THE ABSOLUTE GALOIS GROUPS OF FINITE EXTENSIONS OF $\mathbb{R}(t)$*

by

Dan Haran

School of Mathematics, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

e-mail: haran@post.tau.ac.il

and

Moshe Jarden

School of Mathematics, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

e-mail: jarden@post.tau.ac.il

Abstract

Let R be a real closed field and L be a finite extension of $R(t)$. We prove that $\mathrm{Gal}(L) \cong \mathrm{Gal}(R(t))$ if L is formally real and $\mathrm{Gal}(L)$ is the free profinite group of rank $\mathrm{card}(R)$ if L is not formally real.

MR Classification: 12E30

Directory: \Jarden\Diary\RealFree

3 April, 2007

* Research supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation.

Introduction

Let R be a real closed field, t an indeterminate, and $K = R(t)$ the field of rational functions in t over R. In their work [KrN71], Krull and Neukirch consider the case where R is the field of real numbers $\mathbb{R}$. For each finite set S of prime divisors of $K/\mathbb{R}$ they introduce the maximal extension K_S of K unramified outside S and present $\mathrm{Gal}(K_S/K)$ by generators and relations. Based on this description, they present the absolute Galois group $\mathrm{Gal}(K)$ as a semi-direct product of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and $\mathrm{Gal}(\mathbb{C}(t))$ with an explicit action. Schuppar [Sch80] extends the results of [KrN71] to an arbitrary real closed field R.

In [HaJ85] we apply the presentation of $\mathrm{Gal}(K_S/K)$ by generators and relations to present $\mathrm{Gal}(K)$ (for an arbitrary real closed field R) as a free product $C(X) * F$, where $C(X)$ is a free product of groups of order 2 over an indexed profinite space X of weight $m = \mathrm{card}(R)$ and F is a free profinite group of rank m.

In a letter to the second author, David Harbater asked about the isomorphism type of $\mathrm{Gal}(L)$, where L ranges over the finite extensions of K. In particular he asked whether $\mathrm{Gal}(L)$ depends on the number of the connected components of $\Gamma(R)$, where Γ is a smooth model of K/R.

The goal of this note is to prove that there are actually only two isomorphism types for $\mathrm{Gal}(L)$, either $\mathrm{Gal}(K)$ or a free profinite group of rank $m = \mathrm{card}(R)$. Indeed, we prove the following theorem.

Main Theorem: *Let R be a real closed field, $K = R(t)$ the field of rational functions over R, and L a finite extension of K. Let $C(X)$ be the free product on a constant sheaf of groups of order 2 over the profinite space X of orderings of K, and let F be the free profinite group of rank* $\mathrm{card}(R)$. *If L is formally real, then* $\mathrm{Gal}(L) \cong C(X) * F$; *if L is not formally real, then* $\mathrm{Gal}(L) \cong F$.

Our proof applies Kurosh Subgroup Theorem for free profinite product of finitely many profinite groups to reduce the main theorem to the case $K = L$. An essential ingredient in the proof is Proposition 1.4 which states that every non-empty open-closed subset of the space of orderings $X(K)$ of K is homeomorphic to $X(K)$.

It is possible that the main theorem follows also from of the Kurosh Subgroup Theorems for infinitely many factors stated either in [GiR73] or in [Zal92]. This is hinted in Remark 4.3(c) of [Har07]. Unfortunately, neither of them explicitly gives the rank of the free group nor the structure of the underlying topological space of involutions.

1. Spaces of orderings

Let K be a field. The set $X(K)$ of orderings of K is a profinite space [Pre75, Theorem 6.5] under the **Harrison topology**. This topology is given by the **Harrison subbasis** $\{H(a) \mid a \in K^\times\}$, where $H(a) = \{P \in X(K) \mid a \in P\}$. This set is open-closed in $X(K)$; its complement is $H(-a)$. We revise the description of open-closed Harrison sets as a disjoint union of "open intervals" and prove that they are homeomorphic to each other.

The following observation is obvious.

Lemma 1.1: *Let θ be an automorphism of a field K. Then $P \mapsto \theta(P)$ is a homeomorphism of the space of orderings of K. It maps the Harrison set $H(a)$ onto $H(\theta(a))$.*

For the rest of this section let R be a real closed field and $K = R(t)$ the field of rational functions over R. Put

$$\mathcal{H}' = \{H(t-a), H(a-t) \mid a \in R\}$$

Lemma 1.2: *The family $\mathcal{H}'$ is a subbasis for the Harrison topology on $X(K)$.*

Proof: This is essentially written in the proof of [Cra74, Prop. 12]: For all $f, g \in K^\times$ we have

$$H(f/g) = H(fg) = \big(H(f) \cap H(g)\big) \cup \big(H(-f) \cap H(-g)\big).$$

Therefore the elements of the Harrison subbasis for $X(K)$ are finite unions of finite intersections of sets $H(f), H(-f)$ with either $f \in R$ or $f \in R[t]$ monic and irreducible. In the latter case either $f = t - a$ for some $a \in R$ or $f = (t+a)^2 + b^2$ for some $a \in R$ and $b \in R^\times$. However, if $f \in R$ then $H(f) = X(K)$ or $H(f) = \emptyset$, depending on whether f is positive or negative in the unique ordering on R. Similarly, if $f = (t+a)^2 + b^2$ for some $a \in R$ and $b \in R^\times$, then $H(f) = X(K)$. ∎

For $a, b \in R \cup \{\pm\infty\}$ put $(a, b) = \{P \in X(K) \mid a < t < b \text{ in } P\}$. (Conditions $-\infty < t$, $t < \infty$ are understood to hold for every $P \in X(K)$, while conditions $\infty < t$, $t < -\infty$ hold for no P.)

LEMMA 1.3:

(a) $\mathcal{H} = \{(a, b) \mid a, b \in R \cup \{\pm\infty\}\}$ *is a basis for the Harrison topology of* $X(K)$.

(b) *Every open-closed subset of* $X(K)$ *is the disjoint union of finitely many elements of* $\mathcal{H}$.

Proof of (a): We have $(a, \infty) = H(t - a)$, $(-\infty, b) = H(a - t)$, and $(a, b) = H(t - a) \cap H(b - t)$, if $a, b \in R$. Hence, every $H \in \mathcal{H}$ is the intersection of (at most two) elements of $\mathcal{H}'$. Since $(a, b) \cap (c, d) = (\max(a, c), \min(b, d)) \in \mathcal{H}$, the family $\mathcal{H}$ is closed under finite intersections.

Proof of (b): Let $H \in X(K)$ be open-closed. By (a), $H = \bigcup_{i \in I} H_i$, with $H_i \in \mathcal{H}$ for each i. Since H is compact [Pre75, Theorem 6.5], we may assume that I is finite. Thus, there are $c_1 < c_2 < \cdots < c_m$ in $R \cup \{\pm\infty\}$ such that each H_i is (c_j, c_k) for some $1 \leq j, k \leq m$. If $j \geq k$, then $(c_j, c_k) = \emptyset$; if $j < k$, then $(c_j, c_k) = \bigcup_{\nu=j}^{k-1} (c_\nu, c_{\nu+1})$. Hence, we may assume that $H_i = (c_j, c_{j+1})$. Since $(c_1, c_2), (c_2, c_3), \ldots, (c_{m-1}, c_m)$ are disjoint, H is the disjoint union of some of them. ∎

PROPOSITION 1.4: *Every two non-empty open-closed subsets of* $X(K)$ *are homeomorphic.*

Proof: By Lemma 1.1, the R-automorphism of K which maps t onto $t - a, a - t, \frac{t-b}{c-t}$ induces a homeomorphism between $H(t) = (0, \infty)$ and $H(t - a) = (a, \infty), H(a - t) = (-\infty, a), H(\frac{t-b}{c-t}) = (b, c)$, respectively. Thus, the elements of $\mathcal{H}$, defined in Lemma 1.3(a), are homeomorphic.

Let $H \neq \emptyset$ be an open-closed subset of $X(K)$. By Lemma 1.3(b), H is a disjoint union $H = \dot\bigcup_{i=1}^{n} H_i$ of elements of $\mathcal{H}$. Without loss of generality, each H_i is non-empty. By the preceding paragraph, H_i is homeomorphic to $(i, i + 1)$ and H_n is also homeomorphic to (n, ∞). Therefore, H is homeomorphic to $\dot\bigcup_{i=1}^{n-1} (i, i + 1) \cup (n, \infty) = (1, \infty)$. ∎

2. Free products

Let X be a profinite space and let $C = \langle \varepsilon \rangle$ be the cyclic group of order 2. Let $C(X)$ denote the free product of copies of C over the **constant sheaf** with base X. Thus, $C(X)$ is a profinite group with a continuous map $\omega\colon X \to C(X)$ such that $\omega(x)^2 = 1$ for all $x \in X$, and if $\eta_0\colon X \to H$ is a continuous map into a profinite group H with $\eta_0(x)^2 = 1$ for all $x \in X$, then there exists a unique homomorphism $\eta\colon C(X) \to H$ satisfying $\eta \circ \omega = \eta_0$. For each $x \in X$ put $\varepsilon_x = \omega(x) \in C(X)$. Then $C(X)$ is also the (inner) free product of the groups $\langle \varepsilon_x \rangle$ in the sense of [Mel90, Sec. 1]. In particular, $C(X) = \langle \varepsilon_x \mid x \in X \rangle$.

In addition, fix $\bar{x} \in X$ and let $F(X, \bar{x})$ be the **free group on the pointed space** $(X, \bar{x})$. Thus, $F(X, \bar{x})$ is a profinite group with a continuous map $\lambda\colon X \to F(X, \bar{x})$ such that $\lambda(\bar{x}) = 1$, and if $\eta_0\colon X \to H$ is a continuous map into a profinite group H such that $\eta_0(\bar{x}) = 1$, then there exists a unique homomorphism $\eta\colon F(X, \bar{x}) \to H$ such that $\eta \circ \lambda = \eta_0$. For each $x \in X$ put $\sigma_x = \lambda(x) \in F(X, \bar{x})$; in particular, $\sigma_{\bar{x}} = 1$.

If X is infinite, then $F(X, \bar{x})$ is isomorphic to the free profinite group of rank m, where m is the **weight** of X, that is, the cardinality of the family of open-closed subsets of X [RiZ00, Proposition 3.5.12].

LEMMA 2.1: *The kernel of the epimorphism $\varphi\colon C(X) \to C$, given by $\varepsilon_x \mapsto \varepsilon$, is isomorphic to $F(X, \bar{x})$, and $C(X) \cong C \ltimes F(X, \bar{x})$, with action given by $\sigma_x^\varepsilon = \sigma_x^{-1}$, for every $x \in X$.*

Proof: Let $\alpha_0\colon X \to C(X)$ be the map $x \mapsto \varepsilon_{\bar{x}}\varepsilon_x$. Then $\alpha_0(\bar{x}) = 1$ and α_0 is continuous, since it is the composition of the continuous maps $X \to C(X)$ given by $x \mapsto \varepsilon_x$ and $C(X) \to C(X)$ given by $g \mapsto \varepsilon_{\bar{x}} g$. Therefore α_0 defines a homomorphism $\alpha\colon F(X, \bar{x}) \to C(X)$ by $\sigma_x \mapsto \varepsilon_{\bar{x}}\varepsilon_x$.

The map $X \to F(X, \bar{x})$ given by $x \mapsto \sigma_x^{-1}$ (and in particular $\bar{x} \mapsto \sigma_{\bar{x}}^{-1} = 1$) extends to a continuous automorphism of $F(X, \bar{x})$, given by $\sigma_x \mapsto \sigma_x^{-1}$, which is clearly of order 2. Hence, C acts on $F(X, \bar{x})$ by $\sigma_x^\varepsilon = \sigma_x^{-1}$, for $x \in X$. We have

$$\alpha(\sigma_x^\varepsilon) = \alpha(\sigma_x^{-1}) = \alpha(\sigma_x)^{-1} = (\varepsilon_{\bar{x}}\varepsilon_x)^{-1} = \varepsilon_x\varepsilon_{\bar{x}} = (\varepsilon_{\bar{x}}\varepsilon_x)^{\varepsilon_{\bar{x}}} = (\alpha(\sigma_x))^{\varepsilon_{\bar{x}}}.$$

Hence, α extends to a homomorphism $\alpha\colon C \ltimes F(X, \bar{x}) \to C(X)$ by $\varepsilon \mapsto \varepsilon_{\bar{x}}$.

On the other hand, the map $\beta_0\colon X \to C \ltimes F(X, \bar{x})$ given by $x \mapsto \varepsilon\sigma_x$ is continuous and its image consists of elements of order 1 or 2, since $(\varepsilon\sigma_x)^2 = \sigma_x^\varepsilon \sigma_x = \sigma_x^{-1}\sigma_x = 1$ in $C \ltimes F(X, \bar{x})$. Hence, there is a continuous homomorphism $\beta\colon C(X) \to C \ltimes F(X, \bar{x})$ given by $\varepsilon_x \mapsto \varepsilon\sigma_x$, for each $x \in X$.

For each $x \in X$ we have $\alpha(\beta(\varepsilon_x)) = \alpha(\varepsilon\sigma_x) = \varepsilon_{\bar{x}}(\varepsilon_{\bar{x}}\varepsilon_x) = \varepsilon_x$, $\beta(\alpha(\sigma_x)) = \beta(\varepsilon_{\bar{x}}\varepsilon_x) = \varepsilon\sigma_{\bar{x}}\varepsilon\sigma_x = \sigma_x$, and $\beta(\alpha(\varepsilon)) = \beta(\varepsilon_{\bar{x}}) = \varepsilon\sigma_{\bar{x}} = \varepsilon$. The uniqueness part of the definitions of α and β implies that $\alpha \circ \beta$ and $\beta \circ \alpha$ are the identity maps. Hence, α is an isomorphism. Moreover, $\varphi \circ \alpha$ is the projection $C \ltimes F(X, x) \to C$. Therefore, $\alpha(F(X, x)) = \mathrm{Ker}(\varphi)$. ∎

LEMMA 2.2: *Let F_1, F_2 be free profinite groups of ranks m_1, m_2, respectively. Then $F_1 * F_2$ is a free group of rank $m_1 + m_2$.*

Proof: By definition [FrJ05, Definition 17.4.1], F_i is the free group on a set S_i of cardinality m_i, for $i = 1, 2$. Thus, $S = S_1 \mathbin{\dot\cup} S_2$ is a subset of $F_1 * F_2$ that converges to 1 and each map ψ from S into a profinite group H that converges to 1 uniquely extends to a homomorphism $F_1 * F_2 \to H$. Consequently, $F_1 * F_2$ is the free profinite group on S, so $\mathrm{rank}(F_1 * F_2) = m_1 + m_2$. ∎

PROPOSITION 2.3: *Let F be a free profinite group of rank $m \geq \aleph_0$ and let X be a profinite space of weight m. Assume that every non-empty open-closed subset of X is homeomorphic to X. Let $G = C(X) * F$ and let H be an open subgroup of G. Then either $H \cong G$ or $H \cong F$.*

Proof: Choose an open normal subgroup N of G contained in H and let $\pi\colon G \to G/N$ be the quotient map.

CLAIM A: *There is a partition $X = \dot\bigcup_{i=1}^n X_i$ of X into disjoint open-closed subsets such that for every $1 \leq i \leq n$ we have $\pi(\varepsilon_x) = \pi(\varepsilon_y)$ for all $x, y \in X_i$.* Indeed, the map $\omega\colon X \to C(X) \leq G$ given by $x \mapsto \varepsilon_x$ is continuous, hence so is $\pi \circ \omega\colon X \to G/N$. Its fibers $X_1, \dots, X_n$ satisfy the requirements of the claim.

PART B: *Factors of H.* By [Mel90, Theorem 1.5], $G = \mathop{\Large\ast}_{i=1}^n C(X_i) * F$. By the Kurosh

Subgroup Theorem for free product with finitely many factors [RiZ00, Theorem 9.1.9]

$$H = \mathop{\text{\Large$\ast$}}_{i=1}^{n} \mathop{\text{\Large$\ast$}}_{j=1}^{r_i} (C(X_i)^{g_{ij}} \cap H) * \mathop{\text{\Large$\ast$}}_{j=1}^{r} (F^{g_j} \cap H) * F',$$

where F' is a finitely generated free profinite group, $r, n, r_i \in \mathbb{N}$, and $g_j, g_{ij} \in G$.

Fix $1 \leq i \leq n$. Let N_i be the kernel of the epimorphism $\varphi_i\colon C(X_i) \to C$ given by $\varepsilon_x \mapsto \varepsilon$, for all $x \in X_i$. If $C(X_i)^{g_{ij}} \leq H$, then $C(X_i)^{g_{ij}} \cap H = C(X_i)^{g_{ij}} \cong C(X_i)$. If $C(X_i)^{g_{ij}} \not\leq H$, then $C(X_i) \not\leq N$. Since $C(X_i) = \langle \varepsilon_x \mid x \in X_i \rangle$, there is a $y \in X_i$ such that $\varepsilon_y \notin N$, so $\bar{\varepsilon} = \pi(\varepsilon_y) \in G/N$ is of order 2. By Claim A, $\pi(\varepsilon_x) = \bar{\varepsilon}$ for all $x \in X_i$. Therefore, the map $\varepsilon \mapsto \bar{\varepsilon}$ gives an isomorphism $\gamma\colon C \to \langle \bar{\varepsilon} \rangle$ such that $\gamma \circ \varphi_i = \pi|_{C(X_i)}$, thus $C(X_i) \cap N = N_i$. Since $N_i^{g_{ij}} = C(X_i)^{g_{ij}} \cap N \leq C(X_i)^{g_{ij}} \cap H < C(X)^{g_{ij}}$ and $(C(X_i)^{g_{ij}} : N_i^{g_{ij}}) = 2$, we have $C(X_i)^{g_{ij}} \cap H = N_i^{g_{ij}}$. By Lemma 2.1, N_i is the free profinite group $F(X_i, \bar{x}_i)$ on a pointed space $(X_i, \bar{x}_i)$, for some $\bar{x}_i \in X_i$. Hence, $C(X_i)^{g_{ij}} \cap H = N_i$ is a free group of rank m_i, where m_i is the weight of X_i.

For each $1 \leq j \leq r$, $F^{g_j} \cap H$ is isomorphic to an open subgroup of F, hence [FrJ05, Proposition 17.6.2] isomorphic to F.

Part C: *Conclusion.* By Part B, $H \cong \mathop{\ast}_{i=1}^{s} C(Y_i) * \mathop{\ast}_{j=1}^{t} F_j * F'$, where Y_i is an open-closed subset of X for each i and $F_j \cong F$ for each j. Since all non-empty open-closed subsets are homeomorphic (to X), we may assume that $Y_1, \ldots, Y_s$ are disjoint. It then follows either from [Mel90, Theorem 1.5] or directly from the definition of $C(X)$ that $\mathop{\ast}_{i=1}^{s} C(Y_i) = C(\bigcup_{i=1}^{s} Y_i)$. If $\bigcup_{i=1}^{s} Y_i$ is not empty, it is homeomorphic to X, and hence $C(\bigcup_{i=1}^{s} Y_i) \cong C(X)$. If $\bigcup_{i=1}^{s} Y_i = \emptyset$, then $C(\bigcup_{i=1}^{s} Y_i) = 1$.

By Lemma 2.2, $\mathop{\ast}_{j=1}^{t} F_j * F' \cong F$. Consequently, either $H \cong C(X) * F$ or $H \cong F$. ∎

All of the preliminary results now combine to a proof of our main theorem.

Proof of the Main Theorem: Put $G = \mathrm{Gal}(K)$ and $H = \mathrm{Gal}(E)$. By [HaJ85, Theorem 4.1], $G \cong C(X) * F$, where $X = X(K)$ and F is free of rank $m = |R|$. By Lemma 1.3(a), X is weight m. By Proposition 1.4, any two non-empty open-closed subsets of X are homeomorphic. Hence, by Proposition 2.3, either $H \cong G$ or $H \cong F$.

The first case happens if and only if H contains involutions, that is, by Artin-Schreier theory, if and only if E is formally real. ∎

Remark 2.4: The case where E in the Main Theorem is not formally real has an alternative proof, as noticed by Harbater in [Har07, Thm. 4.2]. His proof relies on a combination of several deep results. In particular, he uses that each finite split embedding problem over E with a nontrivial kernel has as many solutions as the cardinality of R. ∎

References

[Cra74] T. C. Craven, *The topological space of orderings of a rational function field*, Duke Mathematical Journal **41** (1974), 339–347.

[FrJ05] M. D. Fried and M. Jarden, *Field Arithmetic,* 2nd edition, revised and enlarged by M. Jarden, Springer, a series of modern surveys in mathematics, Berlin, 2005.

[GiR73] D. Gildenhuys, L. Ribes, *A Kurosh subgroup theorem for free pro-$\mathcal{C}$-products of pro-$\mathcal{C}$-groups,* Transactions of the AMS **186** (1973), 309–329.

[Har07] D. Harbater, *On function fields with free absolute Galois groups,* manuscript, Philadelphia, 2007.

[HaJ85] D. Haran, M. Jarden, *Real free groups and the absolute Galois group of* $\mathbb{R}(t)$, Journal of Pure and Applied Algebra **37** (1985), 155–165.

[KrN71] W. Krull and J. Neukirch, *Die Struktur der absoluten Galoisgruppe über dem Körper* $\mathbb{R}(t)$, Mathematische Annalen **193** (1971), 197–209.

[Mel90] O.V. Melnikov, *Subgroups and the homology of free products of profinite groups,* Mathematics USSR-Izvestiya **34** (1990), 97–119.

[Pre75] A. Prestel, *Lectures on formally real fields,* Lecture Notes in Mathematics **1093**, Springer, Berlin 1984.

[RiZ00] L. Ribes, P. Zalesskii, *Profinite Groups,* Ergebnisse der Mathematik und ihrer Grenzgebiete **40**, Springer, 2000.

[Sch80] B. Schuppar, *Elementare Aussagen zur Arithmetik und Galoistheorie von Funktionenkörpern,* Journal für die reine und angewandte Mathematik **313** (1980), 59–71.

[Zal92] P. Zalesskii, *Open subgroups of free profinite products,* Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989), Contemporary Mathematics **131** (1992) 473–491.