Algèbre/*Algebra*

The Absolute Galois Group of the Totally Real Numbers

Michael D. FRIED, Dan HARAN and Helmut VÖLKLEIN

Abstract – We determine the absolute Galois group $G_{\mathbb{Q}^{\mathrm{tr}}}$ of the field $\mathbb{Q}^{\mathrm{tr}}$ of totally real algebraic numbers. This group is the free profinite product of groups of order 2 over the Cantor set.

Le groupe de Galois absolu des nombres algébriques totalement réels

Résumé – On détermine le groupe de Galois absolu $G_{\mathbb{Q}^{\mathrm{tr}}}$ du corps $\mathbb{Q}^{\mathrm{tr}}$ des nombres algébriques totalement réels. Ce groupe est le produit profini libre de groupes d'ordre 2 sur l'ensemble de Cantor.

Version française abrégée – Les espaces de modules pour les revêtements de la sphère de Riemann (introduits dans [FV1]) ont la propriété suivante: les points K-rationnels correspondent aux revêtements définis sur K (où K est un sous-corps quelconque de $\mathbb{C}$). De plus, on obtient des solutions à certains problèmes de plongement sur le corps de fonctions rationelles $K(x)$ à partir de points K-rationnels de certains twists de ces espaces de modules.

Dans [FV2], ce principe est utilisé pour montrer que le groupe de Galois absolu $G_K := \mathrm{Gal}(\bar{K}/K)$ d'un corps hilbertien et P(seudo) A(lgébriquement) C(los) K de caractéristique 0 est libre. Dans [FV3], ce résultat est étendu de façon naturelle à la classe des corps hilbertiens P(seudo) R(éel) C(los). Rappelons les définitions suivantes. Un corps K est PAC si toute variété absolument irréductible définie sur K a des points K-rationnels. Un corps K est PRC si toute variété absolument irréductible, non-singulière et définie sur K a des points K-rationnels dès qu'elle a des points rationnels sur toute clôture réelle de K. On prouve [FV3]:

THÉORÈME 0: *Soit K un corps PRC de caractéristique 0. Soit f: $H \to C$ une surjection de groupes finis. Soit $\varphi : G_K \to C$ une surjection telle que, pour toute involution ν de*

G_K, l'élément $\varphi(\nu)$ s'élève à un élément d'ordre ≤ 2 de H. Alors il existe une surjection $\psi : G_{K(x)} \to H$ avec $f \circ \psi = \varphi \circ \mathrm{res}_{\bar{K}}$.

Cette note concerne le corps $\mathbb{Q}^{\mathrm{tr}}$ des nombres algébriques totalement réels (de façon équivalente, le sous-corps de $\bar{\mathbb{Q}}$ fixé par toutes les involutions de $G_{\mathbb{Q}}$)). Le corps $\mathbb{Q}^{\mathrm{tr}}$ est PRC d'après un résultat de Pop [P]. Toute extension finie propre de $\mathbb{Q}^{\mathrm{tr}}$ est un corps hilbertien (Weissauer [FrJ, Prop. 12.4]) et PRC ([Pr, Thm. 3.1]). Donc, d'après [FV3], le groupe de Galois absolu d'un tel corps est connu. Mais le corps $\mathbb{Q}^{\mathrm{tr}}$ n'est pas hilbertien. Nous montrons que $K = \mathbb{Q}^{\mathrm{tr}}$ satisfait une certaine forme affaiblie de la propriété de Hilbert:

LEMME: *Soit $F/K(x)$ une extension galoisienne de degré fini. Supposons que son groupe de Galois soit engendré par des involutions qui se prolongent à des involutions du groupe $G_{K(x)}$. Alors, l'extension $F/K(x)$ admet une spécialisation donnant une extension galoisienne de K ayant le même groupe de Galois.*

Ce lemme nous permet d'appliquer une extension du théorème 0 et de montrer que tous les problèmes de plongement "réels" sur $\mathbb{Q}^{\mathrm{tr}}$ ont une solution. Soit Ω l'ensemble des involutions de $G_{\mathbb{Q}^{\mathrm{tr}}}$.

THÉORÈME: *Soit f: $H \to C$ une surjection de groupes finis et soit $I \subseteq H \setminus \ker(f)$ un ensemble d'involutions clos sous conjugaison. Soit φ: $G_{\mathbb{Q}^{\mathrm{tr}}} \to C$ une surjection telle que $\varphi(\Omega) = f(I)$. Alors, on a un homomorphisme $\chi : G_{\mathbb{Q}^{\mathrm{tr}}} \to H$ tel que $f \circ \chi = \varphi$ et $\chi(\Omega) = I$.*

La condition du Théorème caractérise le groupe de Galois absolu de $\mathbb{Q}^{\mathrm{tr}}$ à isomorphisme près. Il est isomorphe à un produit libre de groupes d'ordre 2 dans la catégorie des groupes profinis.

COROLLAIRE: *Le groupe de Galois absolu $G_{\mathbb{Q}^{\mathrm{tr}}}$ est engendré par un ensemble d'involutions Δ, homéomorphe à l'ensemble de Cantor, avec pour seules relations $\delta^2 = 1$, pour tout $\delta \in \Delta$.*

Introduction.

Let k be a subfield of $\mathbb{C}$, and let $\bar{k}$ be its algebraic closure. Using moduli spaces for covers of the Riemann sphere, one constructs certain varieties defined over k with the following property: k-rational points on these varieties yield solutions of certain embedding problems over the field of rational functions $k(x)$. If k is Hilbertian, specializing yields solutions of embedding problems over k. This gives some information about the absolute Galois group $G_k := \mathrm{Gal}(\bar{k}/k)$ of k.

This principle was applied in [FV2] and [FV3] to "large" Hilbertian fields k—fields over which the existence of rational points on the above varieties is guaranteed. These are the so-called P(seudo) A(lgebraically) C(losed) and P(seudo) R(eal) C(losed) fields. Recall: k is **PRC** if each absolutely irreducible variety defined over k has a k-rational point, provided it has a point over each real closure of k.

The field $\mathbb{Q}^{\mathrm{tr}}$ of all totally real algebraic numbers (equivalently, the fixed field of all involutions in $G_{\mathbb{Q}}$) is PRC by a result of Pop [P]. It follows that every **proper** finite extension k of $\mathbb{Q}^{\mathrm{tr}}$ is Hilbertian (Weissauer [FJ, Prop. 12.4]) and PRC [Pr, Thm. 3.1]. Hence G_k is known by [FV3].

The field $\mathbb{Q}^{\mathrm{tr}}$ is not Hilbertian. However, we show that it satisfies a certain weakening of the Hilbertian property (Lemma 3).

Theorem 4 says that all "real" embedding problems over $\mathbb{Q}^{\mathrm{tr}}$ are solvable. This property characterizes the absolute Galois group of $\mathbb{Q}^{\mathrm{tr}}$ up to isomorphism (Lemma 5). It is freely generated by a set of involutions homeomorphic to the Cantor set.

Compare our result with the Shafarevich conjecture, which says that the absolute Galois group of the full cyclotomic field is free.

In the forthcoming work [FHV] we give various generalizations and applications of the above.

The second author outlined this note and some of its corollaries at the Summer School on Model Theory of Fields, Anogeia (Cretes), August 1992. F. Pop announced another proof of our main result, using rigid geometry, at the Algebra and Number Theory Conference, Essen, December 1992.

The absolute Galois group of the totally real numbers

Let $K = \mathbb{Q}^{\mathrm{tr}}$, and let x be transcendental over K. Let Ω be the set of involutions (elements of order 2) of G_K, and Π the set of involutions of $G_{K(x)}$. Let $\bar{\Omega}$ be the space of conjugacy classes of involutions in G_K, with the quotient topology from Ω. For $\nu \in \Omega$, let $\bar{\nu}$ denote its image in $\bar{\Omega}$. Then $\bar{\Omega}$ is the space of orderings of K. This is homeomorphic to the Cantor set [FV3, final Remark]. Let $\bar{K} = \bar{\mathbb{Q}}$ be the algebraic closure of K, and let $\mathrm{res}_{\bar{K}} : G_{K(x)} \to G_K$ be the restriction. We first improve the main result of [FV3].

Theorem 1: *Let f: $H \to C$ be a surjection of finite groups, and let $I \subseteq H \setminus \ker(f)$ be a set of involutions closed under conjugation. Let $\varphi : G_K \to C$ be a surjection with $\varphi(\Omega) = f(I)$. Then there exists a surjection $\psi : G_{K(x)} \to H$ with $f \circ \psi = \varphi \circ \mathrm{res}_{\bar{K}}$ and $\psi(\Pi) = I$.*

Proof: This is [FV3, Theorem], except for the condition $\psi(\Pi) = I$. We first show how to ensure that $\psi(\Pi) \subseteq I$. By [HJ1, Cor. 6.2] there exists a surjection $q : \tilde{H} \to H$ of finite groups that maps the set $\tilde{I}$ of involutions in $\tilde{H} \setminus \ker(q)$ onto I. Set $\tilde{f} = f \circ q$. Apply [FV3] with f, H, I replaced by $\tilde{f}, \tilde{H}, \tilde{I}$ to get a surjection $\tilde{\psi} : G_{K(x)} \to \tilde{H}$ with $\tilde{f} \circ \tilde{\psi} = \varphi \circ \mathrm{res}_{\bar{K}}$. As $1 \notin f(I) = \varphi(\Omega) = \varphi \circ \mathrm{res}_{\bar{K}}(\Pi) = \tilde{f} \circ \tilde{\psi}(\Pi)$, we have $\tilde{\psi}(\Pi) \subseteq \tilde{H} \setminus \ker(q)$. Thus $\tilde{\psi}(\Pi) \subseteq \tilde{I}$. Set $\psi = q \circ \tilde{\psi}$. Then $f \circ \psi = \varphi \circ \mathrm{res}_{\bar{K}}$ and $\psi(\Pi) \subseteq q(\tilde{I}) = I$.

Let $\bar{I}$ be the (discrete) space of conjugacy classes of elements of I. By [HJ2, Lemma 1.2] there is a continuous surjection $\bar{\lambda} : \bar{\Omega} \to \bar{I}$ with $f(\bar{\lambda}(\bar{\nu})) = \varphi(\bar{\nu})$ for all $\nu \in \Omega$. We may factor $\varphi : G_K \to C$ into surjections $\hat{\varphi} : G_K \to \hat{C}$ and $g : \hat{C} \to C$ with $\hat{C}$ finite, with this property. Two elements of $\bar{\Omega}$ with the same image under $\hat{\varphi}$ have the same image under $\bar{\lambda}$. Set

$$\begin{aligned} \hat{H} = \ & \{(a, b) \in \hat{C} \times H |\ g(a) = f(b)\}, \\ \hat{I} = \ & \{(\hat{\varphi}(\nu), u) |\ \nu \in \Omega,\ u \in \bar{\lambda}(\bar{\nu}),\ \varphi(\nu) = f(u)\}. \end{aligned}$$

Let $\hat{f} : \hat{H} \to \hat{C}$ and $p : \hat{H} \to H$ be the coordinate projections. Note that $\hat{I}$ is a set of involutions in $\hat{H}$ closed under conjugation. For each $\nu \in \Omega$ there is some $u \in \bar{\lambda}(\bar{\nu})$ with $\varphi(\nu) = f(u)$. Therefore, $(\hat{\varphi}(\nu), u) \in \hat{I}$ and $\hat{\varphi}(\Omega) = \hat{f}(\hat{I})$.

The first part of this proof (with $\hat{f}, \hat{H}, \hat{C}, \hat{\varphi}$ replacing f, H, C, φ) gives a surjection $\hat{\psi} : G_{K(x)} \to \hat{H}$ with $\hat{f} \circ \hat{\psi} = \hat{\varphi} \circ \mathrm{res}_{\bar{K}}$ and $\hat{\psi}(\Pi) \subseteq \hat{I}$. Put $\psi = p \circ \hat{\psi} : G_{K(x)} \to H$. This is a surjection, $f \circ \psi = \varphi \circ \mathrm{res}_{\bar{K}}$, and $\psi(\Pi) \subseteq I$.

To complete the proof, take $\mu \in \Pi$, and let $\nu' = \mathrm{res}_{\bar{K}} \mu \in \Omega$. We show that $\psi(\mu) \in \bar{\lambda}(\bar{\nu}')$. Since $\mathrm{res}_{\bar{K}}$: $\Pi \to \Omega$ and $\bar{\lambda} : \bar{\Omega} \to \bar{I}$ are surjective, this implies $\psi(\Pi) = I$.

As $\hat{\psi}(\mu) \in \hat{I}$, we have $\hat{\psi}(\mu) = (\hat{\varphi}(\nu), u)$ for some $\nu \in \Omega$, $u \in \bar{\lambda}(\bar{\nu})$. Here $u = p(\hat{\varphi}(\nu), u) = p \circ \hat{\psi}(\mu) = \psi(\mu)$ and $\hat{\varphi}(\nu) = \hat{f}(\hat{\varphi}(\nu), u) = \hat{f} \circ \hat{\psi}(\mu) = \hat{\varphi}(\nu')$. By the choice of $\hat{\varphi}$ it follows that $\bar{\lambda}(\bar{\nu}) = \bar{\lambda}(\bar{\nu}')$. Thus $\psi(\mu) = u \in \bar{\lambda}(\bar{\nu}')$. ∎

The next lemma follows from [L, Ch. XI, sect. 3].

LEMMA 2: *Let K_0 be an ordered field, and let $\mathcal{K}$ be its real closure. Let M be a finite extension of $K_0(x)$. If M has a $\mathcal{K}$-valued place over K_0 then M is formally real. Conversely, if the ordering of K_0 extends to M, then there is a non-empty open subset A of K_0 (with respect to the order topology) such that each specialization $x \mapsto a \in A$ extends to a $\mathcal{K}$-valued place of M over K_0.*

For a Galois extension M/N, let $I(M/N)$ be the set of involutions of $G(M/N)$ that extend to involutions of G_N. We call these involutions **real**.

Now we state the weak form of Hilbertianity that $K = \mathbb{Q}^{\mathrm{tr}}$ satisfies.

LEMMA 3: *Let L be a finite Galois extension of K, not formally real. Let $F/K(x)$ be a finite Galois extension with $L \subset F$ and $G(F/K(x))$ generated by $I(F/K(x))$. Then there is a Galois extension F' of K containing L, and an isomorphism $\kappa : G(F/K(x)) \to G(F'/K)$ mapping $I(F/K(x))$ onto $I(F'/K)$. Further, $\mathrm{res}_{F'/L} \circ \kappa = \mathrm{res}_{F/L}$.*

Proof: In Claims 1 and 2 we choose a sufficiently large number field K_0 in K. Assume K_0 given for now.

CLAIM 1: There are Galois extensions $F_0/K_0(x)$ and L_0/K_0 such that $F_0 \subset F$ and $L_0 \subset L$ are not formally real, $L_0 \subset F_0$, and the restrictions ρ: $G(F/K(x)) \to G(F_0/K_0(x))$ and $G(L/K) \to G(L_0/K_0)$ are isomorphisms. Further, $\rho(I(F/K(x))) = I(F_0/K_0(x))$.

Proof: Only $\rho(I(F/K(x))) \supseteq I(F_0/K_0(x))$ needs explanation. Every $\iota \in I(F_0/K_0(x))$ extends to some involution $\tilde{\iota} \in G_{K_0(x)}$. Since $K = \mathbb{Q}^{\mathrm{tr}}$, the fixed field of $\mathrm{res}_{\bar{K}} \tilde{\iota}$ contains

K. Hence, $\tilde{\iota}$ restricts to an element of $I(F/K(x))$, and this element restricts via ρ to ι. Thus $\rho(I(F/K(x))) = I(F_0/K_0(x))$.

CLAIM 2: There are $\mu_1, \ldots, \mu_m \in \Pi$ such that $I(F/K(x)) = \mathrm{res}_F\{\mu_1, \ldots, \mu_m\}$, and their images $\nu_1, \ldots, \nu_m \in \Omega$ are pairwise non-conjugate in G_{K_0}.

Proof: The Cantor set $\bar{\Omega}$ has no isolated points and the restriction $\bar{\Pi} \to \bar{\Omega}$ is open. This allows to choose the μ_i so that the ν_i are pairwise non-conjugate in G_K. If K_0 is sufficiently large, they are non-conjugate also in G_{K_0}.

CLAIM 3: There is a Galois extension F_0' of K_0 containing L_0, and an isomorphism $\kappa_0 : G(F_0/K_0(x)) \to G(F_0'/K_0)$ with $\mathrm{res}_{L_0} \circ \kappa_0 = \mathrm{res}_{L_0}$. Further, $\kappa_0(I(F_0/K_0(x))) = I(F_0'/K_0)$.

Proof: There is a Hilbert subset H_0 of K_0 with this property. For all $a \in H_0$ the specialization $x \mapsto a$ extends to an L_0-place $\varphi_a : F_0 \to F_0'$ inducing an isomorphism κ_0 with the desired properties, except, perhaps, the last.

For each $h \in G(F_0/K_0(x))$ let F_0^h be its fixed field. Then $\varphi_a(F_0^h) = (F_0')^{\kappa_0(h)}$. If $\kappa_0(h) \in I(F_0'/K_0)$, then F_0^h has a place in some real closure of K_0. From Lemma 2, F_0^h is formally real. Hence, $h \in I(F_0/K_0(x))$. Conversely, let $h \in I(F_0/K_0(x))$, say, $h = \mathrm{res}_{F_0}\mu_i$. Equip $(F_0)^h$ and K_0 with the orderings induced from the real closed field $\mathcal{K}_i = \overline{K(x)}^{\mu_i}$. By Lemma 2 there is a non-empty $\mathcal{K}_i$-open subset A_i of K_0 with this property. If $a \in A_i$, then $\varphi_a(F_0^h)$ is formally real. In particular, $\kappa_0(h) \in I(F_0'/K_0)$. By Claim 2, the orderings of K_0 induced by the $\mathcal{K}_i$ are pairwise inequivalent. Hence by [G, Lemma 3.4], $\bigcap_i A_i \cap H_0 \neq \emptyset$. Choose a in this set. Then $\kappa_0(I(F_0/K_0(x))) = I(F_0'/K_0)$.

CLAIM 4: $F_0' \cap K = K_0$.

Proof: By hypothesis, $G(F/K(x))$ is generated by its real involutions. By Claim 1 and 3 so is $G(F_0'/K_0)$. However, each $\varepsilon \in I(F_0'/K_0)$ fixes $F_0' \cap K$ (since $K = \mathbb{Q}^{\mathrm{tr}}$ is the fixed field of all involutions in $G_{\mathbb{Q}}$). Hence Claim 4.

CONCLUSION: Set $F' := F_0'K$. Then F' contains $L = L_0K$. From Claim 4 it follows that $G(F'/K_0) = G(F'/F_0') \times G(F'/K)$. Thus $G(F'/K) \cong G(F_0'/K_0))$ via restriction. This is compatible with restriction to L and L_0, respectively, and with real involutions (analogous to Claim 1). Combine this with Claim 1 and 3 for the lemma. ∎

THEOREM 4: *Let $f\colon H \to C$ be a surjection of finite groups, and let $I \subseteq H \setminus \ker(f)$ be a set of involutions closed under conjugation. Let $\varphi\colon G_K \to C$ be a surjection with $\varphi(\Omega) = f(I)$. Then there is a homomorphism $\chi : G_K \to H$ with $f \circ \chi = \varphi$ and $\chi(\Omega) = I$.*

Proof: We may assume that I generates H. Let $\psi : G_{K(x)} \to H$ be as in Theorem 1. Let F (resp., L) be the fixed field of the kernel of ψ (resp., φ). Then $F/K(x)$ and L/K are finite Galois extensions and $L \subset F$. We may assume that $H = G(F/K(x))$, $C = G(L/K)$, $\psi = \mathrm{res}_F$, and $\varphi = \mathrm{res}_L$. Then $I = I(F/K(x))$ and $f = \mathrm{res}_{F/L}$.

As $I(F/K(x))$ generates $G(F/K(x))$, by Lemma 3 there is an isomorphism $\kappa : G(F/K(x)) \to G(F'/K)$ compatible with real involutions and restriction to L. Thus $\chi := \kappa^{-1} \circ \mathrm{res}_{F'} : G_K \to G(F/K(x))$ has the required property. ▮

We rephrase Theorem 4 to say this: All finite real embedding problems for G_K are solvable.

LEMMA 5: *Up to isomorphism, there is at most one profinite group $\mathcal{G}$ of countable rank with the following properties:*

(1) All finite real embedding problems for $\mathcal{G}$ are solvable.

(2) $\mathcal{G}$ is generated by involutions.

(3) $\mathcal{G}$ has a subgroup $\mathcal{G}_1$ of index 2 that contains no involution.

Proof: Suppose $\mathcal{G}'$ is another group with the same properties. The construction in [FJ, Lemma 24.1] produces sequences of open normal subgroups

$$\mathcal{G} = \mathcal{G}_0 > \mathcal{G}_1 > \mathcal{G}_2 > \cdots \qquad \text{and} \qquad \mathcal{G}' = \mathcal{G}'_0 > \mathcal{G}'_1 > \mathcal{G}'_2 > \cdots$$

each with trivial intersection, and compatible isomorphisms $\kappa_i : \mathcal{G}/\mathcal{G}_i \to \mathcal{G}'/\mathcal{G}'_i$. (In the present situation, these isomorphisms map real involutions onto real involutions.) They glue together to yield an isomorphism $\mathcal{G} \to \mathcal{G}'$. ▮

The free (profinite) product of a family of groups of order 2 indexed by the Cantor set satifies the conditions of Lemma 5 (see [HJ3]). So does $G_{\mathbb{Q}^{\mathrm{tr}}}$: It has countable rank since $\mathbb{Q}^{\mathrm{tr}}$ is countable; $G_{\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})}$ contains no involution; and the embedding property follows from Theorem 4.

Corollary 6: *The absolute Galois group $G_{\mathbb{Q}^{\mathrm{tr}}}$ is generated by a subset Δ of involutions, homeomorphic to the Cantor set, subject only to the relations $\delta^2 = 1$ for $\delta \in \Delta$.*

References

[FJ] M. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik III **11**, Springer Verlag, Heidelberg, 1986.

[FHV] M. Fried, D. Haran and H. Völklein, *Real hilbertianity and the field of totally real numbers,* a preprint.

[FV1] M. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces,* Math. Ann. **290** (1991), 771–800.

[FV2] M. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field,* Annals of Math. **135** (1992), 469–481.

[FV3] M. Fried and H. Völklein, *The absolute Galois group of a Hilbertian PRC field,* to appear in Israel J. of Math.

[G] W.-D. Geyer, *Galois groups of intersections of local fields,* Israel J. Math. **30** (1978), 382–396.

[HJ1] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed field,* Annali della Scuola Normale Superiore — Pisa, Serie IV, **12** (1985), 449–489.

[HJ2] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed algebraic field,* Pacific J. Math. **123** (1986), 55–69.

[HJ3] D. Haran and M. Jarden, *Real free groups and the absolute Galois group of $\mathbb{R}(t)$,* J. of Pure and Applied Algebra **37** (1985), 155–165.

[L] S. Lang, *Algebra,* Addison-Wesley, sixth printing 1974.

[P] F. Pop, *Fields of totally Σ-adic numbers,* a preprint.

[Pr] A. Prestel, *Pseudo real closed fields,* Set Theory and Model Theory, Lecture Notes **872** (1981), 127–156, Springer Verlag.

M.D.F. : *UC Irvine, Irvine, CA 92717, USA,* e-mail: mfried@math.uci.edu;
D.H. : *Max-Planck-Institut für Mathematik, Bonn and*
Tel-Aviv University, Tel-Aviv 69978, Israel, e-mail: haran@math.tau.ac.il;
H.V. : *University of Florida, Gainesville, FL 32611, USA and*
Universität Erlangen, Germany, e-mail: helmut@math.ufl.edu.