ILLINOIS JOURNAL OF MATHEMATICS
Volume 37, Number 3, Fall 1993

ON A GENERALIZED ARTIN-SCHREIER THEOREM FOR REAL-MAXIMAL FIELDS

IDO EFRAT[1] AND JOCHEN KOENIGSMANN

Introduction

A celebrated theorem of Artin and Schreier [AS] characterizes the real closed fields as the fields K whose absolute Galois group $G(K)$ consists of precisely two elements. A natural generalization of the class of real closed fields is the class of *real-maximal* fields, i.e., fields K which have no proper separable algebraic extension to which all the orderings of K extend. Thus, a real-maximal field with no orderings is nothing but a separably closed field, and a real-maximal field with precisely one ordering is just a real closed field. We prove:

THEOREM A. *Let $0 \leq e \leq 3$. The following conditions on a field K are equivalent*:
(a) *K is real-maximal with precisely e orderings*;
(b) *$G(K)$ is isomorphic to the free pro-2 product D_e of e copies of $\mathbf{Z}/2\mathbf{Z}$.*

For $e = 1$ this is the Artin-Schreier theorem, while for $e = 2$ it has been proved by Bredikhin, Eršov and Kal'nei using other methods [BEK]. For $e \geq 4$, however, this equivalence is no longer true: Although (b) still implies (a), one can construct real-maximal fields with e orderings whose absolute Galois group is not D_e (Example 2.7). Nevertheless, one has the following result due to Kal'nei, mentioned without proof in [E1] and generalized in Corollary 1.5 below:

THEOREM B. *Let K be a real-maximal field with precisely e orderings $P_1, \ldots, P_e$ and assume that $P_1, \ldots, P_e$ induce distinct order topologies on K. Then $G(K) \cong D_e$.*

As was shown by van den Dries [D, Ch. II] and in subsequent works by Prestel [P1] and Jarden [J1], the real-maximal fields also arise naturally in

Received August 21, 1991.
1991 Mathematics Subject Classification. Primary 12D15; Secondary 12J15.
[1]Partially supported by grants from Lion's Foundation and the G.I.F., the German-Israeli Foundation for Scientific Research and Development.

model theory of fields. Namely, the first-order theory of e-fold ordered fields has a model-companion whose models are the real-maximal fields with precisely e orderings which are pseudo real closed (PRC): this latter property means that any non-empty absolutely irreducible affine variety defined over K has a K-rational point, provided that it has a simple rational point in each real closure of K. It may be interesting to remark that by a recent result of Pop [Po], any intersection of real closures of $\mathbf{Q}$ is PRC (see also [H, Cor. 6.3]). The counter examples mentioned above of real-maximal fields K with $e \geq 4$ orderings and with $G(K) \not\cong D_e$ thus show that Pop's result does not extend to arbitrary intersections of real-closed fields (note that by [HJ1] and Th. 1.1 below, if a real-maximal field with e orderings is PRC then its absolute Galois group is D_e).

Nevertheless, one may still ask whether a weaker result holds, namely, that a field with absolute Galois group D_e is necessarily PRC—as is indeed the case for $e = 0, 1$. For larger values of e this turns out to be false:

THEOREM C. *Let K be a field such that any field E satisfying $G(E) \cong G(K)$ is necessarily PRC. Then K is either separably closed or real closed.*

In [D, p. 77] van den Dries also poses a related open question: Is a real-maximal field K with finitely many orderings which induce distinct order topologies on K (in this case one says that the orderings are independent) necessarily PRC? In this connection we have the following result (actually, in a somewhat more general situation—see Theorem 1.6):

THEOREM D. *Let K be a real-maximal field with finitely many orderings. Then the following conditions are equivalent:*

(a) *The orderings on K are independent;*
(b) *Any Henselization of K with respect to a non-trivial valuation is either separably closed or real closed.*

It should be noted that a Henselization of a PRC field with respect to a non-trivial valuation indeed must be either separably closed or real closed, by results of Frey and Prestel [GJ2, Th. B]. One is therefore led to the following equivalent version of van den Dries' problem (compare also [FJ, Problem 10.16(b)]):

Let K be a real-maximal field with finitely many orderings and assume that all the Henselizations of K with respect to non-trivial valuations are either separably closed or real closed. Is K necessarily PRC?

Acknowledgement. This work was carried out while the first author enjoyed the hospitality of the Faculty of Mathematics at Konstanz University. We are indebted to Alexander Prestel for his remarks on the results of this paper.

1. Independence of valuations in real-maximal fields

Denote the space of orderings of a field K by $X(K)$. It is equipped with the Harrison topology defined by the subbasic sets $H(a) = \{P \in X(K) | a \in P\}$, $a \in K^{\times}$. This topology is Boolean, i.e., Hausdorff, compact and totally disconnected [P2, Th. 6.5]. One says that K has the *strong approximation property* (SAP) if the collection of sets $H(a)$, $a \in K^{\times}$, is closed with respect to intersections (see [P2, Th. 9.1] and [L, §10] for many other equivalent definitions of this widely-studied property).

A profinite group G is said to be *real-projective* if its set of involutions (elements of order precisely 2) is closed in G and if the following local-global principle holds: If $\alpha: B \to A$ is an epimorphism of finite groups, if $\beta: G \to A$ is a continuous homomorphism, and if for each subgroup $H \leq G$ of order 2 there is a continuous homomorphism $\gamma_H: H \to B$ such that $\mathrm{Res}_H \beta = \alpha \circ \gamma_H$, then there exists a continuous homomorphism $\gamma: G \to B$ such that $\beta = \alpha \circ \gamma$.

As an important example we mention the real 2-free group $\hat{D}_2(X)$ on a Boolean space X considered in [J2, §4]. When X is a discrete space of e elements, it is nothing but the free pro-2 product D_e of e copies of $\mathbf{Z}/2\mathbf{Z}$. The properties of $\hat{D}_2(X)$ can be derived just as in [HJ2], working in the category of pro-2 groups instead of the category of profinite groups. In particular, X is a closed system of representatives for the conjugacy classes of the involutions in $\hat{D}_2(X)$ and $\hat{D}_2(X)$ is real-projective (see also [J2, Prop. 13]).

THEOREM 1.1. *The following conditions on a real-maximal field K are equivalent*:

(a) $G(K) \cong \hat{D}_2(X(K))$;

(b) $G(K)$ *is real-projective*;

(c) K *has the SAP*.

Proof. (a) $\Leftrightarrow$ (b). By [J2, Lemma 9[2] and Prop. 13], $G(K)$ is real-projective if and only if it is of the form $\hat{D}_2(X)$ for some Boolean space X. It follows from Artin-Schreier's theory and from the fact that X is a closed system of representatives for the conjugacy classes of the involutions in $\hat{D}_2(X)$ that $X \cong X(K)$. (Alternatively, use [H, Prop. 4.2].)

(b) $\Rightarrow$ (c). [H, Prop. 3.3 and Remark 3.2].

(c) $\Rightarrow$ (a). As K is real-maximal, it is the intersection of its real closures, hence it is pythagorean. By [J2, Lemma 9 and Lemma 11], $G(K)$ is pro-2. The assertion therefore follows from a result of Eršov [E2, Th. 3] (see also [Ef, Cor. 4.4]). □

---

[2]Note that the assumption that the field PRC is redundant in the formulation of that lemma.

Proof of Theorem A. A field with at most 3 orderings has the SAP [L, p. 97], so by Theorem 1.1, (a) $\Rightarrow$ (b). The converse implication follows from [J2, Lemma 9]. $\square$

Recall that an ordering P and a valuation v on a field K are *compatible* if $x \in P$ whenever $v(x-1) > 0$ (see [P2, Lemma 7.2] for equivalent definitions). We say that a second valuation w on K is coarser than v if for all $x \in K^\times$, $v(x) \geq 0$ implies $w(x) \geq 0$. The following (quite well-known) facts are used extensively in the sequel.

LEMMA 1.2. (a) *An ordering on a field K is compatible with some non-trivial valuation if and only if it is non-archimedian.*

(b) *Distinct orderings P_1, P_2 on a field K induce the same topology if and only if there exists a non-trivial valuation w on K which is compatible with both P_1 and P_2.*

(c) *An ordering P and a valuation v on a field K induce the same topology if and only if there exists a non-trivial valuation w on K which is compatible with P and is coarser than v.*

(d) *Two non-trivial valuations v_1, v_2 on a field K induce the same topology if and only if there exists a non-trivial valuation w on K which is coarser than both v_1 and v_2.*

(e) *The orderings on any Henselization of a field K with respect to a valuation v are mapped bijectively via restriction onto the set of orderings on K compatible with v. In particular, an ordering P is compatible with a valuation v on a field K if and only if some Henselization of K with respect to v is contained in some real closure of K with respect to P.*

(f) *A valuation w is coarser than a valuation v on a field K if and only if some Henselization of K with respect to w is contained in some Henselization of K with respect to v.*

Proof. (a) [P2, Cor. 7.10 and Th. 7.14].

(b) From (a) and from the discussion in [L, p. 45] we get the assertion when P_1 and P_2 are both archimedian or both non-archimedian. If P_1, say, is archimedian and P_2 is not, then $\mathbf{Q}$ is dense in the P_1-topology but not in the P_2-topology, so these topologies are distinct, and the claimed equivalence follows again from (a).

(c) [L, Prop. 5.8].

(d) [PZ, Lemma 3.4].

(e) [P2, Th. 8.3].

(f) [J3, Cor. 14.4] or [Ri, p. 210, Cor. 1]. $\square$

For a valuation v we denote its (precise) value group by Γ_v.

PROPOSITION 1.3. *The following conditions on a field K are equivalent*:
(a) *The orderings on K are independent*;
(b) *The Henselization K_v^h of any non-trivial valuation v on K satisfies $|X(K_v^h)| \leq 1$*;
(c) *The residue field $\bar{K}_v$ of any non-trivial valuation $v: K \to \Gamma_v \cup \{\infty\}$ satisfies $|X(\bar{K}_v)| \leq 1$, and if $\bar{K}_v$ is formally real then $\Gamma_v = 2\Gamma_v$.*

Proof. By Lemma 1.2(b)(e), (a) $\Leftrightarrow$ (b). Also, Baer-Krull's theorem [L, Th. 5.3] yields a bijective correspondence between the orderings on K compatible with v and $X(\bar{K}_v) \times \mathrm{Hom}(\Gamma_v/2\Gamma_v, \mathbf{Z}/2\mathbf{Z})$. Lemma 1.2(e) again yields a bijective correspondence between the orderings on K compatible with v and $X(K_v^h)$. Combine these two bijections to obtain that (b) $\Leftrightarrow$ (c). $\square$

COROLLARY 1.4. *If the orderings of a field are independent then it has the SAP.*

Proof. Use the fact that K has the SAP if and only if for every non-trivial valuation $v: K \to \Gamma_v \cup \{\infty\}$ either $X(\bar{K}_v) = \emptyset$ or $\Gamma_v = 2\Gamma_v$ or both $|X(\bar{K}_v)| = 1$ and $(\Gamma_v : 2\Gamma_v) = 2$ [P2, Th. 9.1].

Alternatively, let A and B be disjoint finite subsets of $X(K)$. Stone's weak approximation theorem for V-topologies [PZ, Th. 4.1] yields $a \in K^\times$ such that $A \subseteq H(a)$ and $B \cap H(a) = \emptyset$. This is again equivalent to the SAP [P2, Th. 9.1]. $\square$

As a consequence from this and from Theorem 1.1 we get the following generalization of Kal'nei's result (Theorem B), which answers affirmatively a weaker Galois-theoretic version of van den Dries' problem:

COROLLARY 1.5. *Let K be a real-maximal field whose orderings are independent. Then $G(K) \cong \hat{D}_2(X(K))$.*

THEOREM 1.6. *Let $P_1, \ldots, P_e$, $e \geq 1$, be the distinct orderings on a field K and assume that $K = \bar{K}_1 \cap \cdots \cap \bar{K}_e$, where $\bar{K}_1, \ldots, \bar{K}_e$ are the real closures of K with respect to $P_1, \ldots, P_e$. Then the following conditions are equivalent*:
(a) *$P_1, \ldots, P_e$ are independent*;
(b) *For every non-trivial valuation v on K, the Henselization K_v^h is either algebraically closed or real closed*;
(c) *For every non-trivial valuation $v: K \to \Gamma_v \cup \{\infty\}$, the residue field $\bar{K}_v$ is either separably closed or real closed and the value group Γ_v is divisible.*

Proof. (a) $\Rightarrow$ (b). Let v be a non-trivial valuation on K. If $P_1, \ldots, P_e$, v induce on K distinct topologies then by [He, Prop. 1.3], any Henselization of K with respect to v is algebracially closed. If the v-topology coincides with the P_i-topology for some $1 \leq i \leq e$ then Lemma 1.2 yields a non-trivial valuation w on K which induces on K the same topology as P_i and such that for appropriate Henselizations K_v^h and K_w^h of K with respect to v and w, $K_w^h \subseteq K_v^h, \overline{K}_i$. By [He, Th. 1.1], $K_w^h = \overline{K}_i$ so K_v^h is either real closed or algebraically closed.

(b) $\Rightarrow$ (c): Let v: $K \to \Gamma_v \cup \{\infty\}$ be a non-trivial valuation with an algebraically closed Henselization K_v^h. By general valuation theory, $\overline{K}_v$ is separably closed and Γ_v is divisible. If on the other hand K_v^h is real closed, then [P2, Th. 8.6] gives that $\overline{K}_v$ is real closed and, again, Γ_v is divisible.

(c) $\Rightarrow$ (a): This follows from Proposition 1.3. $\square$

1.7 *Remark.* Using this point of view, one can give the following alternative proof to a result of Prestel, according to which the orderings of a PRC field are independent [P1, Prop. 1.6]. Indeed, if v: $K \to \Gamma_v \cup \{\infty\}$ is a non-trivial valuation then by [GJ2, Th. B], the Henselization K_v^h is either separably closed or real closed, hence $|X(K_v^h)| \leq 1$. This implies the assertion by Proposition 1.3.

2. Absolute Galois groups of fields of generalized formal power series

For an ordered abelian group Γ and a field K let $K((\Gamma))$ be the field of all formal power series $\sum_{\gamma\in\Gamma} a_\gamma t^\gamma$, where $a_\gamma \in K$ for all $\gamma \in \Gamma$, such that $\{\gamma \in \Gamma | a_\gamma \neq 0\}$ is well-ordered with respect to the ordering induced from Γ. It is well known that $K((\Gamma))$ is Henselian with respect to the natural valuation v: $K((\Gamma)) \to \Gamma \cup \{\infty\}$ defined by

$$v\Big(\sum_{\gamma\in\Gamma} a_\gamma t^\gamma\Big) = \min\{\gamma \in \Gamma \mid a_\gamma \neq 0\}$$

[Ri, pp. 103, 112, 198]. Note that v is non-trivial whenever $\Gamma \neq 0$.

LEMMA 2.1. *Let K be a field and let Γ be an ordered abelian group. Then the restriction homomorphism $G(K((\Gamma))) \to G(K)$ is an epimorphism. If in addition* $\operatorname{char} K = 0$ *and Γ is divisible then it is an isomorphism.*

Proof. Set $E = K((\Gamma))$. To prove that $K = \tilde{K} \cap E$, assume by contradiction that

$$\alpha = \sum_{\gamma\in\Gamma} a_\gamma t^\gamma \in (\tilde{K} \cap E) - K$$

and let $f = \operatorname{irr}(\alpha, K)$. Taking formal derivative with respect to t we get $f'(\alpha)\alpha' = (f(\alpha))' = 0$. If $p = \operatorname{char} K \neq 0$ then f, being irreducible, is not a

pth power, so in any case, $f' \neq 0$ and therefore $f'(\alpha) \neq 0$. But as $\alpha \notin K$, also $\alpha' \neq 0$—contradiction.

Now assume that $\operatorname{char} K = 0$ and that Γ is divisible. Let v be the natural valuation on E and let u and $\tilde{v}$ be the unique extensions of v to $\tilde{K}E$ and to $\tilde{E}$, respectively. Note that $\tilde{v}/v$, hence also $\tilde{v}/u$, is unramified. Since the residue field $\tilde{K}$ of u is algebraically closed and of characteristic 0, the residue degree and the defect of $\tilde{v}/u$ are 1. By Henselianity, $\tilde{E} = \tilde{K}E$, so Res: $G(E) \to G(K)$ is an isomorphism. □

Proof of Theorem C. Let $E = K((\mathbf{Q}))$ and assume first that $\operatorname{char} K = 0$. By Lemma 2.1, $G(E) \cong G(K)$. By assumption, E is PRC as well as (non-trivially) Henselian. It follows from [GJ2, Th. B] that it is either separably closed or real closed. Hence $|G(K)| = |G(E)| \leq 2$. If $\operatorname{char} K \neq 0$ then K is not formally real. Since it is PRC, a theorem of Ax [FJ, Th. 10.17] implies that $G(K)$ is projective. In particular the epimorphism Res: $G(E) \to G(K)$ (Lemma 2.1) splits; i.e., there is a separable algebraic extension E_1 of E such that Res: $G(E_1) \to G(K)$ is an isomorphism. By assumption, E_1 is PRC, as well as Henselian and non-formally real. As before, this implies that $|G(K)| = |G(E_1)| = 1$. □

2.2 *Remarks.* (i) For a related construction see [GJ1, §4].

(ii) A certain p-adic analogue of Theorem C also holds: Let K be a field with the property that any field E satisfying $G(E) \cong G(K)$ is pseudo p-adically closed (PpC) in the sense of [HJ3] for instance. Then K is either separably closed or p-adically closed. Indeed, just as in the above proof, if $\operatorname{char} K = 0$ then $E = K((\mathbf{Q}))$ is PpC and $G(E) \cong G(K)$. As E is Henselian, [GJ2, Th. C] implies that E is either algebraically closed or p-adically closed. Use [HJ3, Cor. 6.6] to conclude that either $G(K) = 1$ or $G(K) \cong G(\mathbf{Q}_p)$. In the first case K is of course separably closed. In the second case, since K is PpC, [HJ3, Cor. 15.2] implies that it is p-adically closed. If on the other hand $\operatorname{char} K \neq 0$, then K admits no p-adic valuations, so the proof can be carried out as in Theorem C.

(iii) There exist real-maximal fields, even with absolute Galois group D_e, e arbitrary, all of whose orderings are dependent. For example, let K be a field with $G(K) \cong D_e$, $e \geq 1$. Thus, K is real-maximal with precisely e orderings. By Lemma 2.1, $G(K((\mathbf{Q}))) \cong G(K)$. Since real-maximality and the number of orderings are coded inside the absolute Galois group [J2, Lemma 9], $K((\mathbf{Q}))$ too is real-maximal with e orderings. However, it is Henselian with respect to the natural (non-trivial) valuation v, so by Lemma 1.2(b)(e), these orderings are all dependent.

We now turn to modify the above construction of generalized power series fields in order to construct the counterexamples to the equivalence of Theorem A for $e \geq 4$ mentioned in the introduction (Example 2.7).

PROPOSITION 2.3. *Let K be a field of characteristic* 0, *let p be a prime number, and let Γ be an ordered abelian group such that $\Gamma = q\Gamma$ for all primes $q \neq p$.*

(i) *If L is an algebraic extension of K with $G(L)$ pro-p, then $G(L \cdot K((\Gamma)))$ is pro-p;*

(ii) *If $(\Gamma\colon p\Gamma) = p$ then $G(\tilde{K} \cdot K((\Gamma))) \cong \mathbf{Z}_p$.*

Proof. Let $E = K((\Gamma))$, let v be the natural valuation on E and let $\tilde{v}$ be the unique extension of v to $\tilde{E}$.

(i) Let u be the restriction of $\tilde{v}$ to LE. Since Γ is q-divisible for every prime $q \neq p$, the ramification index $e(\tilde{v}/v)$, hence also $e(\tilde{v}/u)$, is a power of p (as a supernatural number). By assumption, the residue degree $f(\tilde{v}/u) = [\tilde{K}\colon L]$ is also a power of p. Finally, since $\operatorname{char} L = 0$, $\tilde{v}/u$ is defectless. Therefore $G(LE)$ is pro-p.

(ii) Put $F = \tilde{K}E$. By (i), $G(F)$ is a pro-p group. Each element α in F can be written as

$$\alpha = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$$

with $a_\gamma \in \tilde{K}$. Hensel's lemma in F, applied with respect to the polynomial $X^p - a_{\tilde{v}(\alpha)}^{-1} t^{-\tilde{v}(\alpha)}\alpha$, implies that

$$\alpha \equiv a_{\tilde{v}(\alpha)} t^{\tilde{v}(\alpha)} \mod (F^\times)^p.$$

Since $a_{\tilde{v}(\alpha)} \in \tilde{K}$, it is a p-power in $F^\times$. Hence $\alpha \equiv t^{\tilde{v}(\alpha)} \operatorname{mod}(F^\times)^p$. It follows that for any $\alpha, \alpha' \in F^\times$ we have $\alpha \equiv \alpha' \operatorname{mod}(F^\times)^p$ if and only if $\tilde{v}(\alpha) \equiv \tilde{v}(\alpha') \bmod p\Gamma$, i.e., $F^\times/(F^\times)^p \cong \Gamma/p\Gamma$. Since F contains all roots of unity, Kummer's theory gives

$$H^1(G(F), \mathbf{Z}/p\mathbf{Z}) \cong F^\times/(F^\times)^p.$$

Conclude from this and from [R, Ch. IV, Th. 6.8] that

$$\operatorname{rank} G(F) = \dim_{\mathbf{F}_p} F^\times/(F^\times)^p = \dim_{\mathbf{F}_p} \Gamma/p\Gamma = 1.$$

But F contains $\tilde{K}$ and is therefore not formally real. It follows that $G(F) \cong \mathbf{Z}_p$. $\square$

Now fix $\Gamma = \{n/m \in \mathbf{Q} \mid 2 \nmid m\}$. Then $(\Gamma\colon 2\Gamma) = 2$ and $\Gamma = q\Gamma$ for all odd primes q. The following result describes the absolute Galois group $G(K((\Gamma)))$ for K real-maximal by means of generators and relations.

PROPOSITION 2.4. *Assume that*

$$G(K) = \left\langle \{\sigma_i\}_{i\in I} \mid \sigma_i^2 = 1\ \forall i \in I,\ r_j(\boldsymbol{\sigma}) = 1\ \forall j \in J \right\rangle$$

(as a pro-2 group), with $I \neq \emptyset$ and with $r_j(\boldsymbol{\sigma})$, $j \in J$, relations in the σ_i's. Then:
(i) $G(K((\Gamma))) = \langle \{\sigma_i\}_{i\in I}, \tau \mid \sigma_i^2 = (\sigma_i\tau)^2 = 1\ \forall i \in I,\ r_j(\boldsymbol{\sigma}) = 1\ \forall j \in J\rangle$;
(ii) *If K is real-maximal then so is $K((\Gamma))$.*

Proof. (i) First observe that since $G(K)$ contains an involution, char $K = 0$. Let $E = K((\Gamma))$, $F = K((\mathbf{Q}))$, $E_1 = \tilde{E} \cap F$ and $E_2 = \tilde{K}E$. Then Res: $G(F) \to G(E_1)$ is surjective and Res: $\mathscr{G}(E_2/E) \to G(K)$ is injective. By Lemma 2.1 the composition of the restriction homomorphisms

$$G(F) \to G(E_1) \to \mathscr{G}(E_2/E) \to G(K)$$

is an isomorphism. It follows that all three restriction maps are in fact isomorphisms. We therefore get a split exact sequence

$$1 \to G(E_2) \to G(E) \to G(K) \to 1$$

with Res^{-1}: $G(K) \to G(E_1)$ being a section. For simplicity we identify σ_i, $i \in I$, with generators of $G(E_1)$ via this section. Also, by Proposition 2.3(ii), $G(E_2) = \langle\tau\rangle \cong \mathbf{Z}_2$. We show that $G(E_1)$ acts on $G(E_2)$ according to the rule $\sigma_i\tau\sigma_i = \tau^{-1}$, $i \in I$. Both $\sigma_i\tau\sigma_i$ and τ^{-1} are trivial on $\tilde{K}$, hence on E_2. It therefore suffices to show that they coincide on t^γ for each $\gamma \in \mathbf{Q}$. Indeed, $\sigma_i(t^\gamma) = t^\gamma$ and since $2^n\gamma \in \Gamma$ for some $n \geq 0$, $\tau(t^\gamma) = \xi t^\gamma$ for some primitive root of unity ξ. As $\sigma_i(\xi) = \xi^{-1}$, we get $(\sigma_i\tau\sigma_i)(t^\gamma) = \sigma_i(\xi t^\gamma) = \xi^{-1}t^\gamma = \tau^{-1}(t^\gamma)$, as required.

(ii) Use (i) and the fact that a field is real-maximal if and only if its absolute Galois group is pro-2 and is generated by involutions [J2, Lemma 9 and Lemma 11]. □

LEMMA 2.5. *Let $P_1, \dots, P_n, Q$ be distinct orderings on a field K and suppose that Q is archimedian. Then there exists an element a such that $a \in P_1 \cap \cdots \cap P_n$, $a \notin Q$.*

Proof. Let $\tau_1, \dots, \tau_m$ be the distinct order topologies induced by $P_1, \dots, P_n$ on K. Without loss of generality, $P_{i_l+1}, \dots, P_{i_{l+1}}$ induce τ_l, $l = 0, \dots, m$, where $0 = i_0 < \cdots < i_{m+1} = n$. For each $0 \leq l \leq m$, the set $P_{i_l+1}^\times \cap \cdots \cap P_{i_{l+1}}^\times$ is open in τ_l and is non-empty, since it contains 1. By Lemma 1.2(a)(b), the Q-topology does not coincide with any τ_l, $1 \leq l \leq m$. Use the weak approximation theorem [PZ, Th. 4.1] to obtain $a \in K$ as required. □

Denote the Frattini subgroup of a profinite group G by $\Phi(G)$ [FJ, §20.1].

LEMMA 2.6. *Let K be a field such that $G(K)$ is a pro-2 group. Then:*
(a) *$G(K)/\Phi(G(K))$ is an elementary abelian 2-group;*
(b) *$\Phi(G(K))$ contains no involutions;*
(c) *If $\varepsilon_1, \varepsilon_2$ are non-conjugate involutions in $G(K)$ then $\varepsilon_1\varepsilon_2 \notin \Phi(G(K))$;*
(d) *If $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are involutions in $G(K)$ then $\varepsilon_1\varepsilon_2\varepsilon_3 \notin \Phi(G(K))$.*

Proof. (a) This is contained in [FJ, Lemma 20.36].

(b) Use Artin-Schreier's theory and the fact that for K formally real, $\Phi(G(K)) \leq G(K(\sqrt{-1}))$.

(c) By Artin-Schreier's theory, the non-conjugate involutions $\varepsilon_1, \varepsilon_2$ induce distinct orderings P_1, P_2, respectively, on K. Take $a \in P_1 - P_2$. Then ε_1 fixes $\sqrt{a}$ but ε_2 does not. Furthermore, $\sqrt{a}$ is fixed by $\Phi(G(K))$, since the latter group is contained in $G(K(\sqrt{a}))$. Conclude that $\varepsilon_1\varepsilon_2 \notin \Phi(G(K))$.

(d) We may assume that $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are non-conjugate—otherwise use (a) and (b). So let P_1, P_2, P_3, respectively, be the distinct orderings induced by them on K. There exists $a \in K^\times$ such that $a \in P_1 \cap P_2$ and $a \notin P_3$. Then $\sqrt{a}$ is fixed by $\varepsilon_1, \varepsilon_2$ and $\Phi(G(K))$ but not by ε_3. Conclude that $\varepsilon_1\varepsilon_2\varepsilon_3 \notin \Phi(G(K))$. □

Example 2.7. We now construct examples as mentioned in the introduction. We begin with the case $e = 4$. Let K be a field with $G(K) \cong D_2$ (in particular $|X(K)| = 2$). Actually, we may take K to be an algebraic extension of $\mathbf{Q}$ [J2]. Put $E = K((\Gamma))$. By Proposition 2.4, E is real-maximal and

$$G(E) \cong \langle \sigma_1, \sigma_2, \tau \mid \sigma_1^2 = \sigma_2^2 = (\sigma_1\tau)^2 = (\sigma_2\tau)^2 = 1 \rangle.$$

By Baer-Krull's correspondence [L, Th. 5.3], $|X(E)| = |X(K)| \times |\mathrm{Hom}(\Gamma/2\Gamma, \mathbf{Z}/2\mathbf{Z})| = 4$, and the distinct orderings $P_1, \dots, P_4$ on E are determined by the sign of the formal variable t and by their restriction to K. Yet $G(E) \not\cong D_4$, since $\operatorname{rank} G(E) = 3$ and $\operatorname{rank} D_4 = 4$. Note also that the involutions $\varepsilon_1 = \sigma_1$, $\varepsilon_2 = \sigma_2$, $\varepsilon_3 = \sigma_1\tau$ and $\varepsilon_4 = \sigma_2\tau$ are non-conjugate in $G(E)$. Hence, without loss, their fixed fields induce $P_1, \dots, P_4$, respectively, on E.

In a similar way one obtains examples as required with an arbitrary even finite number e of orderings.

To construct examples in the general case, where the number of orderings is $n + 4$, $n \geq 1$, we argue as follows: Choose a transcendence base T for E/K containing t, where K and E are as above. We have $|T| \leq |E| = \aleph = \operatorname{tr.deg.} \mathbf{R}/K$ so $K(T) = K \otimes \mathbf{Q}(T)$ embeds in $\mathbf{R}$, giving rise to an archimedian ordering on $K(T)$. Permuting T we even get infinitely many such orderings. Let $\overline{K}_1, \dots, \overline{K}_n$ be real closures of $K(T)$ with respect to distinct archimedian orderings. Since $G(E), G(\bar{K}_1), \dots, G(\bar{K}_n)$ are closed pro-2 subgroups of $G(K(T))$, we may use Sylow's theorems [FJ, Prop. 20.43] to assume without loss that they generate a pro-2 subgroup of $G(K(T))$. According to [J2, Lemma 9 and Lemma 11] this means that $F = E \cap \bar{K}_1 \cap \cdots \cap \bar{K}_n$ is real-maximal. Note that since $G(E)$ is by construction not real-projective (Theorem 1.1), $G(F)$ is not real-projective either, by [HJ1, Cor. 10.5]. In light of Theorem 1.1 again, we have to show that $|X(F)| = n + 4$. As E is Henselian, $P_1, \dots, P_4$ are non-archimedian (Lemma 1.2(a)(e)). Since $K(T)$ contains t, the restrictions of $P_1, \dots, P_4$ to $K(T)$ (which we keep denoting by $P_1, \dots, P_4$) are distinct. Also let $Q_1, \dots, Q_n$ be the (distinct) archimedian orderings on F induced by $\bar{K}_1, \dots, \bar{K}_n$, respectively. We, thus, have to show that $X(F)$ contains no other orderings beside $P_1, \dots, P_4, Q_1, \dots, Q_n$.

To this end let P be an ordering on F and assume that $P \neq P_1, \dots, P_4, Q_1, \dots, Q_n$. Choose involutions $\varepsilon, \delta_1, \dots, \delta_n$ in $G(F)$ whose fixed fields in $\tilde{F}$ induce $P, Q_1, \dots, Q_n$, respectively. We have

$$\varepsilon \in G(F) = \langle \varepsilon_1, \dots, \varepsilon_4, \delta_1, \dots, \delta_n \rangle,$$

so Lemma 2.6(a) yields $1 \leq i_1 < \cdots < i_r \leq 4$ $1 \leq j_1 < \cdots < j_s \leq n$ and $\varphi \in \Phi(G(F))$ such that

$$\varepsilon = \varepsilon_{i_1} \cdots \varepsilon_{i_r} \delta_{j_1} \cdots \delta_{j_s} \varphi.$$

For each $1 \leq j \leq n$ we obtain from Lemma 2.5 an element $a_j \in F^\times$ such that $\sqrt{a_j}$ is fixed by $\varepsilon, \varepsilon_1, \dots, \varepsilon_4, \delta_1, \dots, \delta_{j-1}, \delta_{j+1}, \dots, \delta_n$ but not by δ_j. Since $\Phi(G(F)) \leq G(F(\sqrt{a_j}))$, $\sqrt{a_j}$ is also fixed by φ. Conclude that no j_l can equal j. But $1 \leq j \leq n$ was arbitrary, so $\varepsilon = \varepsilon_{i_1} \cdots \varepsilon_{i_r} \varphi$. Using the fact that $\varepsilon_1 \varepsilon_3 \varepsilon_2 \varepsilon_4 = 1$ and the commutativity of $G(F)/\Phi(G(F))$ (Lemma 2.6(a)) we may in fact assume that $r \leq 2$. However the cases $r = 0, 1, 2$ are all impossible by parts (b), (c) and (d), respectively, of Lemma 2.6. This yields the desired contradiction.

References

[AS] E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlosenen Körper*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 225–231.

[BEK] S. Bredikhin, Yu. Eršov and V.E. Kal'nei, *Fields with two linear orderings*, Mathematicheski Zametki 7 (1970), 525–536 (Russian); Mathematical Notes of the Academy of Sciences of the USSR (1970), 319–325 (English translation).

[D] L. van den Dries, *Model theory of fields*, Thesis, Utrecht, 1978.

[E1] Yu.L. Eršov, *Semilocal fields*, Dokl. Akad. Nauk. SSSR **215**(2) (1974), 41–44 (Russian); Soviet Math. Dokl. **15** (1974), 424–428 (English translation).

[E2] Yu.L. Eršov, *Galois groups of maximal 2-extensions*, Matematicheski Zametki **36** (1984), 913–923 (Russian); Mathematical Notes of the Academy of Sciences of the USSR (1985), 956–961 (English translation).

[Ef] I. Efrat, *Local-global principles for Witt rings*, J. Pure Appl. Algebra, to appear.

[FJ] M. Fried and M. Jarden, *Field arithmetic*, Ergeb. Math. Grenzgeb. III **11**, Springer, Heidelberg, 1986.

[GJ1] W.-D. Geyer and M. Jarden, *On the normalizer of finitely generated subgroups of absolute Galois groups of uncountable Hilbertian fields of characteristc* 0, Israel J. Math. **63** (1988), 323–334.

[GJ2] ______, *The Henselian closures of a PpC field*, Abh. Math. Sem. Univ. Hamburg, **61** (1991), 63–71.

[H] D. Haran, *Closed subgroups of* $G(\mathbf{Q})$ *with involutions*, J. Algebra **129** (1990), 393–411.

[He] B. Heinemann, *On finite intersections of "Henselian valued" fields*, Manuscripta Math. **52** (1985), 37–61.

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

[HJ2] ______, *Real free groups and the absolute Galois group of* $\mathbf{R}(t)$, J. Pure Appl. Algebra **37** (1985), 155–165.

[HJ3] ______, *The absolute Galois group of a pseudo p-adically closed field*, J. Reine Angew. Math. **383** (1988), 147–206.

[J1] M. Jarden, *On the model companion of the theory of e-fold ordered fields*, Acta Math. **150** (1983), 243–253.

[J2] ______, *The algebraic nature of the elementary theory of PRC fields*, Manuscripta Math. **60** (1988), 463–475.

[J3] ______, *Intersections of local algebraic extensions of a Hilbertian field*, Proceedings of the NATO Advanced Study Institute on "Generators and Relations in Groups and Geometries", to appear.

[L] T.Y. Lam, "The theory of ordered fields" in *Ring theory and algebra III* (editor, B.R. MacDonald), Lecture notes in pure and applied mathematics **55**, Marcel Dekker, New York, 1980, 1–152.

[P1] A. Prestel, "Pseudo real closed fields" in *Set theory and model theory*, Lecture Notes in Mathematics **872**, Springer, Berlin, 1981, 127–156.

[P2] A. Prestel, *Lectures on formally real fields*, Lecture Notes in Mathematics **1093**, Springer, Berlin, 1984.

[Po] F. Pop, *Fields of totally* Σ*-adic numbers*, Arithmetik der Körper, manuscript, 1990.

[PZ] A. Prestel and M. Ziegler, *Model theoretic methods in the theory of topological fields*, J. Reine Angew. Math. **299/300** (1978), 318–341.

[R] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's University, Kingston, 1970.

[Ri] P. Ribenboim, *Théorie des Valuations*, Les presses de l'Université de Montréal, Montréal 1968.

Universität Heidelberg
Heidelberg, Federal Republic of Germany

Universität Konstanz
Konstanz, Federal Republic of Germany