$, so N_i is G-invariant. Furthermore, $N_i^G = N_i \cap N^G = N_i \cap Q \supseteq Q_i$, by (2). If $\sum_{g\in G} ag$ is an element of $N_i \cap Q$, then $a \in P_i$ and (in particular) $a^h = a$ for all $h \in G_i$, thus $a \in P_i^{G_i} = Q_i$. We deduce that $N_i^G = Q_i$. □

Lemma 3.7. *For $i = 1, 2$, there exists a basis $\mathcal{C}_i$ for N over Q, contained in N_i, such that the transition matrix from $\mathcal{S}$ to $\mathcal{C}_i$ lies in $\mathrm{GL}_n(R)$.*

Proof. Let $\tau_1, \ldots, \tau_r$ be an enumeration of the elements of G_i and let $\omega_1, \ldots, \omega_m$ be a system of representatives for G/G_i. (Thus $n = |G| = mr$.) By our assumptions, there exists a primitive element f for F_i/E, such that its conjugates $f_1 = f^{\tau_1}, \ldots, f_r = f^{\tau_r}$ belong to R (since R contains both R_1, R_2), and moreover $d := \prod_{\nu<\mu}(f_\nu - f_\mu)$ is invertible in R. Consider the following n-tuple of elements of N_i

$$\mathcal{C}_i = \left(\sum_{\nu=1}^{r} f_\nu^{\mu-1} \cdot \omega_k \tau_\nu \;\middle|\; 1 \le k \le m,\ 1 \le \mu \le r \right)$$

and let A_i be the transition matrix from $\mathcal{S}$ to $\mathcal{C}_i$ (with respect to any fixed ordering of $\mathcal{S}$ and $\mathcal{C}_i$), i.e. $\mathcal{C}_i = \mathcal{S}A_i$.

By direct computation, A_i consists, up to a permutation of the rows and columns (that depends on the chosen ordering of $\mathcal{S}$ and $\mathcal{C}_i$), of m block matrices on the diagonal, each

being the Vandermonde matrix $(f_\nu^{\mu-1})_{\nu,\mu=1,\dots,r}$. By our assumptions, $A_i \in \mathrm{Mat}_n(R)$, and $\det(A_i) = \pm d^m$ is invertible in R. Therefore $A_i \in \mathrm{GL}_n(R) \subseteq \mathrm{GL}_n(Q)$, and in particular $\mathcal{C}_i$ is a basis for N over Q. □

Lemma 3.8. *The intersection $F = N_1 \cap N_2$ is a field.*

Proof. The definition (2) of N_i gives an explicit presentation of F as

$$F = \left\{ \sum_{g\in G} a_g g \in N \;\middle|\; a_g \in P_1 \cap P_2,\ a_{g\tau} = a_g^\tau \text{ for all } g \in G \text{ and } \tau \in G_1 \cup G_2 \right\}.$$

It follows that if $\alpha = \sum_{g\in G} a_g g \in F$ is such that $a_g \neq 0$ for some $g \in G$ then $a_{g'} \neq 0$ for all $g' \in G$. Indeed, since $G = \langle G_1, G_2 \rangle$, we have $g' = g\tau_1\tau_2 \dots \tau_l$, where $\tau_1, \dots, \tau_l \in G_1 \cup G_2$. Now $a_{g'} = a_{g\tau_1\tau_2\dots\tau_l} = a^{\tau_l}_{g\tau_1\dots\tau_{l-1}} = \dots = a_g^{\tau_1\cdots\tau_l} \neq 0$ (since the τ_i are automorphisms). Thus if $\alpha \neq 0$ then $a_g \neq 0$ for all g, and so $\beta = \sum_{g\in G} a_g^{-1} g$ is a multiplicative inverse of α which clearly lies in F. □

Note that since $E \subseteq Q_1, Q_2$, the intersection F is an E-algebra, that is, F/E is a field extension. We conclude the proof of Proposition 3.5 by showing that F/E is Galois with group G:

Proof of Proposition 3.5. For $i = 1, 2$ let $\mathcal{C}_i$ be the basis given by Lemma 3.7, and let $A_i \in \mathrm{GL}_n(R)$ be the transition matrix from $\mathcal{S}$ to $\mathcal{C}_i$, so that $\mathcal{C}_i = \mathcal{S}A_i$. By Proposition 2.5 applied to $A_1^{-1}A_2 \in \mathrm{GL}_n(R)$ there exist $B_i \in \mathrm{GL}_n(R_i), i = 1, 2$ and $C \in \mathrm{GL}_n(E)$ such that $A_1^{-1}A_2 = B_1B_2C$. Put

$$\mathcal{C} = \mathcal{C}_1B_1 = \mathcal{S}A_1B_1 = \mathcal{S}A_2C^{-1}B_2^{-1} = \mathcal{C}_2(C^{-1}B_2^{-1}).$$

Since $B_1 \in \mathrm{GL}_n(R_1) \subseteq \mathrm{GL}_n(Q_1)$ and $C^{-1}B_2^{-1} \in \mathrm{GL}_n(E) \cdot \mathrm{GL}_n(R_2) \subseteq \mathrm{GL}_n(Q_2)$ we get that the basis $\mathcal{C}$ for N/Q is contained in $N_1 \cap N_2 = F$.

By Lemma 3.6, $F = N_1 \cap N_2$ is G-invariant and $F^G = N_1^G \cap N_2^G = Q_1 \cap Q_2 = E$, by (1). Since $\mathcal{C}$ consists of n elements that are linearly independent over $E \subseteq Q$, we see that $[F : E] \geq n = |G|$. By Artin's Lemma in basic Galois theory [Lan02, VI Thm. 1.8], F/F^G is Galois and its Galois group is a quotient of G. Thus, $[F : E] = n$ and $\mathrm{Gal}(F/E) \cong G$.

Let $\phi\colon N \to Q$ be the homomorphism of Q-algebras $\sum_g a_g g \mapsto a_1$. Since F is a field, ϕ maps F onto a subfield F' of Q. Since ϕ maps E identically onto E (recall that $E \subseteq Q$ embeds into N diagonally), F'/E is Galois with group isomorphic to G. Finally, choose a primitive element $f \in Q$ for F'/E. Then all the conjugates $f_1, \dots, f_n$ of f over E, as well $(f_\nu - f_\mu)^{-1}$, $\nu < \mu$, belong to $Q = \mathrm{Quot}(R)$. In particular, they are quotients of elements of $R = \mathcal{H}_{(r_1,r_2)}$, and hence are meromorphic functions on $A_{(r_1,r_2)}$. Thus, F' is analytic over some domain $D \subseteq A_{(r_1,r_2)}$. □

We can now easily solve the inverse Galois problem over $\mathbb{C}(z)$:

Theorem 3.9. *Every finite group G is analytically realizable.*

Proof. We prove the theorem by induction on the minimal number d of generators of $G = \langle g_1, \ldots, g_d \rangle$.

If $d = 1$, then G is cyclic, so the claim follows from Example 3.2.

If $d > 1$, then $G_1 = \langle g_1 \rangle$ and $G_2 = \langle g_2, \ldots, g_d \rangle$ are generated by 1 resp. $d-1$ elements, hence by the induction hypothesis, G_1 and G_2 are analytically realizable. By Proposition 3.5, so is $G = \langle G_1, G_2 \rangle$. □

Acknowledgements

The authors wish to thank Nir Lev for interesting discussions on the Wiener algebra.

This research was supported by the Israel Science Foundation (grant No. 696/13), by the Deutsche Forschungsgemeinschaft, and by the Minerva Minkowski Center for Geometry at Tel Aviv University. The first and the third author were supported by short-term research grants of the Minerva Foundation of the Max-Planck Society.

References

[BS06] A. Böttcher and B. Silbermann. *Analysis of Toeplitz Operators*. Second Edition. Springer, 2006.

[DD99] P. Dèbes and B. Deschamps. The regular inverse Galois problem over large fields. In L. Schneps and P. Lochak (eds.), *Geometric Galois actions, vol. 2*, London Math. Soc., Lec. Note Ser. **243**, pp. 119–138. Cambridge University Press, 1999.

[GF74] I. C. Gohberg and I. A. Fel'dman. *Convolution Equations and Projection Methods for Their Solution*. Transl. Math. Monogr., vol. 41. Amer. Math. Soc., 1974.

[HJ98] D. Haran and M. Jarden. Regular split embedding problems over complete valued fields. *Forum Math.*, 10:329–351, 1998.

[HV96] D. Haran and H. Völklein. Galois groups over complete valued fields. *Israel J. Math.*, 93:9–27, 1996.

[Har87] D. Harbater. Galois coverings of the arithmetic line. In: *Number Theory*. Lecture Notes in Math., Volume 1240, pp. 165–195. Springer, 1987.

[Har03] D. Harbater. Patching and Galois theory. In L. Schneps (ed.), *Galois groups and fundamental groups*, volume 41 of *MSRI Publications*, pp. 313–424. Cambridge University Press, 2003.

[HH10] D. Harbater and J. Hartmann. Patching over fields. *Israel J. Math.*, 176(1):61–107, 2010.

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

[Lam09] K. Lamotke. Riemannsche Flächen. Second Edition. Springer, 2009.

[Lan02] S. Lang. *Algebra*. Third edition. Springer, 2002.

[Liu95] Q. Liu. Tout groupe fini est une groupe de Galois sur $\mathbb{Q}_p(T)$, d'après Harbater. In M. D. Fried (ed.), *Recent developments in the inverse Galois problem*, volume 186 of *Contemp. Math.*, pp. 261–265. Amer. Math. Soc., 1995.

[Ser92] J.-P. Serre. *Topics in Galois theory*. Jones and Bartlett, 1992.

[Voe96] H. Völklein. *Groups as Galois groups: an Introduction*. Cambridge University Press, 1996.

Institut für Algebra, Fakultät Mathematik, Technische Universität Dresden
Email address: arno.fehm@tu-dresden.de

Raymond and Beverly School of Mathematical Sciences, Tel Aviv University
Email address: haran@tauex.tau.ac.il

Department of Mathematics, Open University of Israel
Email address: paran@openu.ac.il