# The Absolute Galois Group of a $p$-adic Field

In Erinnerung an Jürgen Ritter (1943–2021)

Moshe Jarden, Tel Aviv University
jarden@tauex.tau.ac.il
and
Mark Shusterman, Harvard University
mshusterman@math.harvard.edu

10 January 2023

**Abstract**

We compute the number of generators and the number of relations needed to present the absolute Galois group of a given finite extension of $\mathbb{Q}_p$.

## 1 Introduction

Let $p$ be a prime number and $K$ a finite extension of $\mathbb{Q}_p$. Uwe Jannsen proved in [Jan82] that the absolute Galois group $\mathrm{Gal}(K)$ of $K$ is finitely generated (as a profinite group). The third paragraph of the introduction of [JaR91] provides another proof of Jannsen's result.

Our goal in this note is to prove that $\mathrm{Gal}(K)$ is even "finitely presented" and to compute the number of "generators" and "relations" needed for the "presentation". Here we say that an arbitrary profinite group $G$ is **finitely presented** if there exist a short exact sequence $\mathbf{1} \to N \to \hat{F}_e \to G \to \mathbf{1}$ for some positive integer $e$ and elements $y_1, \ldots, y_d \in \hat{F}_e$ such that $N$ is the smallest closed normal subgroup of the free profinite group $\hat{F}_e$ on $e$ generators that contains $y_1, \ldots, y_d$. The elements $y_1, \ldots, y_d$ are said to be **relations** of $G$.

Uwe Jannsen and Kay Wingberg give in [JaW82] an "explicit description" of $\mathrm{Gal}(K)$ for $p \neq 2$. Indeed, with $n = [K : \mathbb{Q}_p]$, the article [JaW82] gives generators $\sigma, \tau, x_0, \ldots, x_n$ satisfying two "tame relations" and the following condition:

(1) The closed normal subgroup $N$ of $\mathrm{Gal}(K)$ generated by $x_0, \ldots, x_n$ is a pro-$p$-group. {jawn}

Volker Diekert [Die84] proves an analogous result for $p = 2$ under the condition that $K(\sqrt{-1})/K$ is an unramified extension. In particular, Diekert's result does not cover the case $K = \mathbb{Q}_2$.

Theorem 1.1 states that the minimal number of generators of $\mathrm{Gal}(K)$ is $[K : \mathbb{Q}_p] + 2$ while Theorem 3.4 says that the minimal number of relations needed to define $\mathrm{Gal}(K)$ is $[K : \mathbb{Q}_p] + 1$.

A central tool in the proof of our results was initiated by Alexander Lubotzky (Section 2). The authors were inspired to apply that initiative in the present context by several recent works using the initiative to obtain a finite presentation for some other profinite groups in arithmetic geometry and algebraic number theory. Most notably, these are the papers [Shu18], [Liu20], and [ESV21].

For every prime number $\ell$, an explicit presentation for the maximal pro-$\ell$ quotient of $\mathrm{Gal}(K)$ is known from the works of Demushkin and Labute. The latter group is either free or a Demushkin group defined by a single explicit relation. We shall use this presentation for the case $\ell = p$ in order to obtain a lower bound on the rank of $\mathrm{Gal}(K)$ (see proof of Thm. 1.1).

**Remark 1.1.** Acknowledgment The authors are indebted to Aharon Razon for carefully reading drafts of this work.

The authors also thank the anonymous referee for useful comments and suggestions.

# 2 Number of Generators

{NGN}

Recall that the rank of a finitely generated profinite group $G$ is the minimal number of elements $x_1, \ldots, x_e$ of $G$ (called **generators**) such that $G$ is the minimal closed subgroup of itself containing $x_1, \ldots, x_e$. In this case, we write $\mathrm{rank}(G) := e$ [FrJ08, Sec. 16.10].

As mentioned in the introduction, the absolute Galois group of a finite extension $K$ of $\mathbb{Q}_p$ is finitely generated. It turns out that $\mathrm{rank}(\mathrm{Gal}(K))$ depends only on $[K : \mathbb{Q}_p]$.

Indeed, well known results imply that $\mathrm{rank}(\mathrm{Gal}(K))$ is either $[K : \mathbb{Q}_p] + 1$ or $[K : \mathbb{Q}_p] + 2$. This is pointed our in the proof of Theorem 1.1 below. The Theorem says that the later option holds.

{GNGa}

**Theorem 2.1.** *Let $p$ be a prime number and $K$ a finite extension of $\mathbb{Q}_p$. Then,* $\mathrm{rank}(\mathrm{Gal}(K)) = [K : \mathbb{Q}_p] + 2$.

*Proof.* Theorem 7.4.1 of [NSW20] says that $\mathrm{Gal}(K)$ is generated by $[K : \mathbb{Q}_p] + 2$ elements. By definition,

$$\mathrm{rank}(\mathrm{Gal}(K)) \leq [K : \mathbb{Q}_p] + 2. \tag{2}$$ {ngna}

Let $K^{(p)}$ be the maximal pro-$p$ extension of $K$. Thus, $K^{(p)}/K$ is a Galois extension and $\mathrm{Gal}(K^{(p)}/K)$ is the maximal pro-$p$ quotient of $\mathrm{Gal}(K)$. In particular, $\mathrm{rank}(\mathrm{Gal}(K)) \geq \mathrm{rank}(\mathrm{Gal}(K^{(p)}/K))$. Let $\zeta_p$ be a primitive root of unity of order $p$.

Case A: $\zeta_p \in K$. In this case, $\mathrm{Gal}(K^{(p)}/K)$ is a Demushkin group of rank $[K : \mathbb{Q}_p] + 2$ [NSW20, p. 416, Thm. 7.5.11(ii)] (see also [Koc70, p. 96, Satz 10.3] for the rank of $\mathrm{Gal}(K^{(p)}/K)$). Thus,

$$\mathrm{rank}(\mathrm{Gal}(K)) \geq \mathrm{rank}(\mathrm{Gal}(K^{(p)}/K)) = [K : \mathbb{Q}_p] + 2 \overset{(2)}{\geq} \mathrm{rank}(\mathrm{Gal}(K)),$$

so $\mathrm{rank}(\mathrm{Gal}(K)) = [K : \mathbb{Q}_p] + 2$.

Case B: $\zeta_p \notin K$. Then, $\mathrm{Gal}(K^{(p)}/K)$ is the free pro-$p$ group of rank $[K : \mathbb{Q}_p]+1$ [NSW20, p. 416, Thm. 7.5.11(i)] and the method used in Case A does not work.

However, we may apply Case A to the field $L := K(\zeta_p)$ and get

$$\mathrm{rank}(\mathrm{Gal}(L)) = [L : \mathbb{Q}_p] + 2. \tag{3}$$ {ngnc}

Assume toward contradiction that $\mathrm{rank}(\mathrm{Gal}(K)) \neq [K : \mathbb{Q}_p] + 2$. Then, by (2), $\mathrm{rank}(\mathrm{Gal}(K)) \leq [K : \mathbb{Q}_p] + 1$. Hence,

$$\begin{aligned} [L : \mathbb{Q}_p] + 2 \overset{(3)}{=} \mathrm{rank}(\mathrm{Gal}(L)) &\leq 1 + [L : K](\mathrm{rank}(\mathrm{Gal}(K)) - 1) && (4) \quad \{\texttt{ngnd}\} \\ &\leq 1 + [L : K][K : \mathbb{Q}_p] = 1 + [L : \mathbb{Q}_p], && (5) \end{aligned}$$

where the inequality in (4) is a special case of the Nielsen-Schreier inequality [FrJ08, p. 359, Cor. 17.6.3] applied to the open subgroup $\mathrm{Gal}(L)$ of $\mathrm{Gal}(K)$. Thus, $2 \leq 1$, which is a contradiction. □

# 3 Lubotzky's initiative

{LBI}

Again, let $K$ be a finite extension of $\mathbb{Q}_p$. We establish the finite presentation of $\mathrm{Gal}(K)$ in all cases but we do not attempt to give explicit generators and relations. The existence of the presentation is based on the following result of Alexander Lubotzky.

**Proposition 3.1.** *[Lub01, Thm. 0.3] A finitely generated profinite group $G$ is finitely presented if and only if there exists a constant $c$ such that for every prime number $\ell$, and every finite simple $\mathbb{F}_\ell[G]$-module $A$, we have* $\dim_{\mathbb{F}_\ell} \mathrm{H}^2(G, A) \leq c \cdot \dim_{\mathbb{F}_\ell} A$. {GEN1}

Another tool that we need is due to John Tate:

**Proposition 3.2.** *[NSW20, Thm. 7.3.1] Every finite* $\mathrm{Gal}(K)$*-module $A$ satisfies the following equality:* {GEN2}

$$\frac{\mathrm{card}(\mathrm{H}^0(\mathrm{Gal}(K), A)) \cdot \mathrm{card}(\mathrm{H}^2(\mathrm{Gal}(K), A))}{\mathrm{card}(\mathrm{H}^1(\mathrm{Gal}(K), A))} = ||\mathrm{card}(A)||_K. \tag{6}$$ {gen2}

Here, $\mathrm{card}(S)$ is the cardinality of a set $S$ and for each $a \in K$ we have $||a||_K := q^{-\mathrm{ord}_K(a)}$ [Neu99, p. 134], where $q$ is the cardinality of the residue field of $K$ and $\mathrm{ord}_K$ is the normalized valuation of $K$. If $a \in \mathbb{Q}_p$, in particular if $a = \mathrm{card}(A)$, then $\mathrm{ord}_K(a) = e(K/\mathbb{Q}_p)\mathrm{ord}_p(a)$, where $\mathrm{ord}_p$ is the usual $p$-adic valuation of $\mathbb{Q}_p$ and $e(K/\mathbb{Q}_p)$ is the ramification index of $K$ over $\mathbb{Q}_p$.

Moreover, $q = p^{f(K/\mathbb{Q}_p)}$, where $f(K/\mathbb{Q}_p)$ is the degree of the residue degree of $K$ over $\mathbb{Q}_p$. Since $e(K/\mathbb{Q}_p)f(K/\mathbb{Q}_p) = [K : \mathbb{Q}_p]$ [CaF67, p. 19, Prop. 3], we have $||a||_K = p^{-[K:\mathbb{Q}_p]\mathrm{ord}_p(a)}$. In particular,

$$||\mathrm{card}(A)||_K = p^{-[K:\mathbb{Q}_p]\mathrm{ord}_p(\mathrm{card}(A))}. \tag{7}$$ {hen2}

Finally, we need the following elementary result:

{GEN3}

**Lemma 3.3.** *Let $G$ be a profinite group with $e$ generators and $A$ a finite $G$-module. Then,* $\mathrm{card}(\mathrm{H}^1(G,A)) \leq \mathrm{card}(A)^e$.

*Thus, if $A$ is a finite $\mathbb{F}_\ell[G]$-module for a prime number $\ell$, then* $\dim_{\mathbb{F}_\ell}(\mathrm{H}^1(G,A)) \leq e \cdot \dim_{\mathbb{F}_\ell}(A)$.

*Proof.* By definition, $\mathrm{H}^1(G,A)$ is the quotient of the group $Z^1(G,A)$ of all crossed homomorphisms from $G$ to $A$ modulo the group of all principal crossed homomorphisms [Rib70, p. 97, Sec. II2]. Thus, it suffices to prove that $\mathrm{card}(Z^1(G,A)) \leq \mathrm{card}(A)^e$.

Indeed, by definition, each crossed homomorphism $\chi\colon G \to A$ is a continuous map that satisfies $\chi(\sigma\tau) = \chi(\sigma) - \sigma\chi(\tau)$ for all $\sigma, \tau \in G$ [Rib70, p. 97]. Hence, $\chi$ is determined by its values on a system of generators $\sigma_1, \ldots, \sigma_e$ of $G$, first on the discrete subgroup generated by $\sigma_1, \ldots, \sigma_e$ and then, by continuity, on $G$. This implies that the number of crossed homomorphisms of $G$ into $A$ is at most $\mathrm{card}(A)^e$, as claimed.

For the second part of the lemma note that if $A$ is a finite $\mathbb{F}_\ell[G]$-module, then $A$ is also a finite dimensional vector space over $\mathbb{F}_\ell$, so $\mathrm{card}(A) = \ell^{\dim(A)}$. Similarly, $\mathrm{card}(\mathrm{H}^1(G,A)) = \ell^{\dim(\mathrm{H}^1(G,A))}$. Taking the $\ell$-th logarithm on both sides of the already proved first inequality yields the second inequality. □

This brings us to our second main result.

{GEN4}

**Theorem 3.4.** *Let $K$ be a finite extension of $\mathbb{Q}_p$. Then,* $\mathrm{Gal}(K)$ *is finitely presented.*

*Proof.* By Theorem 1.1, $\mathrm{Gal}(K)$ is a finitely generated profinite group. Thus, by Proposition 2.1, it suffices to prove the existence of a constant $c$ such that for each prime number $\ell$ and every finite $\mathbb{F}_\ell[\mathrm{Gal}(K)]$-module $A$ we have

$$\dim_{\mathbb{F}_\ell}\mathrm{H}^2(\mathrm{Gal}(K),A) \leq c \cdot \dim_{\mathbb{F}_\ell} A.$$

If $\ell \neq p$, then $||\ell||_K = 1$, hence $||\mathrm{card}(A)||_K = 1$. As in the proof of Lemma 2.3, taking the $\ell$-th logarithm of (6) and using (7), gives

$$\begin{aligned}\dim_{\mathbb{F}_\ell}(\mathrm{H}^0(\mathrm{Gal}(K),A)) + \dim_{\mathbb{F}_\ell}(\mathrm{H}^2(\mathrm{Gal}(K),A)) \\ - \dim_{\mathbb{F}_\ell}(\mathrm{H}^1(\mathrm{Gal}(K),A)) = h(\ell),\end{aligned} \tag{8}$$

{gen4}

where

$$h(\ell) = 0 \text{ if } \ell \neq p \text{ and } h(\ell) = -[K:\mathbb{Q}_p]\dim_{\mathbb{F}_p}(A) \text{ if } \ell = p. \tag{9}$$

{gen5}

Thus, in each case $h(\ell) \leq 0$. The first summand on the left hand side of (8) is non-negative. Hence, $\dim_{\mathbb{F}_\ell}(\mathrm{H}^2(\mathrm{Gal}(K),A)) \leq \dim_{\mathbb{F}_\ell}(\mathrm{H}^1(\mathrm{Gal}(K),A))$. Denoting the number of generators of $\mathrm{Gal}(K)$ by $e$, we conclude from Lemma 2.3 that $\dim_{\mathbb{F}_l}(\mathrm{H}^2(\mathrm{Gal}(K),A)) \leq e \cdot \dim_{\mathbb{F}_l}(A)$. It follows from Proposition 2.1 that $\mathrm{Gal}(K)$ is finitely presented, as claimed. □

# 4 Number of Relations

We strengthen Theorem 2.4 with a simple formula for the number of relations of $\mathrm{Gal}(K)$, where $K$ is, as before, a finite extension of $\mathbb{Q}_p$. To this end we deduce from Hensel's lemma that if the residue field $\bar{K}$ of $K$ contains a root of unity of prime order $\ell \neq p$, then $K$ contains a root of unity of order $\ell$. Thus, the following lemma is a consequence of [CaF67, p. 32, Prop. 1].

{CFRc}

**Proposition 4.1.** *Let $\ell \neq p$ be a prime number.*

(a) *Let $L$ be a totally and tamely ramified Galois extension of $K$ of degree $\ell$. Then, $\bar{K}$ contains a root of unity of order $\ell$.*

(b) *Conversely, suppose that $\bar{K}$ contains a root of unity of order $\ell$. Then, $K$ has a cyclic extension $L$ of degree $\ell$ which is a totally and tamely extension of $K$.*

For a finitely generated profinite group $G$, the paragraph preceding [Lub01, Thm. 0.1] says that $G$ is $\mathrm{rank}(G)$**-abelian-indexed** if for every closed subgroup $H$ of $G$ of finite index, $H/[H,H]$ is isomorphic to $\hat{\mathbb{Z}}^r$ with $r = 1 + (\mathrm{rank}(G) - 1)(G:H)$. To this end note that if $H = \mathrm{Gal}(K')$ for some finite extension $K'$ of $K$, then $(G:H) = [K':K]$ is finite and $H/[H,H] \cong \mathrm{Gal}(K'_{\mathrm{ab}}/K')$, where $K'_{\mathrm{ab}}$ is the maximal abelian extension of $K'$.

{IWSw}

**Lemma 4.2.** *The field $K$ has a finite extension $K'$ such that $\mathrm{Gal}(K'_{\mathrm{ab}}/K')$ is isomorphic to no group of the form $\hat{\mathbb{Z}}^r$. Thus, $\mathrm{Gal}(K)$ is not $\mathrm{rank}(\mathrm{Gal}(K))$-abelian-indexed.*

*Proof.* Consider a prime number $\ell \neq p$. Replacing $K$ by a finite extension, we may assume that $\bar{K}^\times$ contains a primitive $\ell$-th root of unity.

Let $K_{\mathrm{ur}}$ be the maximal unramified extension of $K$. By [CaF67, p. 28, I], $\mathrm{Gal}(K_{\mathrm{ur}}/K) \cong \hat{\mathbb{Z}}$. Hence, $K$ has a unique extension $K_\ell$ in $K_{\mathrm{ur}}$ such that $\mathrm{Gal}(K_\ell/K) \cong \mathbb{Z}/\ell\mathbb{Z}$.

On the other hand, by Proposition 3.1(b), $K$ has a totally and tamely ramified Galois extension $L$ of degree $\ell$. In particular $K_\ell \cap L = K$, so $\mathrm{Gal}(K_\ell L/K) \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Thus, $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ is a quotient of $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ but not of $\hat{\mathbb{Z}}$. It follows that $\mathrm{Gal}(K_{\mathrm{ab}}/K) \ncong \hat{\mathbb{Z}}$.

Now assume toward contradiction that $\mathrm{Gal}(K_{\mathrm{ab}}/K) \cong \hat{\mathbb{Z}}^r$ for some $r \geq 2$. Then, for each prime number $\ell'$, $K$ has two cyclic extensions $L_0, L_1$ of degree $\ell'$ of $K$, such that $L_0 \cap L_1 = K$. In particular, we may choose $\ell' \neq p$ such that $\bar{K}^\times$ contains no root of unity of order $\ell'$. Also, we may assume without loss that $L_1/K$ is ramified, hence totally and tamely ramified. This contradicts Proposition 3.1(a). $\square$

We denote the minimal number of relations needed to define a finitely generated group $G$ by $\mathrm{rel}(G)$. Also, we denote the minimal integer which is greater or equal to a real number $x$ by $\lceil x \rceil$.

Now we apply a special case of [Lub01, Thm. 0.2] to establish an explicit formula for $\mathrm{rel}(\mathrm{Gal}(K))$. The latter theorem is used in [Lub01] to deduce [Lub01, Thm. 0.3] which we cited as Proposition 2.1.

Recall that a finite $\mathbb{F}_\ell[\mathrm{Gal}(K)]$-module $A$ is said to be **simple** if $A \neq \mathbf{0}$ and if $A$ contains no $\mathbb{F}_\ell[\mathrm{Gal}(K)]$-submodules except itself and $\mathbf{0}$.

**Proposition 4.3.** *Let $K$ be a finite extension of $\mathbb{Q}_p$. Then,* {GEN5}

$$\begin{aligned}\mathrm{rel}(\mathrm{Gal}(K)) = \sup_{\ell,A}\Big\{\Big\lceil \frac{\dim_{\mathbb{F}_\ell}(\mathrm{H}^2(\mathrm{Gal}(K),A)) - \dim_{\mathbb{F}_\ell}(\mathrm{H}^1(\mathrm{Gal}(K),A))}{\dim_{\mathbb{F}_\ell}(A)}\Big\rceil \\ + \mathrm{rank}(\mathrm{Gal}(K)) - \xi_{K,A}\Big\},\end{aligned} \tag{10}$$ {gen6}

*where $\ell$ runs over all prime numbers, $A$ ranges over all finite simple $\mathbb{F}_\ell[\mathrm{Gal}(K)]$-modules, and for all such $A$ we have $\xi_{K,A}$ is $0$ if $\mathrm{Gal}(K)$ acts trivially on $A$ and $\xi_{K,A} = 1$ otherwise.*

*Proof.* Lemma 3.2 assures that $\mathrm{Gal}(K)$ is not $\mathrm{rank}(\mathrm{Gal}(K))$-abelian-indexed. Hence, equality (10) is a special case of [Lub01, Thm. 0.2]. □

This brings us to our main result.

**Theorem 4.4.** *Let $p$ be a prime number and $K$ a finite extension of $\mathbb{Q}_p$. Then,* {MANt}

$$\mathrm{rel}(\mathrm{Gal}(K)) = \mathrm{rank}(\mathrm{Gal}(K)) - 1 = [K:\mathbb{Q}_p] + 1. \tag{11}$$ {heil}

*Proof.* The second equality in (11) is just Theorem 1.1. In view of equality (10), it suffices for the proof of the first equality of (11) to prove that for each prime number $\ell$, and every simple finite $\mathbb{F}_\ell[\mathrm{Gal}(K)]$-module $A$ we have

$$\Big\lceil \frac{\dim_{\mathbb{F}_\ell}(\mathrm{H}^2(\mathrm{Gal}(K),A)) - \dim_{\mathbb{F}_\ell}(\mathrm{H}^1(\mathrm{Gal}(K),A))}{\dim_{\mathbb{F}_\ell}(A)}\Big\rceil - \xi_{K,A} \leq -1. \tag{12}$$ {geil}

and that there exists a simple finite $\mathbb{F}_\ell[\mathrm{Gal}(K)]$-module $A$ for which the left hand side of (12) is $-1$.

Indeed, recall that $\mathrm{H}^0(\mathrm{Gal}(K),A)$ is the subgroup $A^{\mathrm{Gal}(K)}$ of elements of $A$ fixed under the action of $\mathrm{Gal}(K)$ [Rib70, p. 97]. Also note that $\lceil x - m\rceil \leq \lceil x\rceil$ for every real number $x$ and every non-negative number $m$. Finally, for each prime number $\ell$, let $h(\ell)$ be as in (9). Hence,

$$\Big\lceil \frac{\dim_{\mathbb{F}_\ell}(\mathrm{H}^2(\mathrm{Gal}(K),A)) - \dim_{\mathbb{F}_\ell}(\mathrm{H}^1(\mathrm{Gal}(K),A))}{\dim_{\mathbb{F}_\ell}(A)}\Big\rceil - \xi_{K,A} \tag{13}$$ {ceil}

$$\overset{(8)}{=} \Big\lceil \frac{-\dim_{\mathbb{F}_\ell}(\mathrm{H}^0(\mathrm{Gal}(K),A)) + h(\ell)}{\dim_{\mathbb{F}_\ell}(A)}\Big\rceil - \xi_{K,A} \tag{14}$$

$$\overset{(9)}{=} \begin{cases} \Big\lceil \frac{-\dim_{\mathbb{F}_p}(A^{\mathrm{Gal}(K)})}{\dim_{\mathbb{F}_p}(A)} - [K:\mathbb{Q}_p]\Big\rceil - \xi_{K,A} & \text{if } \ell = p \\ \Big\lceil \frac{-\dim_{\mathbb{F}_\ell}(A^{\mathrm{Gal}(K)})}{\dim_{\mathbb{F}_\ell}(A)}\Big\rceil - \xi_{K,A} & \text{if } \ell \neq p, \end{cases} \tag{15}$$ {deil}

where $\xi_{K,A}$ is the constant introduced in Proposition 3.3.

If the action of $\mathrm{Gal}(K)$ on $A$ is non-trivial, then $\xi_{K,A} = 1$ and $A^{\mathrm{Gal}(K)} = \mathbf{0}$ (because $A$ is a simple $\mathbb{F}_\ell[\mathrm{Gal}(K)]$-module). Thus, the expression on the upper row of (15) is $-[K:\mathbb{Q}_p] - 1$. Similarly, for $\ell \neq p$, the expression on the lower row of (15) is $-1$.

If $\mathrm{Gal}(K)$ acts trivially on $A$, then $A^{\mathrm{Gal}(K)} = A$ and $\xi_{K,A} = 0$. If, in addition $\ell = p$, then the left expression on the upper row of (15) becomes $\lceil -1 - [K:\mathbb{Q}_p] \rceil \leq -1$. Similarly, for $\ell \neq p$, the left expression on the lower row of (15) is $-1$. Note that this case occurs for $A := \mathbb{Z}/\ell\mathbb{Z}$ with the trivial action of $\mathrm{Gal}(K)$ on $A$, because $\mathbb{Z}/\ell\mathbb{Z}$ has no non-trivial proper subgroup, so $A$ is a simple $\mathbb{F}_\ell[\mathrm{Gal}(K)]$-module.

It follows that in all cases the expression in (13) is at most $-1$ and the equality holds in at least one case, as claimed. □

# 5 Comments

We conclude with three remarks, with $K$ being, as above, a $p$-adic field.

**Remark 5.1.** The equality of the left hand side of (12) to $-1$ in the case $\ell \neq p$ and $A = \mathbb{Z}/\ell\mathbb{Z}$ with a trivial action of $\mathrm{Gal}(K)$ follows also from a precise knowledge of $\mathrm{H}^i(\mathrm{Gal}(K), \mathbb{Z}/\ell\mathbb{Z})$ for $i = 1, 2$.

Indeed, let $\zeta_\ell$ be a primitive root of unity of order $\ell$. Let $\delta = 1$ if $\zeta_\ell \in K$ and $\delta = 0$ if $\zeta_\ell \notin K$. By [NSW20, p. 399, Cor. 7.3.9], $\dim_{\mathbb{F}_\ell} \mathrm{H}^1(\mathrm{Gal}(K), \mathbb{Z}/\ell\mathbb{Z}) = 1+\delta$. By the proof of the latter corollary

$$\dim_{\mathbb{F}_\ell} \mathrm{H}^2(\mathrm{Gal}(K), \mathbb{Z}/\ell\mathbb{Z}) = \delta.$$

Also, $\dim_{\mathbb{F}_\ell}(\mathbb{Z}/\ell\mathbb{Z}) = 1$ and $\xi_{K,\mathbb{Z}/\ell\mathbb{Z}} = 0$. Hence,

$$\left\lceil \frac{\dim_{\mathbb{F}_\ell}(\mathrm{H}^2(\mathrm{Gal}(K), \mathbb{Z}/\ell\mathbb{Z})) - \dim_{\mathbb{F}_\ell}(\mathrm{H}^1(\mathrm{Gal}(K), \mathbb{Z}/\ell\mathbb{Z}))}{\dim_{\mathbb{F}_\ell}(\mathbb{Z}/\ell\mathbb{Z})} \right\rceil - \xi_{K,\mathbb{Z}/\ell\mathbb{Z}} = -1,$$

as claimed.

{cntb}

**Remark 5.2.** For an element $w$ in a profinite group $G$, the condition "the closed subgroup $\langle w \rangle$ of $G$ generated by $w$ is a pro-$p$ group" can be expressed by the profinite relation $w^\pi = 1$, where $\pi$ is the element of $\hat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_l$ (with $\ell$ ranging over all prime numbers) whose $\ell$th entry is 1 if $\ell = p$ and 0 if $\ell \neq p$. In this case $(w^\sigma)^\pi = (w^\pi)^\sigma = 1$ for each $\sigma \in G$.

By Jannsen-Wingberg, [NSW20, p. 419, Thm. 7.5.14], $\mathrm{Gal}(K)$ is generated by elements $\sigma, \tau, x_0, \ldots, x_n$, with $n = [K:\mathbb{Q}_p]$, satisfying two relations, (B) and (C), and the following one:

(A) The closed normal subgroup $N$ of $\mathrm{Gal}(K)$ generated by $x_0, \ldots, x_n$ is a pro-$p$ group.

Let $G_0$ be the abstract subgroup of $G$ generated by $\sigma, \tau, x_0, \dots, x_n$ and let $N_0$ be the abstract normal subgroup of $G_0$ generated by $x_0, \dots, x_n$. Then, $N$ is the closure of $N_0$ in $G$ and the condition "$w^\pi = 1$ for each word in $N_0$" is equivalent to (A).

Note that $N_0$ is countable. Hence, Condition (A) can be replaced by infinite countable set of explicit relations involving $\sigma, \tau, x_0, \dots, x_n$. But a priori it is not clear that the result of Jannsen-Wingberg yields a finite presentation of $\mathrm{Gal}(K)$. Compare footnote on page 418 of [NSW20].

{Dem}

**Remark 5.3.** The first equality $\mathrm{rel}(\mathrm{Gal}(K)) = \mathrm{rank}(\mathrm{Gal}(K)) - 1$ in Theorem 3.4 does not always hold if we replace $\mathrm{Gal}(K)$ by a quotient $\mathrm{Gal}(N/K)$, with $N$ being a Galois extension of $K$.

For example, put $G = \mathrm{Gal}(K)$ and let, $K^{(p)}$ be the maximal pro-$p$ extension of $K$. Then, $G(p) := \mathrm{Gal}(K^{(p)}/\mathbb{Q}_p)$ is the maximal pro-$p$ quotient of $G$. It is well known that $G(p)$ is either a finitely generated free pro-$p$ group or a Demuskin group.

Indeed, let $\mu_p$ be the group of roots of unity of order $p$ in $\tilde{\mathbb{Q}}_p$. If $\mu_p \not\subseteq K$, then by [NSW20, p. 416, Thm. 7.5.11(i)], $G(p)$ is a free pro-$p$ group (i.e. $\mathrm{rel}(G(p)) = 0$) with $\mathrm{rank}(G(p)) = [K : \mathbb{Q}_p] + 1 \geq 2$. Thus, $\mathrm{rel}(G(p)) < \mathrm{rank}(G(p)) - 1$.

If $\mu_p \subseteq K$, then, by [NSW20, p. 416, Thm. 7.5.11(ii)], $G(p)$ is a Demuskin group of rank $[K : \mathbb{Q}_p] + 2$, so $\mathrm{rank}(G(p)) \geq 3$. Also, by [NSW20, p. 231, Def. 3.9.9(ii)], $\dim_{\mathbb{F}_p} H^2(G(p), \mathbb{F}_p) = 1$, so by [NSW20, p. 227, Cor. 3.9.5], $\mathrm{rel}(G(p)) = 1$. Hence, $\mathrm{res}(G(p)) = 1 < 2 \leq \mathrm{rank}(G(p)) - 1$.

Thus, in all cases $\mathrm{rel}(G(p)) < \mathrm{rank}(G(p)) - 1$.

{MTRf}

**Remark 5.4.** Theorem 1.1 does not apply to infinite algebraic extensions of $\mathbb{Q}_p$. For example, the algebraic closure $\tilde{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ is an infinite extension of $\mathbb{Q}_p$, while its absolute Galois group is trivial, so $\mathrm{rank}(\mathrm{Gal}(\tilde{\mathbb{Q}}_p)) = 0$, hence $\mathrm{rank}(\mathrm{Gal}(\tilde{\mathbb{Q}}_p)) \neq [\tilde{\mathbb{Q}}_p : \mathbb{Q}_p] + 2$.

Similarly, the left hand side of Theorem 3.4 does not apply to infinite algebraic extensions of $\mathbb{Q}_p$. For example, let $K$ be the fixed field of the ramification group of $\mathrm{Gal}(\mathbb{Q}_p)$. By [NSW20, p. 423, Prop. 7.5.1], $\mathrm{Gal}(K)$ is the free pro-$p$ group of rank $\aleph_0$. Hence, $\mathrm{rel}(\mathrm{Gal}(K)) = 0$ and $\mathrm{rank}(\mathrm{Gal}(K)) = \infty$. Therefore, $\mathrm{rel}(\mathrm{Gal}(K)) \neq \mathrm{rank}(\mathrm{Gal}(K)) - 1$.

{CHRp}

**Remark 5.5.** The analog of a $p$-adic field in positive characteristic $p$ is the field $\mathbb{F}_q((t))$ of formal power series in an indeterminate $t$ with coefficients in the field $\mathbb{F}_q$ of $q$ elements, where $q$ is a power of $p$. Helmut Koch proved in [Koc65] that $\mathrm{Gal}(\mathbb{F}_q((t)))$ is generated by infinitely many elements $\sigma, \tau, x_1, x_2, x_3, \dots$ such that $\tau\sigma\tau^{-1} = \sigma^q$, the closed normal subgroup generated by $x_1, x_2, x_3, \dots$ is a free pro-$p$ group of rank $\aleph_0$, and $\sigma, \tau$ "act freely" on this subgroup (see also [NSW20, p. 418, Thm. 7.5.13]). On the other hand, $\mathbb{F}_q((t))$ has infinitely many Artin-Schreier cyclic extensions of degree $p$ [BJL16, Rem. 4.3]. In particular, $\mathrm{Gal}(\mathbb{F}_q((t)))$ is not finitely generated. A posteriori, $\mathrm{Gal}(\mathbb{F}_q((t)))$ is not finitely presented.

# References


[BJL16] S. Böge, M. Jarden, and A. Lubotzky, *Sliceable groups and towers of fields,* Journal of Group Theory **19** (2016), 365–390.

[CaF67] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Academic Press, London, 1967.

[Die84] V. Dieckert, *Über die absolute Galoisgruppe dydischer Zahlkörper,* Journal für die reine und angewandte Mathematik **350** (1984), 152–172.

[ESV21] H. Esnault, M. Shusterman, and V. Srinivas, *Finite presentation for fundamental groups in characteristic p,* arXiv:2102.13424v1 [math.AG] 26 Feb 2021.

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

[Jan82] U. Jannsen, *Über Galoisgruppen lokaler Körper,* Inventiones mathematicae **70** (1982), 53–69.

[JaW82] U. Jannsen und K. Wingberg, *Die Stuktur der absoluten Galoisgruppe* $\mathfrak{p}$*-adischer Zahlkörper,* Inventiones mathematicae **70** (1982), 71–98.

[JaR91] M. Jarden and J. Ritter, *On the Frattini subgroup of the absolute Galois group of a local field,* Israel Journal of Mathematics **74** (1991), 81–90.

[Koc65] H. Koch, *Über Galoissche Gruppen von* $\mathfrak{p}$*-adischen Zahlkörpern,* Mathematische Nachrichten **29** (1965), 77–111.

[Koc70] H. Koch, *Galoissche Theorie der p-Erweiterungen,* Mathematische Monographien **10**, VEB Deutscher Verlag der Wissenschaften, Berlin 1970.

[Lan97] S. Lang, *Algebra (third edition),* Addison-Wesley, Reading, 1997.

[Liu20] Y. Liu, *Presentations of Galois groups of maximal extensions with restricted ramification,* arXiv.org ¿ math ¿ arXiv:2005.07329

[Lub01] A. Lubotzky, *Pro-finite Presentations,* Journal of Algebra **242** (2001), 672–690.

[Neu99] J. Neukirch, *Algebraic Number Theory, translated from German by N. Schppachar,* Grundlehren der mathematischen Wissenschaften **322**, Springer, Heidelberg, 1999.

[NSW20] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields,* Grundlehren der mathematischen Wissenschaften **323**, Springer-Verlag, Heidelberg, Second Edition, corrected version 2.3, May 2020. Electronic Edition, www.mathi.uni-heidelberg.de/∼schmidt/NSW2e/index-de.html

[Rib70] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology*, Queen's papers in Pure and Applied Mathematics **24**, Queen's University, Kingston, 1970.

[Shu18] M. Shusterman, *Balanced presentation for fundamental groups of curves over finite fields*, arXiv.org > math > arXiv:1811.04192