REAL FREE GROUPS AND THE ABSOLUTE GALOIS GROUP OF $\mathbb{R}(t)$

Dan HARAN
Mathematisches Institut, Bismarckstr. 1 1/2, D-8520 Erlangen, West Germany

Moshe JARDEN*
School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel

Communicated by K.W. Gruenberg
Received 14 July 1983
Revised 26 March 1984

Introduction

The following four notions are well known to be strongly connected with each other: PAC (pseudo algebraically closed) fields, projective groups, the fields $C(t)$, where C is an algebraically closed field of characteristic zero and free profinite groups.

Indeed, the absolute Galois group $G(K)$ of every PAC field K is projective. Conversely, for every projective group G there exists a PAC field K such that $G(K)\cong G$. Also, a profinite group is projective if and only if it is isomorphic to a closed subgroup of a free profinite group, and $G(C(t))$ is free.

In our work [6] we generalize this situation and add the adjective 'real' to the first two results. Relying on a suitable definition of PRC (pseudo real closed) fields we define real projective groups and prove: *If K is a PRC field, then $G(K)$ is real projective; if G is a real projective group, then there exists a PRC field K such that $G(K)\cong G$.*

The aim of the present note is to establish the 'real' analogue of the two remaining notions and results. We define real free groups and show that a profinite group is real projective if and only if it is isomorphic to a closed subgroup of a real free group. We also discuss some basic properties of real free groups and point out that, analogously to free profinite groups, every real free group is an inverse limit of finitely generated real free groups. Combining this observation with well-known results of Krull and Neukirch [7] and Schuppar [10] we deduce that for every real closed field R the group $G(R(t))$ is real free.

* Partially supported by the fund for Basic Research administered by the Israel Academy of Sciences and Humanities.

1. Real free groups

Free profinite groups over compact spaces are introduced in [4, Proposition 1.3]. The appropriate concept in our context involves involutions.

Definition 1.1. A profinite group $\hat{D}$ is said to be *real free* if it contains disjoint closed subsets X and Y such that $X \subseteq \mathrm{Inv}(\hat{D})$; $1 \in Y$; and

(*) every continuous map φ from $X \cup Y$ into a profinite group G, such that $\varphi(x)^2 = 1$ for every $x \in X$ and $\varphi(1) = 1$, extends to a unique homomorphism of $\hat{D}$ into G.

The pair of Boolean spaces (X, Y) is said to be a *basis* of $\hat{D}$.

It may be noted that $\hat{D}$ is a free profinite product in the sense of Gildenhuys-Ribes [5], where the underlying pointed topological space is $X \cup Y$, and $A_x = \{1, x\} \cong \mathbb{Z}/2\mathbb{Z}$ for every $x \in X$ and $A_y = \langle y \rangle \cong \hat{\mathbb{Z}}$ for every $y \in Y - \{1\}$. Nevertheless the above direct definition simplifies the derivation of the properties of real free groups needed in the sequel.

It is easy to see that the definition of real free groups does no change, if we write 'finite' instead of 'profinite' in (*); we shall often use this modified version of Definition 1.1.

In order to construct real free groups, let X and Y be two Boolean spaces and let e be a distinguished point of Y. Consider the Boolean space $Z = X \cup Y$ (such that X and Y are disjoint closed-open subspaces of Z) and let D be the free discrete group on the set Z. Denote by $\mathcal{N}$ the family of normal subgroups N of D of finite index such that $e \in N$ and $x^2 \in N$ for every $x \in X$ and such that $Z \cap dN$ is open in Z for every $d \in D$. Let $\hat{D} = \varprojlim D/N$, where N ranges over $\mathcal{N}$, be the corresponding completion of D and $\hat{i}: D \to \hat{D}$ the natural completion map. Its restriction i to Z is clearly continuous.

Lemma 1.2. *The map $i: Z \to \hat{D}$ satisfies:*

(a) *$i(e) = 1$, $i(x)^2 = 1$ for every $x \in X$, and $\hat{D} = \langle i(Z) \rangle$.*

(b) *Let $\varphi_0: Z \to G$ be a continuous map into a finite group G such that $\varphi_0(e) = 1$ and $\varphi_0(x)^2 = 1$ for every $x \in X$. Then there exists a unique continuous homomorphism $\varphi: \hat{D} \to G$ such that $\varphi_0 = \varphi \circ i$.*

(c) *Let z, z' be distinct elements of Z; then $i(z)$ is not conjugate to $i(z')$ in $\hat{D}$.*

Proof. (a) and (b) are clear.

(c) W.l.o.g. assume $z \neq e$. There exists a closed-open subset U of Z such that $z \in U$ and $z', e \notin U$. The continuous map $\varphi_0: Z \to \{\pm 1\}$, given by $\varphi_0(U) = -1$ and $\varphi_0(Z - U) = 1$, defines, by (b), a homomorphism $\varphi: \hat{D} \to \{\pm 1\}$ such that $\varphi(i(z)) = -1$ and $\varphi(i(z')) = 1$. Thus $i(z)$ is not conjugate to $i(z')$. □

Lemma 1.3. *Let X and Y be two disjoint Boolean spaces and e a distinguished point*

of Y. Then there exists a unique real free group $\hat{D}(X, Y, e)$ with the basis (X, Y) such that e coincides with the unit element of $\hat{D}(X, Y, e)$. Moreover:

(a) *the set $X \cup Y$ (topologically) generates $\hat{D}(X, Y, e)$;*

(b) *let $z, z' \in X \cup Y$; then z is conjugate to z' if and only if $z = z'$.*

Proof. The uniqueness of $\hat{D}(X, Y, e)$ (up to a unique isomorphism) is clear. To establish its existence consider the construction discussed in Lemma 1.2 and put $\hat{D}(X, Y, e) = \hat{D}$. The map $i : Z \to \hat{D}$ is injective, by 1.2(c), hence a homeomorphism of Z onto $i(Z)$. Thus we may assume that Z is a closed subset of $\hat{D}$ and i is the inclusion. By 1.2(a) we have $e = 1$, and $\hat{D} = \langle Z \rangle$. If $x \in X$, then $x \neq e = 1$, hence x is an involution of $\hat{D}$, by 1.2(a). Property (*) of Definition 1.1 is 1.2(b), and (b) of our Lemma is 1.2(c). □

Examples of real free groups. In most of our applications the Boolean space Y is the one-point-compactification $Y = S \cup \{e\}$ of a discrete space S. In such a case we write $\hat{D}(X, S)$ instead of $\hat{D}(X, Y, e)$.

(a) $\hat{D}(\emptyset, Y, e)$ is precisely the free profinite group $\hat{F}(Y, e)$ generated by the pointed Boolean space (Y, e) [4, Proposition 1.3]. In particular, $\hat{D}(\emptyset, S)$ is the (restricted) free group on a set S.

(b) Let X and S be finite sets of k and l elements, respectively. Then $\hat{D}(X, S)$ is the free product $\hat{D}_{k,l}$ (in the category of profinite groups) of k copies of $\mathbb{Z}/2\mathbb{Z}$ and l copies of $\hat{\mathbb{Z}}$ (it has been denoted as $\hat{D}_{k,k+l}$ and studied in [6, Section 6]).

2. The rank of real free groups

Recall that the *rank* of a profinite group G is the least cardinal of a set of (topological) generators of G converging to 1 (Ribes [9, Definition 6.7]).

Lemma 2.1. *The real free group on a basis (X, Y) is finitely generated if and only if both X and Y are finite, in which case its rank is $|X| + |Y| - 1$.*

Proof. The real free group $\hat{D}$ on a basis (X, Y) is generated by $X \cup (Y - \{1\})$ hence $\operatorname{rank}(\hat{D}) \leq |X| + |Y| - 1$. Thus it suffices to show for every $n \in \mathbb{N}$ that if $|X \cup Y| \geq n + 1$, then $\operatorname{rank}(\hat{D}) \geq n$. Now, there exist disjoint closed-open subsets $V_0, V_1, \ldots, V_n$ of Z such that $Z = V_0 \cup \cdots \cup V_n$, and $1 \in V_0$. Let $\varepsilon_1, \ldots, \varepsilon_n$ generate the direct product C of n copies of $\mathbb{Z}/2\mathbb{Z}$. Then the map $\varphi : Z \to C$, given by $\varphi(V_i) = \varepsilon_i$, for $i = 1, \ldots, n$ and $\varphi(V_0) = 1$, extends to an epimorphism $\hat{D} \to C$. This implies that $\operatorname{rank}(\hat{D}) \geq \operatorname{rank}(C) = n$. □

This characterization may be generalized as follows. Recall that the *weight* of a topological space is the least cardinality of a base for its topology. Thus the weight of a finite Boolean space is equal to the number of its elements. The weight of an

infinite Boolean space is equal to the cardinality of the family of its closed-open subsets (since every closed-open subset is compact and hence a finite union of basic sets). The weight of an infinite profinite group G is therefore equal to the cardinality of the family $\mathcal{N}$ of its open normal subgroups. In particular, if G is not finitely generated, then $\text{weight}(G)=\text{rank}(G)$. Indeed, let $A\subseteq G$ be a set of generators converging to 1, of the least (infinite) cardinality. Then A is a discrete subspace of G, hence clearly $|A|\leq\text{weight}(G)$. Conversely, for every finite subset S of A we have $|\{N\in\mathcal{N}\,|\,A-N=S\}|\leq\aleph_0$, hence

$$\text{weight}(G)=|\mathcal{N}|\leq|\{S\subseteq A\,|\,S \text{ is finite}\}|=|A|.$$

Lemma 2.2. *Let $\hat{D}$ be a real free group and let (X, Y) be its basis. Then*

$$\text{rank}(\hat{D})+1=\text{weight}(X\cup Y).$$

Proof. By Lemma 2.1 we may assume that $Z=X\cup Y$ is infinite, whence $\hat{D}$ is not finitely generated; we want to show that $\text{rank}(\hat{D})=\text{weight}(Z)$.

As $Z\subseteq\hat{D}$, we have: $\text{weight}(Z)\leq\text{weight}(\hat{D})=\text{rank}(\hat{D})$. Conversely, let $\mathcal{M}$ be the family of continuous maps from Z into finite groups and let $\mathcal{E}$ be the family of continuous epimorphisms from $\hat{D}$ onto finite groups. Then

$$\text{rank}(\hat{D})=|\{N\lhd\hat{D}\,|\,N \text{ is open in } \hat{D}\}|\leq|\mathcal{E}|,$$

and $|\mathcal{E}|\leq|\mathcal{M}|$, since the mapping from $\mathcal{E}$ to $\mathcal{M}$, defined by restriction of functions to Z, is injective, since $\hat{D}=\langle Z\rangle$. Let $\mathcal{P}$ be the family of finite collections of closed-open subsets of Z. Every $f: Z\to G$ in $\mathcal{M}$ defines an element of $\mathcal{P}$, namely $\{f^{-1}(g)\,|\,g\in G\}$. The map from $\mathcal{M}$ into $\mathcal{P}$ defined in this manner has countable fibers (since there are countably many finite groups), hence $|\mathcal{M}|\leq|\aleph_0||\mathcal{P}|=|\mathcal{P}|$. Clearly $|\mathcal{P}|=\text{weight}(Z)$. Thus $\text{rank}(\hat{D})\leq\text{weight}(Z)$. □

3. Inverse limits of finitely generated real free groups

We show that every real free group $\hat{D}(X, Y, e)$ is an inverse limit of finitely generated real free groups.

Let $Z=X\cup Y$. Recall that a *partition* Z_0 of Z is a finite collection $Z_0=\{B_1,\ldots,B_n\}$ of disjoint nonempty closed-open subsets of Z such that $Z=B_1\cup\cdots\cup B_n$. Furthermore, a partition Z_1 is said to be *finer* than Z_0 if for every $V'\in Z_1$ there exists a $V\in Z_0$ such that $V'\subseteq V$. An (X, Y)-*partition* is simply a partition of Z finer than the partition $\{X, Y\}$.

Let $\mathcal{P}=\{Z_i\,|\,i\in I\}$ be a family of (X, Y)-partitions. To every $i\in I$ there corresponds a continuous surjection $p_i: Z\to Z_i$, defined by: $p_i(z)=V$ if $z\in V$, for every $z\in Z$ and every $V\in Z_i$. Let $X_i=p_i(X)$, $Y_i=p_i(Y)$ and $e_i=p_i(e)$; then $Z_i=X_i\cup Y_i$ and the map p_i extends to a unique epimorphism $p_i:\hat{D}(X, Y, e)\to\hat{D}(X_i, Y_i, e_i)$. If

$Z_j \in \mathscr{P}$ is finer than Z_i – in which case we write $j \geq i$ – then there exists a unique surjection $p_{ji}: Z_j \to Z_i$ such that $p_{ji} \circ p_j = p_i$. In particular $p(X_j) = X_i$, $p(Y_j) = Y_i$ and $p_{ji}(e_j) = e_i$, so p_{ji} extends to a unique epimorphism $p_{ji}: \hat{D}(X_j, Y_j, e_j) \to \hat{D}(X_i, Y_i, e_i)$; moreover, $p_{ji} \circ p_j = p_i$, by the universal property of $\hat{D}(X, Y, e)$.

In this notation we may state:

Proposition 3.1. *The group $\hat{D}(X, Y, e)$ is an inverse limit of finitely generated real free groups. More specifically, let $\mathscr{P} = \{Z_i \mid i \in I\}$ be a family of (X, Y)-partitions such that for every partition Z_0 of $X \bigcup Y$ there exists a $Z_i \in \mathscr{P}$ finer than Z_0. Then $\mathscr{P}$ defines an inverse system $\langle \hat{D}(X_i, Y_i, e_i), p_{ji} \rangle_{i,j \in I}$ and a compatible family of epimorphisms $p_i: \hat{D}(X, Y, e) \to \hat{D}(X_i, Y_i, e_i)$, $i \in I$. These induce an isomorphism $p: \hat{D}(X, Y, e) \to \varprojlim_{i \in I} \hat{D}(X_i, Y_i, e_i)$.*

Proof. The map p is surjective, since $\{p_i\}$ are surjective. We have to show that p is injective (i.e., $\bigcap_{i \in I} \mathrm{Ker}(p_i) = 1$). Denote $\hat{D} = \hat{D}(X, Y, e)$, let N be an open normal subgroup of $\hat{D}$ and $\pi: \hat{D} \to \hat{D}/N$ the quotient map. By assumption there exists an $i \in I$ such that Z_i is finer than the partition $\{\sigma N \cap Z \mid \sigma \in \hat{D}, \sigma N \cap Z \neq \emptyset\}$ of $Z = X \cup Y$. By the universal property of $\hat{D}(X_i, Y_i, e_i)$, there exists a homomorphism $\pi_i: \hat{D}(X_i, Y_i, e_i) \to \hat{D}/N$ such that $\pi_i \circ p_i = \pi$; hence $\bigcap \mathrm{Ker}(p_i) \subset \mathrm{Ker}(\pi) = N$. □

Corollary 3.2. *The set X is a complete system of representatives of conjugacy classes of involutions in $\hat{D} = \hat{D}(X, Y, e)$. For every involution ε of $\hat{D}$ we have*

$$\{\sigma \in \hat{D} \mid \varepsilon^\sigma = \varepsilon\} = \{1, \varepsilon\}.$$

Proof. If $X \cup Y$ is finite, then our corollary is a reformulation of Proposition 6.1 of [6].

The general case follows from the finite case and from Proposition 3.1 by a routine compactness argument. Use also Lemma 1.3(b). □

We recall [6, Section 7] that a profinite group G is *real projective* if:

(a) $\mathrm{Inv}(G)$ is closed in G.

(b) Let $\alpha: B \to A$ be an epimorphism of finite groups and let $\varphi: G \to A$ be a homomorphism such that for every $\delta \in \mathrm{Inv}(G) - \mathrm{Ker}(\varphi)$ there exists an $\varepsilon \in \mathrm{Inv}\, B$ for which $\alpha(\varepsilon) = \varphi(\delta)$. Then there exists a homomorphism $\gamma: G \to B$ such that $\alpha \circ \gamma = \varphi$.

Corollary 3.3. *The group $\hat{D}(X, Y, e)$ is real projective.*

Proof. Let $G = \hat{D}(X, Y, e)$. By Corollary 3.2 the set $\mathrm{Inv}(G)$ is the image of the compact set $X \times G$ under the map $(x, \sigma) \to x^\sigma$, hence compact. Let α and φ be as in (b) above. By assumption there exists a section $\vartheta: A \to B$ of α such that $[\vartheta \circ \varphi(x)]^2 = 1$ for evey $x \in X$. The restriction of $\vartheta \circ \varphi$ to $X \cup Y$ can be extended to a unique homomorphism $\gamma: G \to B$. We have $\alpha \circ \gamma = \varphi$, since

$$\mathrm{res}_{X\cup Y}\,\alpha\circ\gamma=\mathrm{res}_{X\cup Y}\,\alpha\circ\vartheta\circ\varphi=\mathrm{res}_{X\cup Y}\,\varphi. \qquad \square$$

Proposition 3.4. *Let $\hat{D}(X, Y, e)$ be a real free group and let X', Y' be closed subsets of X, Y, respectively, such that $1=e\in Y'$. Then the closed subgroup $\langle X'\cup Y'\rangle$ of $\hat{D}(X:Y, e)$ is real free with the basis (X', Y').*

Proof. Denote $Z=X\cup Y$ and $Z'=X'\cup Y'$. Let φ be a continuous map from Z' into a finite group G such that $\varphi(x)^2=\varphi(e)=1$ for every $x\in X'$. It suffices to show that φ extends to a continuous map $\psi: Z\to G$ such that $\psi(x)^2=1$ for every $x\in X$. Indeed, ψ extends to a homomorphism $\psi:\hat{D}(X, Y, e)\to G$ and is restriction to $\langle Z'\rangle$ extends φ; the extension of φ to $\langle Z'\rangle$ is of course unique. Thus

$$\langle Z'\rangle=\hat{D}(X', Y', e)\rangle.$$

The Boolean space Z possesses a basis consisting of closed-open subsets. Since Z' inherits its topology from Z, there exists an (X, Y)-partition Z_0 of Z such that for every $V\in Z_0$ either $V\cap Z'=\emptyset$ or $V\cap Z'\subseteq\varphi^{-1}(g)$ for a unique $g'\in G$. Define $\psi: Z\to G$ as follows: Let $V\in Z_0$; if $V\cap Z'\subseteq\varphi^{-1}(g)$, let $\psi(z)=g$ and if $V\cap Z'=\emptyset$, let $\psi(z)=1$, for every $z\in V$. Then ψ has the required property. $\square$

To deduce the next result we need a lemma, which is an easy corollary of some of the deeper theorems of [6].

Lemma 3.5. *Let P and G be real projective groups.*

(a) *There exists a closed system of representatives of the conjugacy classes of* $\mathrm{Inv}(G)$.

(b) *Let $\alpha: P\to G$ be a continuous epimorphism and let X be a system of representatives of the conjugacy classes of* $\mathrm{Inv}(P)$. *If α maps X bijectively onto a system of representatives of the conjugacy classes of* $\mathrm{Inv}(G)$, *then there exists a continuous monomorphism $\gamma: G\to P$ such that $\alpha\circ\gamma=\mathrm{id}_G$.*

Proof. By [6, Proposition 7.7] there exists an open subgroup G' of index ≤ 2 in G such that $G'\cap(\mathrm{Inv}\,G)=\emptyset$ and $\mathbf{G}=\langle G, G', \mathrm{Inv}\,G\xrightarrow{\text{incl.}}G\rangle$ is a projective Artin-Schreier structure. Thus (a) follows from [6, Corollary 9.2(i)].

Let $P'=\alpha^{-1}(G)$. Then $(P:P')\le 2$ and $P'\cap\mathrm{Inv}(P)=\emptyset$, since $P'\cap X=\emptyset$. Again, by [6, Proposition 7.7] $\mathbf{P}=\langle P, P', \mathrm{Inv}(P)\longrightarrow P\rangle$ is a projective Artin-Schreier structure. Condition (b) implies that $\alpha(\mathrm{Inv}(P))=\mathrm{Inv}(G)$ and that α may be viewed as a cover of Artin-Schreier structures. By the projectivity of $\mathbf{G}$ there exists a morphism $\gamma:\mathbf{G}\to\mathbf{P}$ such that $\alpha\circ\gamma=\mathrm{id}_{\mathbf{G}}$. In particular there exists a continuous homomorphism $\gamma: G\to P$ such that $\alpha\circ\gamma=\mathrm{id}_G$. $\square$

Theorem 3.6. *A profinite group G is real projective if and only if G is isomorphic to a closed subgroup of a real free group.*

Proof. Let G be real projective. Choose a closed system X of representatives of the conjugacy classes of $\mathrm{Inv}(G)$ and let $Y=G$ with $e=1$. Let $P=\hat{D}(X, Y, e)$; the identity inclusions of X and Y into G extend to an epimorphism $\alpha: P\to G$. By Corollary 3.3 and Lemma 3.5(b) there exists an embedding of G into P.

Conversely, every real free group P is real projective, by Corollary 3.3. Therefore, by [6, Corollary 10.5], every closed subgroup of P is real projective. □

4. The absolute Galois group of $\mathbb{R}(t)$

Let R be a real closed field and $F=R(t)$ the field of rational functions in one variable over R. The aim of this section is to show that the absolute Galois group of F is real free. This result relies on a characterization of $G(F)$ found by Krull and Neukirch [7] in the case that R is the field of real numbers, and on a generalization of this characterization to an arbitrary real closed field R (Schuppar [10]).

We need a few facts about the space $X(F)$ of orderings of F.

It is not difficult to show (see [8, Theorem 6.5] and [1, Corollary 9 and Proposition 12]) that $X(F)$ is a Boolean space under the Harrison topology given by the basis consisting of

$$\{x\in X(F)\,|\,t<_x b\} \quad \text{where } b\in R, \tag{1}$$

$$\{x\in X(F)\,|\,a<_x t\} \quad \text{where } a\in R, \tag{2}$$

$$\{x\in X(F)\,|\,a<_x t<_x b\} \quad \text{where } a<b\in R. \tag{3}$$

It follows that for every partition X_0 of $X(F)$ there exists a partition X_1 finer than X_0, of the form

$$\{\{x\,|\,t<_x a_1\},\{x\,|\,a_1<_x t<_x a_2\},\ldots,\{x\,|\,a_n<_x t\}\}, \quad \text{where } a_1<\cdots<a_n\in R.$$

Let us denote by $x(+\infty), x(-\infty), x(a+), x(a-)$, where $a\in R$, those orderings of F, for which $t, -t, 1/(t-a), 1/(a-t)$, respectively, is infinitely large with respect to R.

Next, let us fix some notation concerning prime divisors of $R(t)/R$. These are of three types:

(a) real primes, $\mathfrak{p}_a$, of degree 1, one for each $a\in R$, corresponding to the specialization $t\to a$;

(b) complex primes, $\mathfrak{p}_c$, of degree 2, one for each $c=a+b\sqrt{-1}$, with $a, b\in R$ and $b>0$, corresponding to the specialization $t\to c$;

(c) the prime $\mathfrak{p}_\infty$ of degree 1, which is infinite at t.

Theorem 4.1. *Let R be a real closed field and let t be a transcendental element over R. Denote by X the space of orderings of $R(t)$ and let $H=\{a+b\sqrt{-1}\,|\,a, b\in R \,\&\, b>0\}$. Then $G(R(t))\cong\hat{D}(X, H)$.*

Moreover, an isomorphism $\vartheta:\hat{D}(X, H)\to G(R(t))$ can be defined such that for

each $a \in R$ and $b \in H$ the groups $\vartheta(x(a+), x(a-))$ and $\vartheta(b)$ are the decomposition groups in $G(R(t))$ of primes lying over $\mathfrak{p}_a$ and $\mathfrak{p}_b$, respectively.

Proof. We show that $G(R(t))$ and $\hat{D}(X, H)$ are inverse limits of isomorphic inverse systems of finitely generated profinite groups.

Part A: *The inverse sysem for* $G(R(t))$.

For every finite subset S of $R \cup H$ let $R(t)_S$ be the maximal normal extension of $R(t)$ unramified at $\{\mathfrak{p}_a \mid a \in R \cup H \cup \{\infty\} - S\}$ and denote $G(S) = \mathcal{G}(R(t)_S/R(t))$. If $S \subseteq S'$, then $R(t)_S \subseteq R(t)_{S'}$, hence the restriction map $\mathrm{Res}_{S'/S}: (G(S') \to G(S)$ is an epimorphism. Thus $\langle G(S), \mathrm{Res}_{S'/S}\rangle_{S,S'}$ is an inverse system and $G(R(t)) \cong \varprojlim G(S)$.

Part B: *The inverse system for* $\hat{D}(X, H)$.

Let Y be the one-point compactification of the discrete space H. With every finite subset S of $R \cup H$ we associate an (X, Y)-partition in the following way. Let $e(S) = Y - (S \cap H)$ and for each $a \in S \cap H$ let $y(S, a) = \{a\}$. Then $Y(S) = \{y(S, a) \mid a \in S \cap H\} \cup \{e(S)\}$ is a partition of Y. If $a_1 < \cdots < a_k$ are the elements of $S \cap R$, denote $x_0(S) = \{x \in X \mid t <_x a_1\}$, $x_i(S) = \{x \in X \mid a_i <_x t <_x a_{i+1}\}$ for $i = 1, \ldots, k-1$ and $x_k(S) = \{x \in X \mid a_k <_x t\}$. Then $X(S) = \{x_0(S), \ldots, x_k(S)\}$ is a partition of X. The union $X(S) \cup Y(S)$ is an (X, Y)-partition. Clearly, $x(a_i -) \in x_{i-1}(S)$ and $x(a_i +) \in x_i(S)$; if $a \in S \cap H$, then $a \in y(S, a)$. Note that for every partition Z_0 of $X \cup Y$ there exists a set S such that $X(S) \cup Y(S)$ is finer than Z_0.

If $S \subseteq S'$, then the partition $X(S') \cup Y(S')$ is finer than $X(S) \cup Y(S)$, hence there exists a canonical map

$$p_{S'/S}: X(S') \cup Y(S') \to X(S) \cup Y(S)$$

given by $p_{S'/S}(V') = V$ if $V' \subseteq V$. This map uniquely extends to an epimorphism

$$p_{S'/S}: \hat{D}(X(S'), Y(S'), e(S')) \to \hat{D}(X(S), Y(S), e(S)).$$

By Proposition 3.1, we know that $\langle \hat{D}(X(S), Y(S), e(S)), p_{S'/S}\rangle_{S,S'}$ is an inverse system and $\hat{D}(X, H) \cong \varprojlim \hat{D}(X(S), Y(S), e(S))$.

Thus our theorem follows from the following lemma.

Lemma 4.2. *For every finite subset S of $R \cup H$ there exists an isomorphism*

$$\vartheta_S: \hat{D}(X(S), Y(S), e(S)) \to G(S)$$

such that for every $S \subseteq S'$ the following diagram commutes

$$\begin{array}{ccc} \hat{D}(X(S'), Y(S'), e(S')) & \xrightarrow{\vartheta_{S'}} & G(S') \\ \downarrow{\scriptstyle p_{S'/S}} & & \downarrow{\scriptstyle \mathrm{Res}_{S'S}} \\ \hat{D}(X(S), Y(S), e(S)) & \xrightarrow[\vartheta_S]{} & G(S) \end{array}$$

Moreover, for each $a=a_i\in S\cap R$, *where* $1\le i\le k$, *and each* $b\in S\cap H$ *the groups* $\vartheta\langle x_{i-1}(S), x_i(S)\rangle$ *and* $\theta\langle y(S,b)\rangle$ *are the decomposition groups in* $G(S)$ *of primes lying over* $\mathfrak{p}_a$ *and* $\mathfrak{p}_b$, *respectively.*

Proof of Lemma 4.2. Again, we proceed by parts.

Part C: *Generators and relations for* $G(S)$.

The group $G(S)$ possesses a system of generators $\{\varphi(S), \tau(S,a)\,|\,a\in S\}$ with defining relations (we omit the reference to S if no confusion arises):

$$\sigma^2=1, \tag{1}$$

$$\sigma\tau(a_i)\sigma=\tau(a_1)^{-1}\cdots\tau(a_{i-1})^{-1}\tau(a_i)^{-1}\tau(a_{i-1})\cdots\tau(a_1), \tag{2}$$

for $1\le i\le k$, where $a_1<\cdots<a_k$ are the elements of $S\cap R$ (see [7, Satz 2] and [10, Satz 3.1]). Moreover,

$$\tau(a)\in G(R(t,\sqrt{-1})) \quad \text{for all } a\in S, \tag{3}$$

(4) for each $a\in S$ there exists a prime of $R(t)_S$ lying over $\mathfrak{p}_a$ such that its decomposition group in $G(S)$ is $\langle\tau(a)\rangle$ if $a\in S\cap H$, and $\langle\tau(a_i),\tau(a_{i-1})\cdots\tau(a_1)\sigma\rangle$ if $a=a_i\in S\cap R$.

It should be remarked that Schuppar does not include (3) in his account [10, Satz 3.1] of $G(S)$. Nevertheless, this property can be easily attained using the method of his paper, since it holds for $R=\mathbb{R}$ (see [7, p. 206, line 3]) and can be elementarily expressed.

Note that if a system $\{\sigma',\tau'(a)\,|\,a\in S\}$ of generators of $G(S)$ satisfies relations (1) and (2), then these are defining relations for $G(S)$. Indeed, the map $\sigma\to\sigma'$ and $\tau(a)\to\tau'(a)$ for $a\in S$ extends to an endomorphism of $G(S)$, which is necessarily an automorphism (see [9, p. 68]).

Part D: *The restriction map.*

Observe that if $S\subseteq S'$ and $\{\sigma,\tau(a)\,|\,a\in S'\}$ satisfies (1)–(4), then $\mathrm{Res}_{S'/S}\,\tau(a)=1$, for every $a\in S'-S$. Indeed, let $\bar{\mathfrak{p}}$ be the prime of $C(t)=R(t,\sqrt{-1})$ lying over $\mathfrak{p}_a$. By (3) and (4) we know that $\tau(a,S')$ belongs to the decomposition group $H\le\mathcal{G}(R(t)_{S'}/C(t))$ of a prime $\mathcal{P}$ of $R(t)_{S'}$ lying over $\bar{\mathfrak{p}}$. But H is also the inertia group of $\mathcal{P}$ in $\mathcal{G}(R(t)_{S'}/C(t))$, since $\bar{\mathfrak{p}}$ and have $\mathcal{P}$ have the same residue field. Therefore $\mathrm{Res}_{S'/S}\,H=\{1\}$, since $\bar{\mathfrak{p}}$ is unramified in $R(t)_S$.

A slight modification of the proof of [7, Satz 3] shows that it is possible to choose for every S a system of generators $\{\sigma(S),\tau(S,a)\,|\,a\in S\}$ of $G(S)$ that satisfies (1)–(4) and such that:

(5) If $S\subseteq S'$, then the restriction map $\mathrm{Res}_{S'/S}: G(S')\to G(S)$ is given by $\mathrm{Res}_{S'/S}\,\sigma(S')=\sigma(S)$ and

$$\mathrm{Res}_{S'/S}\,\tau(S',a)=\begin{cases}\tau(S,a) & \text{for } a\in S,\\ 1 & \text{for } a\in S'-S.\end{cases}$$

We assume in the sequel that this has been done.

Part E: *Construction of the isomorphism* ϑ_S.
Define $\vartheta_S : X(S) \cup Y(S) \to G(S)$ by:

$$\vartheta_S(e) = 1,$$

$$\vartheta_S(y(a)) = \tau(a) \quad \text{for } a \in S \cap H, \quad \text{and}$$

$$\vartheta_S(x_i) = \tau(a_i)\tau(a_{i-1}) \cdots \tau(a_1)\sigma \quad \text{for } 0 \le i \le k.$$

Then for every $S \subseteq S'$

$$\mathrm{Res}_{S'/S} \circ \vartheta_{S'} = \vartheta_S \circ p_{S'/S} \tag{6}$$

holds on $X(S') \cup Y(S')$. Moreover, by (1) and (2), $\vartheta_S(x_i)^2 = 1$, for $0 \le i \le k$. By the universal property of free real groups the map ϑ_S uniquely extends to a homomorphism such that (6) holds on $\hat{D}(X(S'), Y(S'), e(S'))$ for all $S \subseteq S'$. Note that

$$\vartheta_S\langle x_{i-1}, x_i\rangle = \langle \tau(a_i)\tau(a_{i-1}) \cdots \tau(a_1)\sigma, \tau(a_i)\tau(a_{i-1}) \cdots \tau(a_1)\sigma\rangle$$

$$= \langle \tau(a_i), \tau(a_{i-1}) \cdots \tau(a_1)\sigma\rangle.$$

To show that ϑ_S is an isomorphism we construct its inverse. Define $\varrho : G(S) \to \hat{D}(X(S), Y(S), e(S))$ by

$$\varrho(\sigma) = x_0,$$

$$\varrho(\tau(a)) = \begin{cases} y(a) & \text{if } a \in S \cap H, \\ x_i x_{i-1} & \text{if } a = a_i \in S \cap R \text{ and } 1 \le i \le k. \end{cases}$$

One easily checks that this is a good definition, since (1) and (2) are defining relations for $G(S)$.

A direct computation shows that the restrictions of $\varrho \circ \vartheta_S$ and $\vartheta_S \circ \varrho$ to $X(S) \cup Y(S)$ and $\{\sigma, \tau(a) \mid a \in S\}$, respectively, are identities. Hence $\varrho \circ \vartheta = \mathrm{id}$ and $\vartheta \circ \varrho = \mathrm{id}$, whence ϑ is an isomorphism. □

References

[1] T.C. Craven, The topological space of orderings of a rational function field, Duke Math. J. 41 (1974) 339–347.

[2] T.C. Craven, The Boolean space of orderings of a field, Trans. AMS 209 (1975) 225–235.

[3] A Douady, Détermination d'un groupe de Galois, C.R. Acad. Sci. Paris 258 (1964) 5305–5308.

[4] D. Gildenhuys and C.K. Lim, Free pro-$\mathscr{C}$-groups, Math. Z. 125 (1972) 233–254.

[5] D. Gildenhuys and L. Ribes, A Kurosh subgroup theorem for free pro-$\mathscr{C}$-products of pro-$\mathscr{C}$-groups, Trans. AMS 186 (1973) 309–329.

[6] D. Haran and M. Jarden, The absolute Galois group of a pseudo real closed field, Ann. Scuola Norm. Sup. Pisa, to appear.

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

[8] A. Prestel, Lectures on formally real fields, Monografias de Matemática 22 (IMPA, Rio de Janeiro, 1975).

[9] L. Ribes, Introduction to profinite groups and Galois cohomology, Queen's papers in Pure and Applied Mathematics 24 (Queen's University, Kingston, 1970).

[10] B. Schuppar, Elementare Aussagen zur Arithmetik und Galoistheorie von Funktionenkörpern, J. Reine Angew. Math. 313 (1980) 59–71.