Springer Monographs in Mathematics

Dan Haran
Moshe Jarden

The Absolute Galois Group of a Semi-Local Field

Springer

Springer Monographs in Mathematics

This series publishes advanced monographs giving well-written presentations of the "state-of-the-art" in fields of mathematical research that have acquired the maturity needed for such a treatment. They are sufficiently self-contained to be accessible to more than just the intimate specialists of the subject, and sufficiently comprehensive to remain valuable references for many years. Besides the current state of knowledge in its field, an SMM volume should ideally describe its relevance to and interaction with neighbouring fields of mathematics, and give pointers to future directions of research.

More information about this series at http://www.springer.com/series/3733

Dan Haran · Moshe Jarden

The Absolute Galois Group of a Semi-Local Field

Springer

Dan Haran
School of Mathematics
Tel Aviv University
Tel Aviv, Israel

Moshe Jarden
School of Mathematics
Tel Aviv University
Tel Aviv, Israel

ISSN 1439-7382 ISSN 2196-9922 (electronic)
Springer Monographs in Mathematics
ISBN 978-3-030-89190-9 ISBN 978-3-030-89191-6 (eBook)
https://doi.org/10.1007/978-3-030-89191-6

Mathematics Subject Classification: 12E30, 12-02, 12F12, 20E06, 20E18

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

In Erinnerung an Wulf-Dieter Geyer
(1939–2019)

Introduction

The main result of [HJP12], which is Theorem A below, describes the absolute Galois group of distinguished semi-local algebraic extensions of $\mathbb{Q}$ (among others) as free products of $\hat{F}_\omega$ and local Galois groups. The proof of Theorem A depends on two results of Florian Pop from [Pop96] and on the main result of [Pop95].

The aim of this monograph is to work out proofs of the above mentioned result of [HJP12] along with the supporting results of Pop. In addition we follow Melnikov's construction in [Mel90] of free products of profinite groups. Finally, we generalize the theory of free products of profinite groups and their subgroups developed in [Har87], and present results appearing in [HJP05] needed in the proofs.

Absolute Galois groups

Our result is an instance of a positive answer to the generalized inverse problem of Galois theory. Originally, this problem asked whether every finite group occurs as a Galois group of a Galois extension of $\mathbb{Q}$. For many groups this is the case [MaM99], but the general case is still wide open.

One way to realize a finite group over $\mathbb{Q}$ is to do it in pieces. That is, one has to properly solve finite embedding problems over $\mathbb{Q}$. Again, there are many examples of such problems which are properly solvable [MaM99]. But we do not have a characterization of all finite embedding problems over $\mathbb{Q}$ that are properly solvable. In particular, the structure of the absolute Galois group $\mathrm{Gal}(\mathbb{Q})$ of $\mathbb{Q}$ is unknown.

Still, there are several families of fields with known absolute Galois groups. The most renowned example of a field with this property is $\mathbb{C}(t)$, with t transcendental over $\mathbb{C}$, or, more generally, finite extensions of $\mathbb{C}(t)$. The Riemann Existence Theorem [Voe96, p. 37, Thm. 2.13] implies that $\mathrm{Gal}(\mathbb{C}(t))$ is the free profinite group on $2^{\aleph_0}$ generators ([Rib70, p. 70, Thm. 8.1]). An analogous result holds for an arbitrary algebraically closed field of characteristic 0. Various "patching methods" give similar results in the case where K is algebraically closed of positive characteristic (see [Hrb95], [Pop96], or [Jar11]).

By definition, the absolute Galois group of a field K is trivial if K is algebraically closed or, more generally, separably closed.

More subtle is the case where K is the field $\mathbb{R}$ of real numbers or, more generally, real closed. In this case, $\mathrm{Gal}(K)$ is isomorphic to the group with two elements [Lan93, p. 452, Thm. 2.2].

Much more difficult is the case where K is a finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$ for some prime number p. In both cases K is complete with respect to a discrete valuation and $\mathrm{Gal}(K) = T \ltimes W$ is the semi-direct product of its "maximal tame quotient" T and its "wild part" W (Lemma 8.2.2). By Iwasawa, the tame group T is generated by two elements σ, τ satisfying the relation $\sigma\tau\sigma^{-1} = \tau^q$. The wild group W is a free pro-p group of rank $\aleph_0$.

For the exact structure of $\mathrm{Gal}(K)$ by generators, relations, and "conditions" we refer the reader to [NSW20, p. 418, Thm. 7.5.13] in the case where $\mathrm{char}(K) = p$ due to Helmut Koch [Koc67] and to [NSW20, p. 419, Thm. 7.5.14] for $\mathrm{char}(K) = 0$ and $p \neq 2$ due to Uwe Jannsen and Kay Wingberg [JaW82]. The case where $\mathrm{char}(K) = 0$ and $p = 2$ was treated by Volker Diekert under the condition that $K(\sqrt{-1})/K$ is unramified. See [NSW20, p. 431] or [Die84].

The field $K_{\mathrm{tot},S}$

From our point of view, more important than the fields $\mathbb{Q}_p$ and $\mathbb{F}_q((t))$ are their algebraic parts. We consider a *classically local prime* $\mathfrak{p}$ of a field K. Thus, the "completion" $\hat{K}_\mathfrak{p}$ of K with respect to $\mathfrak{p}$ is either a finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_q((t))$, where p is a prime number and q is a power of a prime number, or $\hat{K}_\mathfrak{p} = \mathbb{R}$. Then, the algebraic part $K_\mathfrak{p} = K_{\mathrm{sep}} \cap \hat{K}_\mathfrak{p}$ of $\hat{K}_\mathfrak{p}$ is the Henselian (respectively, real) closure of K with respect to $\mathfrak{p}$. This closure is uniquely defined up to K-isomorphism. By a lemma of Krasner (in the Henselian case), $\mathrm{Gal}(K_\mathfrak{p})$ is isomorphic to $\mathrm{Gal}(\hat{K}_\mathfrak{p})$, so whatever information we have on $\mathrm{Gal}(\hat{K}_\mathfrak{p})$ applies also to $\mathrm{Gal}(K_\mathfrak{p})$.

This allows us to consider a finite set S of classically local primes of K and set $K_{\mathrm{tot},S} = \bigcap_{\mathfrak{p}\in S} \bigcap_{\rho\in\mathrm{Gal}(K)} K_\mathfrak{p}^\rho$. By [Pop96, Thm. 3],

$$\mathrm{Gal}(K_{\mathrm{tot},S}) \cong \mathop{\ast\!\!\prod}_{\mathfrak{p}\in S} \mathop{\ast\!\!\prod}_{\rho\in R_\mathfrak{p}} \mathrm{Gal}(K_\mathfrak{p})^\rho.$$

Here, $\mathop{\ast\!\!\prod}_{\rho\in R_\mathfrak{p}} \mathrm{Gal}(K_\mathfrak{p})^\rho$ stands for the free product of the profinite groups $\mathrm{Gal}(K_\mathfrak{p})^\rho$ (Definition 4.1.1), while $\mathop{\ast\!\!\prod}_{\mathfrak{p}\in S}$ denotes the free product of finitely many profinite groups following the operator.

We refer to the fields $K_{\mathrm{tot},S}$ as fields of "semi-local type".

The fields $K_{\mathrm{sep}}(\sigma)$ and $K_{\mathrm{sep}}[\sigma]$

Next we consider fields of another type, "with no arithmetic". Basic Galois theory shows that the absolute Galois group of a finite field K is isomorphic to $\hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}$ [FrJ08, p. 15, Sec. 1.5]. It is not difficult to show that the latter property extends to non-principal ultra products [FrJ08, p. 141, Sec. 7.7] of finite fields. If F is a field of this type and $\mathrm{char}(F) = 0$, then $\mathrm{Gal}(F \cap \tilde{\mathbb{Q}})$ is *procyclic*. Thus, there exists a $\sigma \in \mathrm{Gal}(\mathbb{Q})$ such that $F \cap \tilde{\mathbb{Q}}$ is the fixed field $\tilde{\mathbb{Q}}(\sigma)$ of σ in $\tilde{\mathbb{Q}}$. Conversely, for each $\sigma \in \mathrm{Gal}(\mathbb{Q})$ there exists a non-principal ultraproduct F of finite fields such that $\tilde{\mathbb{Q}}(\sigma) = F \cap \tilde{\mathbb{Q}}$ [Ax67, Thm. 5].

Note that for an arbitrary $\sigma \in \mathrm{Gal}(\mathbb{Q})$ it may happen that $\mathrm{Gal}(\tilde{\mathbb{Q}}(\sigma))$ is not isomorphic to $\hat{\mathbb{Z}}$. For example, this is the case if $\sigma = 1$ or σ is an involution. However, $\mathrm{Gal}(\tilde{\mathbb{Q}}(\sigma)) \cong \hat{\mathbb{Z}}$ for *almost all* $\sigma \in \mathrm{Gal}(\mathbb{Q})$ in the sense of the Haar measure of $\mathrm{Gal}(\mathbb{Q})$ [Ax67, Prop. 3].

The proof of the latter result uses the theory of cyclotomic extensions of $\mathbb{Q}$. An alternative proof of this theorem applies Hilbert's irreducibility theorem for $\mathbb{Q}$, hence it holds for every Hilbertian field K. Moreover, the following result holds for every positive integer e and for almost all $\boldsymbol{\sigma} := (\sigma_1, \dots, \sigma_e) \in \mathrm{Gal}(K)^e$: the group $\mathrm{Gal}(K_{\mathrm{sep}}(\boldsymbol{\sigma}))$ is isomorphic to the free profinite group $\hat{F}_e$ on e generators [FrJ08, p. 379, Thm. 18.5.6]. If K is also countable, then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ is, in addition, *PAC* [FrJ08, p. 380, Thm. 18.6.1]. This means that every geometrically integral variety over $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ has a $K_{\mathrm{sep}}(\boldsymbol{\sigma})$-rational point.

The latter property implies that the Henselian closures (and the real closures) of almost all fields $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ are separably closed (a result of Frey–Prestel [FrJ08, p. 205, Cor. 11.5.5]). In this sense, these fields "lack arithmetic".

Digging further down, we denote the maximal Galois extension of K in $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ by $K_{\mathrm{sep}}[\boldsymbol{\sigma}]$. Under the latter assumptions on K and e, [FrJ08, p. 669, Thm. 27.4.8] asserts that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $K_{\mathrm{sep}}[\boldsymbol{\sigma}]$ is PAC, the group $\mathrm{Gal}(K_{\mathrm{sep}}[\boldsymbol{\sigma}])$ is isomorphic to the free profinite group $\hat{F}_\omega$ on countably many generators, and $K_{\mathrm{sep}}[\boldsymbol{\sigma}]$ is Hilbertian.

The fields $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$

As above, we consider a countable Hilbertian field K, a finite set S of classically local primes of K, and a positive integer e. Given $\boldsymbol{\sigma} := (\sigma_1, \dots, \sigma_e) \in \mathrm{Gal}(K)^e$, we consider the fields $K_{\mathrm{tot},S}(\boldsymbol{\sigma}) = K_{\mathrm{tot},S} \cap K_{\mathrm{sep}}(\boldsymbol{\sigma})$ and $K_{\mathrm{tot},S}[\boldsymbol{\sigma}] = K_{\mathrm{tot},S} \cap K_{\mathrm{sep}}[\boldsymbol{\sigma}]$ of "mixed type".

Our goal is to reproduce the description of $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}])$ as it appears in [HJP12, Thm. 3.11] along with all supporting results from [Pop96], [Pop95], [Mel90], and [Har87].

The main result

The main result of this monograph strengthens the main result of [HJP12].

Theorem A (Theorem 9.1.6) *Let K be a countable Hilbertian field, S a finite set of classically local primes of K, and e a positive integer. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is Hilbertian,* PSC*, and ample. Moreover, for* *each* $\mathfrak{p} \in S$ *there exists a closed subset* $R_\mathfrak{p}$ *of* $\mathrm{Gal}(K)$ *such that* $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) \cong \hat{F}_\omega * \prod^*_{\mathfrak{p}\in S} \prod^*_{\rho\in R_\mathfrak{p}} \mathrm{Gal}(K_\mathfrak{p})^\rho$.

Here an extension M of K in $K_{\mathrm{tot},S}$ is said to be PSC if every geometrically integral curve Γ over M with a simple $K_\mathfrak{p}^\rho$-point for each $\mathfrak{p} \in S$ and every $\rho \in \mathrm{Gal}(K)$ has infinitely many M-rational points. Also, one says that M is *ample* if every geometrically integral curve over M with a simple M-rational point has infinitely many M-rational points [Jar11, p. 68, Def. 5.3.2].

The Hilbertianity of $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ follows from [BSF13, Thm. 1.1]. By [GeJ02], $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is PSC for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. This implies that M is ample [Pop96, Prop. 3.1].

Remark B The free factor $C := \prod^*_{\mathfrak{p}\in S} \prod^*_{\rho\in R_\mathfrak{p}} \mathrm{Gal}(K_\mathfrak{p})^\rho$ appearing in Theorem A depends (up to isomorphism) only on K and S but not on the choice of the fields $K_\mathfrak{p}$ nor on $\boldsymbol{\sigma}$. In particular, this factor is isomorphic to $\mathrm{Gal}(K_{\mathrm{tot},S})$ (Remark 9.2.4).

We call C a *Cantor free product over* S, because each of the spaces $R_\mathfrak{p}$ is homeomorphic to the Cantor middle-third set (Section 1.5).

Using the group-theoretic Lemma 4.7.5, Theorem A yields the following corollary.

Corollary C (Remark 9.2.4 and Lemma 9.2.1) *Let K be a countable Hilbertian field, S a finite set of classically local primes of K, and e a non-negative integer. Then, for almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ *and for each* $\mathfrak{p} \in S$ *there exists a closed subset* $R_\mathfrak{p}$ *of* $\mathrm{Gal}(K)$ *such that*

$$\mathrm{Gal}(K_{\mathrm{tot},S}(\boldsymbol{\sigma})) \cong \hat{F}_e * \prod^*_{\mathfrak{p}\in S} \prod^*_{\rho\in R_\mathfrak{p}} \mathrm{Gal}(K_\mathfrak{p})^\rho.$$

Remark D If S is an empty set, then $C = \mathbf{1}$. Thus, in this case, Corollary C and Theorem A say that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ we have $\mathrm{Gal}(K_{\mathrm{sep}}(\boldsymbol{\sigma})) \cong \hat{F}_e$ and $\mathrm{Gal}(K_{\mathrm{sep}}[\boldsymbol{\sigma}]) \cong \hat{F}_\omega$, as mentioned in the Subsection "The fields $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ and $K_{\mathrm{sep}}[\boldsymbol{\sigma}]$".

A result of Pop

The proof of Theorem A depends on [Pop96, Thm. 2.8]:

Proposition E (The fundamental result, Proposition 8.4.3) *Let S be a finite set of classically local primes of a countable Hilbertian field K. Consider an infinite extension M of K in $K_{\mathrm{tot},S}$ which is ample and Hilbertian. Suppose that* $\mathrm{Gal}(M)$ *is* $\mathcal{G}_{K,S}$*-projective. Then,* $\mathcal{G}_{K,S} = \mathcal{G}_{K,S,\max}$ *and* $\mathcal{G}_{K,S}$ *has an étale profinite system* $\mathcal{R}$ *of representatives for its* $\mathrm{Gal}(M)$*-orbits such that* $\mathrm{Gal}(M) \cong \hat{F}_\omega * \prod^*_{\Gamma\in\mathcal{R}} \Gamma$.

Here, $\mathcal{G}_{K,S}$ is the set of all groups $\mathrm{Gal}(K_\mathfrak{p})^\rho$ with $\mathfrak{p} \in S$ and $\rho \in \mathrm{Gal}(K)$ and the symbol $\mathcal{G}_{K,S,\max}$ stands for the set of all maximal elements of $\mathcal{G}_{K,S}$.

We say that $\mathrm{Gal}(M)$ is $\mathcal{G}_{K,S}$*-projective* if every finite $\mathcal{G}_{K,S}$-embedding problem for $\mathrm{Gal}(M)$ is solvable:

Let G be a profinite group and let $\mathcal{G}$ be a subset of the set of all closed subgroups of G. A *finite $\mathcal{G}$-embedding problem* for G is a triple $(\varphi\colon G \to A,\ \alpha\colon B \to A,\ \mathcal{B})$, where $\alpha\colon B \to A$ is an epimorphism of finite groups, $\varphi\colon G \to A$ is a homomorphism of profinite groups, and $\mathcal{B}$ is a set of subgroups of B closed under B-conjugation and taking subgroups, such that for each $\Gamma \in \mathcal{G}$ there exists a homomorphism $\gamma_\Gamma\colon \Gamma \to B$ with $\alpha \circ \gamma_\Gamma = \varphi|_\Gamma$ and $\gamma_\Gamma(\Gamma) \in \mathcal{B}$. We say that a homomorphism $\gamma\colon G \to B$ is a *solution* if $\alpha \circ \gamma = \varphi$. The solution is *strong* if $\gamma(\Gamma) \in \mathcal{B}$ for each $\Gamma \in \mathcal{G}$. Finally, the embedding problem is *proper* if φ is surjective. In this case, a solution γ to the embedding problem is *proper* if γ is surjective.

We write $\mathrm{Subgr}(G)$ for the set of all closed subgroups of G and equip $\mathrm{Subgr}(G)$ with the *étale topology*. A base for this topology is the family of all open subgroups H of G. A subset $\mathcal{R}$ of $\mathrm{Subgr}(G)$ is said to be *étale profinite* if $\mathcal{R}$ is a profinite space under the induced étale topology of $\mathrm{Subgr}(G)$.

Another result of Pop

The proof of Proposition E depends on the following consequence of a variant of [Pop95, Thm. 3]:

Proposition F (Proposition 6.4.8) *Let G be a profinite group and let $\mathcal{G}$ be a subset of* $\mathrm{Subgr}(G)$ *of $\mathcal{P}$-type. Suppose that every finite $\mathcal{G}$-embedding problem for G has a proper solution.*

Then, every finite $\mathcal{G}$-embedding problem for G has a proper strong solution.

We do not repeat the definition of $\mathcal{P}$-type here and only mention that by Definition 6.4.5, $\mathcal{G}_{K,S}$ is of $\mathcal{P}$-type for every field K and every finite set S of classically local primes of K.

Supporting results

In order to prove Proposition E we also need, in addition to Proposition F, the following result.

Lemma G (Lemma 8.4.2) *Let M be an ample Hilbertian field and let $\mathcal{G}$ be a strictly closed* $\mathrm{Gal}(M)$*-invariant subset of* $\mathrm{Subgr}(M)$ *of $\mathcal{P}$-type. Suppose that* $\mathrm{Gal}(M)$ *is $\mathcal{G}$-projective. Then, every finite proper $\mathcal{G}$-embedding problem for* $\mathrm{Gal}(M)$ *has a proper strong solution.*

The proof of Lemma G uses the main Galois-theoretic property of ample fields: Every finite split embedding problem over $M(t)$ with M as in Lemma G and t transcendental over M is properly solvable (see [Pop96, Main Theorem B] or [Jar11, p. 89, Thm. 5.10.2]).

The group-theoretic assumption in Lemma G is satisfied if we assume a stronger field-theoretic assumption on M:

Lemma H (Lemma 8.3.5) *Let M be an infinite field and $\mathcal{X}$ a family of separable algebraic extensions of M. Suppose that $\mathcal{G} := \{\mathrm{Gal}(M')\}_{M' \in \mathcal{X}}$ is étale compact and M is* P$\mathcal{X}$C *(Definition 8.3.2). Then,* $\mathrm{Gal}(M)$ *is $\mathcal{G}$-projective.*

Generalized Iwasawa isomorphism theorem

In addition to results F and G, the proof of Proposition E uses the following generalization of Iwasawa isomorphism theorem [Pop96, Thm. 4.5]:

Proposition I (Proposition 7.2.2) *Let G and G' be profinite groups. Let $\mathcal{G}$ (resp. $\mathcal{G}'$) be a subset of* $\mathrm{Subgr}(G)$ *(resp* $\mathrm{Subgr}(G')$*) that satisfies the following conditions:*

(a) $\mathrm{rank}(G) \le \aleph_0$ *(resp.* $\mathrm{rank}(G') \le \aleph_0$*).*
(b) *$\mathcal{G}$ (resp. $\mathcal{G}'$) is an étale compact set of representatives of the distinct conjugacy classes in $(\mathcal{G}^G)_{\mathrm{max}}$.*
(c) *G (resp. G') is properly strongly $\mathcal{G}$-projective (resp. $\mathcal{G}'$-projective).*
(d) *There is a homeomorphism $\mu\colon \bigcup_{\Gamma\in\mathcal{G}} \Gamma \to \bigcup_{\Gamma'\in\mathcal{G}'} \Gamma'$ that satisfies the following condition: for every $\Gamma \in \mathcal{G}$ there is a $\Gamma' \in \mathcal{G}'$ such that $\mu|_\Gamma\colon \Gamma \to \Gamma'$ is an isomorphism of groups.*

Then, there is an isomorphism $\theta\colon G \to G'$ such that $\theta(\mathcal{G}^G) = (\mathcal{G}')^{G'}$.

Condition (b) in Proposition I is achieved by the following result.

Lemma J (Lemma 7.1.3) *Let G be a profinite group of rank $\le \aleph_0$ and let $\mathcal{G}$ be a G-invariant étale compact subset of* $\mathrm{Subgr}(G)$ *such that $\mathcal{G} = \mathcal{G}_{\mathrm{max}}$ and G is strongly $\mathcal{G}$-projective. Then, $\mathcal{G}$ has an étale compact subset of representatives for its G-orbits.*

Tel Aviv University *Dan Haran*
August 2021 *Moshe Jarden*

Contents