# SUBFIELDS OF A REAL CLOSED FIELD OF COUNTABLE CODIMENSION

J.M. GAMBOA

Abstract. Given a real closed field $R$ we provide an elementary method to construct directed systems $\{K_n : n \in \mathbb{N}\}$ of subfields of $R$ of countable codimension, that is, the dimension of $R$ as $K_n$-vector space is $\aleph_0$, such that $R = \varinjlim K_n$. Next we deduce some properties of the family of subfields of countable codimension of a real closed field.

## 1. Introduction

Artin and Schreier's solution to Hilbert's 17th problem [1] led them to introduce the key notion of *a real closed field* and to prove the existence and uniqueness of the real closure of any ordered field. These fields are unavoidable in real algebraic geometry for much the same reason as algebraically closed fields of characteristic zero are unavoidable in algebraic geometry over $\mathbb{C}$.

René Thom regrets, as late as 1972, *the piteous state of neglect of real algebraic geometry compared with the sophistication and formal perfection of complex algebraic geometry.* Some years later Jean Dieudonné [3] wrote with scepticism: In principle, in "abstract" algebraic geometry, algebraic equations with coefficients in any field whatsoever can be taken; but the experience of real geometry, where it is possible that no point of $\mathbb{R}^n$ satisfies a polynomial equation of positive degree, shows that it would not be possible to have workable geometric statements without being over algebraically closed fields.

Fortunately, Dieudonné erred his forecast and nowadays real algebraic geometry, that is, the study of the geometry and the topology of semialgebraic subsets of $R^n$, where $R$ is a real closed field, is a subject established over firm grounds. The book [2] by Jacek Bochnak, Michel Coste and Marie-Francoise Roy is the recommended reading to study the fundamentals of real algebraic geometry, even for those only interested in the knowledge of algebraic subsets of $\mathbb{R}^n$.

As Dieudonné pointed out, the main difference between algebraically closed fields and real closed fields is that polynomial equations of positive degree have solutions over the first ones and may have no solutions over the second ones. This has important topological consequences; for example irreducible real algebraic varieties may be non-connected, contrary to the situation over the complex field, see [11]. But this note is concerned with algebraic aspects of the theory of real closed fields, so we must put in evidence some differences among the algebraic behaviour of algebraically closed fields and real closed fields. Among other facts it seems worthwhile mentioning the following.

Every field isomorphism $\sigma : E \to F$ extends to an isomorphism $\overline{\sigma} : \overline{E} \to \overline{F}$ between their algebraic closures $\overline{E}$ and $\overline{F}$, but this extension is by no means unique. As opposed, every isomorphism between two ordered fields extends *in an unique way* to an isomorphism between their real closures. This is due to the rigidity that the order structure imposes on real closed fields. Along the same line recall that the field $\mathbb{R}$ of real numbers admits a unique field automorphism whereas the field $\mathbb{C}$ of complex numbers admits $2^{2^{\aleph_0}}$ automorphisms, although just the identity

*Date*: June 19, 2020.
2010 *Mathematics Subject Classification.* Primary 12F10; Secondary 12F05.
*Key words and phrases.* Real closed field, Galois theory, Krull topology.
Author supported by Spanish MTM2017-82105-P.

and complex conjugation are continuous. As far as we know the first proof of this result was given in [7].

The next difference seems deeper. Steinitz's theorem states that two uncountable algebraically closed fields are isomorphic if and only if they have the same characteristic and the same cardinality. The uncountability is a necessary condition in the statement above; for example, the algebraic closures in $\mathbb{C}$ of $\mathbb{Q}$ and $\mathbb{Q}(\mathtt{t})$ are both countable of zero characteristic but they are not isomorphic because $\mathbb{Q}(\mathtt{t})$ cannot be embedded inside an algebraic closure of $\mathbb{Q}$ since $\mathtt{t}$ is not algebraic over $\mathbb{Q}$. A proof of the above result for fields of characteristic zero appears in [9, Prop. 2.2.5]. On the other hand there is exactly one ordering in $\mathbb{R}(\mathtt{t})$ such that $\mathtt{t}$ is positive and smaller than any positive real number. Its real closure $R$ is not isomorphic to $\mathbb{R}$ although both have zero characteristic and the same cardinality. Note that this last implies that their algebraic closures are isomorphic.

We fix along this note an algebraic closure $\overline{K}$ of a given field $K$. Recall that $K$ is *real* if $-1$ is not a sum of squares in $K$. This is equivalent to say that $K$ admits an *ordering,* that is, $K$ admits a total order relation compatible with sums and products in the obvious way. The real field $K$ is said to be *real closed* if it is real and if any algebraic extension of $K$ which is real must coincide with $K$.

Given a field extension $E|F$ we call the *codimension* of $F$ (with respect to $E$) the dimension $[E : F]$ of $E$ as $F$-vector space.

Let $R$ be a maximal proper subfield of an algebraically closed field $C$ of zero characteristic. It is easily seen using Zorn's Lemma that $R$ is real closed and the codimension $[C : R] = 2$. In addition, this field $R$ is by no means unique. The situation changes dramatically for subfields of a real closed field because real closed fields do not admit proper subfields of finite codimension. The main goal of this paper is to prove, see Theorem 2.6, that given a real closed field $R$ and a proper algebraic field extension $R|K$, there exists a countable family of fields $\{K_n : n \in \mathbb{N}\}$ with $K \subset K_n \subset R$ such that every $K_n$ is a subfield of $R$ of countable codimension (which is the smallest possible codimension.) In addition, $K_n \subset K_m$ if $m$ divides $n$. Our proof just uses elementary methods.

Section 3 is mainly devoted to study the family $\mathcal{F}_R^{cc}$ of all subfields of a real closed field $R$ with countable codimension and, in particular, the subfamily $\{K_n : n \in \mathbb{N}\}$ constructed in Section 2. We prove in Remark 3.2 that no $K_n$ is real closed, but each $K_n$ is an euclidean field, that is, each positive element of $K_n$ with respect to the ordering inherited from $R$, is a square in $K_n$. We prove in Corollary 3.4 that $\mathcal{F}_R^{cc}$ does not contain maximal elements and in Proposition 3.7 we show that the intersection of all these subfields is $\mathbb{Q}$.

## 2. Statement and proof of the main result

Fix in what follows $\mathtt{i} := \sqrt{-1}$. A useful characterization of real closed fields is the following, (see e.g. [8, Ch. XI, Prop. 3]).

**Proposition 2.1.** *Let $R$ be a non algebraically closed field whose algebraic closure $\overline{R}$ satisfies the equality $\overline{R} = R(\mathtt{i})$. Then $R$ is a real closed field.*

A deeper result is the next one, due to E. Artin [1], that the reader can see also in [8, Ch, VIII, §9, Cor. 2].

**Proposition 2.2.** *Let $K$ be a field and assume that $[\overline{K} : K] > 1$ is finite. Then $\overline{K} = K(\mathtt{i})$. In particular $K$ is a real closed field and $[\overline{K} : K] = 2$.*

It follows immediately from Propositions 2.1 and 2.2 that real closed fields do not admit subfields of finite codimension as it was announced in the Introduction.

Given a field extension $E|F$ we denote $\operatorname{Aut}(E)$ the group of automorphisms of $E$ under composition, and let

$$\operatorname{Gal}(E|F) := \{\sigma \in \operatorname{Aut}(E) : \sigma(x) = x \ \ \forall\, x \in F\}$$

be its *Galois group,* that is, the group of $F$-automorphisms of $E$. Moreover, the *fixed subfield* of a subgroup $H$ of $\operatorname{Gal}(E|F)$ is the field

$$\operatorname{Fix}(H) := \{x \in E : \sigma(x) = x \ \ \forall\, \sigma \in H\}.$$

We will use the following corollary of Proposition 2.2.

**Corollary 2.3.** *Let $K$ be a field with $\operatorname{ch}(K) = 0$ and let $H \neq \{\operatorname{id}\}$ be a finite subgroup of the absolute Galois group $\operatorname{Gal}(\overline{K}|K)$ of $K$. Then $\operatorname{ord}(H) = 2$ and $\overline{K} = F(\mathtt{i})$ where $F := \operatorname{Fix}(H)$.*

*Proof.* Notice that $K \subset F \subsetneq \overline{K}$, so $K \subset F \subsetneq \overline{F} = \overline{K}$; in particular $1 < [\overline{F} : F]$. In addition, since $\operatorname{ch}(K) = 0$ and $H$ is finite,

$$[\overline{F} : F] = [\overline{K} : \operatorname{Fix}(H)] = \operatorname{ord}(H) < +\infty.$$

This implies, by Proposition 2.2, that $\overline{F} = F(\mathtt{i})$ and $\mathtt{i} \notin F$. Thus, the only nontrivial $F$-automorphism of $\overline{F}$ is *conjugation:*

$$\kappa : \overline{F} \to \overline{F},\ x + \mathtt{i}y \mapsto x - \mathtt{i}y$$

and $H \subset \operatorname{Gal}(\overline{K}|F) = \operatorname{Gal}(\overline{F}|F) = \{\operatorname{id}, \kappa\}$, which implies that $\operatorname{ord}(H) = 2$. □

Next we prove a lemma about the Krull topology in the Galois group $G := \operatorname{Gal}(\overline{K}|K)$. Recall, see e.g. [10, §17], that the closure in this topology of a subgroup $H$ of $G$ is the subgroup $\operatorname{Cl}_G(H) = \operatorname{Gal}(\overline{K}|\operatorname{Fix}(H))$, where $\operatorname{Fix}(H)$ is the fixed field of $H$.

Let $\mathtt{x}_1, \dots, \mathtt{x}_n$ be indeterminates and let $\mathtt{s}_1, \dots, \mathtt{s}_n \in \mathbb{Z}[\mathtt{x}_1, \dots, \mathtt{x}_n]$ denote the elementary symmetric forms

$$\mathtt{s}_1 := \mathtt{x}_1 + \cdots + \mathtt{x}_n, \quad \mathtt{s}_k := \sum_{1 \le i_1 < \cdots < i_k \le n} \mathtt{x}_{i_1} \cdots \mathtt{x}_{i_k} \quad \& \quad \mathtt{s}_n := \mathtt{x}_1 \cdots \mathtt{x}_n,$$

where $2 \le k \le n-1$.

**Lemma 2.4.** *Let $S$ and $T$ be two subgroups of $G := \operatorname{Gal}(\overline{K}|K)$ such that $S \subset T$ and the index $[T : S]$ is finite. Denote $H := \operatorname{Gal}(\overline{K}|\operatorname{Fix}(S))$ and $H' := \operatorname{Gal}(\overline{K}|\operatorname{Fix}(T))$, respectively, the closures of $S$ and $T$ in $G$ with respect to the Krull topology. Then,*

(1) *$H$ is an open and closed subgroup of finite index of $H'$. In addition, $[H' : H] \le [T : S]$.*

(2) *Suppose that $T$ is cyclic. Then $H$ is a normal subgroup of $H'$.*

*Proof.* (1) Since the index $[T : S] := n$ is finite, $T = \bigcup_{i=1}^n g_i S$ for some $g_1, \dots, g_n \in T$. Each $\widehat{g_i} : G \to G,\ g \mapsto g_i g$ is a continuous map, because $G$ is a topological group. Hence $\widehat{g_i}$ is a homeomorphism, since its inverse is multiplication by $g_i^{-1}$. Therefore,

$$H' = \operatorname{Cl}_G(T) = \operatorname{Cl}_G\Big(\bigcup_{i=1}^n g_i S\Big) = \operatorname{Cl}_G\Big(\bigcup_{i=1}^n \widehat{g_i}(S)\Big) = \bigcup_{i=1}^n \operatorname{Cl}_G(\widehat{g_i}(S))$$

$$= \bigcup_{i=1}^n \widehat{g_i}(\operatorname{Cl}_G(S)) = \bigcup_{i=1}^n \widehat{g_i}(H) = \bigcup_{i=1}^n g_i H,$$

and this shows that $[H' : H] \le n = [T : S]$. On the other hand, $H$ is closed in $G$, so it is closed in $H'$. To see that it is open in $H'$, pick a set $\{\sigma_1, \dots, \sigma_m\}$ of representatives of the right cosets of $H'$ with respect to $H$, where $\sigma_1 := \operatorname{id}$. Then

$$H' = \sigma_1 H \sqcup \cdots \sqcup \sigma_m H,$$

and each coset $\sigma_j H$ is a closed subset of $H'$ because it is the image of $H$ under the homeomorphism $\widehat{\sigma_j} : G \to G$, $g \mapsto \sigma_j g$. Thus,

$$H = H' \setminus \bigsqcup_{j=2}^{m} \sigma_j H$$

is also open in $H'$.
(2) Since $[T : S] = n$ we can suppose that $S := \langle \gamma^n \rangle$ where $\gamma \in G$ is a generator of $T$. We must prove that given $f \in H'$ and $g \in H$ then $f^{-1} \circ g \circ f \in H$. Notice that

$$\mathtt{s}_k(x, \gamma(x), \dots, \gamma^{n-1}(x)) \in \operatorname{Fix}(\gamma)$$

for each $x \in \operatorname{Fix}(\gamma^n)$ and each $k = 1, \dots, n$, because

$$\{x, \gamma(x), \dots, \gamma^{n-1}(x)\} = \{\gamma(x), \dots, \gamma^{n-1}(x), \gamma^n(x)\}.$$

Since $f|_{\operatorname{Fix}(\gamma)}$ is the identity it follows that

$$\mathtt{s}_k(f(x), f(\gamma(x)), \dots, f(\gamma^{n-1}(x))) = f(\mathtt{s}_k(x, \gamma(x), \dots, \gamma^{n-1}(x))) = \mathtt{s}_k(x, \gamma(x), \dots, \gamma^{n-1}(x)).$$

Therefore,

$$\begin{aligned}\prod_{j=0}^{n-1}(\mathtt{t} - \gamma^j(x)) &= \mathtt{t}^n + \sum_{k=1}^{n}(-1)^k \mathtt{s}_k(x, \gamma(x), \dots, \gamma^{n-1}(x))\mathtt{t}^{n-k} \\ &= \mathtt{t}^n + \sum_{k=1}^{n}(-1)^k \mathtt{s}_k(f(x), f(\gamma(x)), \dots, f(\gamma^{n-1}(x)))\mathtt{t}^{n-k} = \prod_{j=0}^{n-1}(\mathtt{t} - f(\gamma^j(x))).\end{aligned}$$

Thus there exists an index $i = 0, \dots, n-1$ such that $f(x) = \gamma^i(x)$, so $f^{-1}(\gamma^i(x)) = x$. Notice also that $\gamma^i(x) \in \operatorname{Fix}(S)$, because $\gamma^n(\gamma^i(x)) = \gamma^i(\gamma^n(x)) = \gamma^i(x)$. Hence, $g(\gamma^i(x)) = \gamma^i(x)$ and

$$(f^{-1} \circ g \circ f)(x) = (f^{-1} \circ g)(f(x)) = (f^{-1} \circ g)(\gamma^i(x)) = f^{-1}(g(\gamma^i(x))) = f^{-1}(\gamma^i(x)) = x,$$

which shows that $f^{-1} \circ g \circ f \in H$. □

**Lemma 2.5.** *Let $\gamma \in G := \operatorname{Gal}(\overline{K}|K)$ and for each positive integer $n$ consider the subgroup $G_n := \langle \gamma^n \rangle$ of $G$ generated by $\gamma^n$. Let $H_n := \operatorname{Gal}(\overline{K}|\operatorname{Fix}(G_n))$ be the closure of $G_n$ in $G$ with respect to the Krull topology. Then $\bigcap_{n \in \mathbb{N}} H_n = \{\mathrm{id}\}$.*

*Proof.* Since $H_1$ is a Hausdorff space, it is enough to check that $\mathcal{H} := \{H_n : n \in \mathbb{N}\}$ is a basis of open neighbourhoods of the identity in $H_1$. But it follows from [10, §17] that the family

$$\mathcal{B} := \{U : U \text{ is a normal closed subgroup of finite index of } H_1\}$$

is a basis of open neighbourhoods of the identity in $H_1$ and, by the previous lemma, $\mathcal{H} \subset \mathcal{B}$. Hence it suffices to see that each $U \in \mathcal{B}$ contains some member of $\mathcal{H}$. Let $g_1, \dots, g_k \in H_1$ such that $H_1 = \bigsqcup_{\ell=1}^{k} g_\ell U$. Since $\gamma$ has infinite order and

$$\langle \gamma \rangle = G_1 \subset H_1 = \bigsqcup_{\ell=1}^{k} g_\ell U,$$

there exist an index $\ell$ with $1 \le \ell \le k$ and two positive integers $0 < r < s$ such that $\gamma^r, \gamma^s \in g_\ell U$, so $\gamma^{s-r} \in U$. Hence

$$\mathrm{id} \in H_{s-r} = \operatorname{Cl}_{H_1}(\langle \gamma^{s-r} \rangle) \subset \operatorname{Cl}_{H_1}(U) = U,$$

as desired. □

We are ready to state and prove the main result of this note.

**Theorem 2.6.** *Let $R$ be a real closed field and let $R|K$ be a proper algebraic field extension. Then,*
(1) *There exists a countable family of subfields $\{K_n : n \in \mathbb{N}\}$ of $R$ containing $K$ such that every $K_n$ is a subfield of $R$ of countable codimension, that is, $[R : K_n] = \aleph_0$.*
(2) *In addition, $K_n \subset K_m$ if $m$ divides $n$. Consequently, $\{K_n : n \in \mathbb{N}\}$ is a directed system of subfields of $R$ with respect to inclusion, and $R = \bigcup_{n\in\mathbb{N}} K_n = \varinjlim K_n$.*

*Proof.* Let $\alpha \in R \setminus K$ and let $f$ be the minimal polynomial of $\alpha$ over $K$, whose roots in the algebraic closure $\overline{R} = R(\mathtt{i})$ of $R$ are simple because $\mathrm{ch}(K) = 0$. In particular there exists a root $\beta \in \overline{R}$ of $f$ with $\alpha \neq \beta$, and let $\varphi : K(\alpha) \to K(\beta)$ be the unique $K$-isomorphism that maps $\alpha$ onto $\beta$. Since $\overline{R}$ is an algebraic closure of $K(\alpha)$ and $K(\beta)$ there exists an automorphism $\sigma : \overline{R} \to \overline{R}$ such that $\sigma|_{K(\alpha)} = \varphi$. In particular $\sigma$ is a $K$-automorphism and $\sigma(\alpha) = \beta$. Consider the involution

$$\kappa : R(\mathtt{i}) \to R(\mathtt{i}),\ x + \mathtt{i}y \mapsto x - \mathtt{i}y,$$

which is different to $\sigma$ since $\kappa(\alpha) = \alpha$ and $\sigma(\alpha) = \beta$. Note that $\overline{K} = \overline{R}$, so $\sigma, \kappa \in \mathrm{Gal}(\overline{K}|K)$. We claim the existence of an element of infinite order $\gamma \in \mathrm{Gal}(\overline{K}|K)$ such that either $\kappa \circ \gamma = \gamma \circ \kappa$ or $\kappa \circ \gamma = \gamma^{-1} \circ \kappa$.

Indeed, suppose first that $\kappa \circ \sigma = \sigma \circ \kappa$. If $o(\sigma)$ is finite then, by Corollary 2.3, $\sigma^2 = \mathrm{id}$, and $H := \{\mathrm{id}, \kappa, \sigma, \kappa \circ \sigma\}$ is a finite subgroup of $\mathrm{Gal}(\overline{K}|K)$ with 4 elements. This contradicts Corollary 2.3. Hence $\gamma := \sigma$ has infinite order in this case and $\kappa \circ \gamma = \gamma \circ \kappa$.
Suppose now that $\kappa \circ \sigma \neq \sigma \circ \kappa$, and define $\gamma := \kappa \circ \sigma^{-1} \circ \kappa \circ \sigma \in \mathrm{Gal}(\overline{K}|K) \setminus \{\mathrm{id}\}$. Then,

$$\gamma^{-1} \circ \kappa = \sigma^{-1} \circ \kappa \circ \sigma \circ \kappa^2 = \sigma^{-1} \circ \kappa \circ \sigma = \kappa \circ \gamma.$$

If $o(\gamma)$ is finite then $\gamma^2 = \mathrm{id}$, by Corollary 2.3, and the last equality says that $\gamma \circ \kappa = \kappa \circ \gamma$, which implies that $H' := \{\mathrm{id}, \kappa, \gamma, \kappa \circ \gamma\}$ is a finite subgroup of $\mathrm{Gal}(\overline{K}|K)$ with 4 elements. Again, this contradicts Corollary 2.3, so $\gamma$ has infinite order and $\kappa \circ \gamma = \gamma^{-1} \circ \kappa$.

For later purposes let us see that $\kappa \circ \gamma^r = \gamma^{\varepsilon r} \circ \kappa$ for every $r \in \mathbb{Z}$, where $\varepsilon = 1$ if $\kappa \circ \gamma = \gamma \circ \kappa$ and $\varepsilon = -1$ if $\kappa \circ \gamma = \gamma^{-1} \circ \kappa$. This is evident for $r = 0$ and we have proved it for $r = 1$. Let $r > 1$ and suppose that $\kappa \circ \gamma^{r-1} = \gamma^{\varepsilon(r-1)}\kappa$. Then,

$$\kappa \circ \gamma^r = \kappa \circ \gamma^{r-1} \circ \gamma = \gamma^{\varepsilon(r-1)}\kappa \circ \gamma = \gamma^{\varepsilon(r-1)} \circ \gamma^{\varepsilon} \circ \kappa = \gamma^{\varepsilon r}\kappa.$$

This proves the statement for positive exponents $r$, and if $r < 0$ we denote $s = -r > 0$ and

$$\gamma^{-\varepsilon r} \circ \kappa \circ \gamma^r = \gamma^{\varepsilon s} \circ \kappa \circ \gamma^{-s} = (\kappa \circ \gamma^s) \circ \gamma^{-s} = \kappa,$$

that is, $\kappa \circ \gamma^r = \gamma^{\varepsilon r} \circ \kappa$.

For each positive integer $n$ consider the cyclic infinite subgroup $G_n := \langle \gamma^n \rangle$ of $G := \mathrm{Gal}(\overline{K}|K)$ generated by $\gamma^n$ and let $H_n := \mathrm{Cl}_G(G_n) = \mathrm{Gal}(\overline{K}|\,\mathrm{Fix}(G_n))$ be the closure of $G_n$ in $G$ with respect to the Krull topology. Let us see that each union $S_n := H_n \cup \kappa H_n$ is a closed subgroup of $G$. Since the map $\widehat{\kappa} : G \to G,\ g \mapsto \kappa g$ is a homeomorphism, we have

$$S_n = \mathrm{Cl}_G(G_n) \cup \widehat{\kappa}(\mathrm{Cl}_G(G_n)) = \mathrm{Cl}_G(G_n \cup \widehat{\kappa}(G_n)) = \mathrm{Cl}_G(G_n \cup \kappa G_n),$$

so it suffices to see that $G'_n := G_n \cup \kappa G_n$ is a subgroup of $G$. But given integers $m$ and $\ell$,

$$(\kappa \circ \gamma^{nm})^{-1} = \gamma^{-nm} \circ \kappa = \kappa \circ \gamma^{-\varepsilon nm} \in \kappa G_n, \quad \gamma^{nm} \circ (\kappa \circ \gamma^{n\ell}) = \kappa \circ \gamma^{n(\ell+\varepsilon m)} \in \kappa G_n \quad \&$$
$$(\kappa \circ \gamma^{nm}) \circ (\kappa \circ \gamma^{n\ell}) = \gamma^{n(\ell+\varepsilon m)} \in G_n.$$

We check now that each $G'_n$ is a subgroup of finite index of $G'_1$. As $G_n \subset G'_n \subset G'_1$, it is enough to prove that $G_n$ is a subgroup of finite index of $G'_1$. But $G_1 = \bigcup_{r=0}^{n-1} \gamma^r G_n$, thus

$$\kappa G_1 = \bigcup_{r=0}^{n-1} (\kappa \circ \gamma^r) G_n,$$

which implies that

$$G'_1 = G_1 \cup \kappa G_1 = \bigcup_{r=0}^{n-1} \gamma^r G_n \cup \bigcup_{r=0}^{n-1} (\kappa \circ \gamma^r) G_n$$

and, consequently, $[G'_1 : G_n] \leq 2n$.

By the Fundamental Theorem of Galois Theory, [6, §IV], the subfield $K_n := \mathrm{Fix}(S_n)$ of $\overline{K}$ contains $K$ and $\mathrm{Gal}(\overline{K}|K_n) = S_n$. Note that each $K_n \subset R = \mathrm{Fix}(\kappa)$ since $\kappa \in S_n$, and $K_1 \subset K_n$ because $S_n \subset S_1$. Indeed $K_n|K_1$ is a finite extension because, by Lemma 2.4 and the inequality just proved,

$$[K_n : K_1] = [\mathrm{Fix}(S_n) : \mathrm{Fix}(S_1)] = [S_1 : S_n] \leq [G'_1 : G'_n] \leq 2n.$$

Notice also that $K_m \subset K_\ell$ if $\ell|m$, so the union $K_\infty := \bigcup_{n\in\mathbb{N}} K_n$ is a subfield of $R$ that contains $K$. Let us show that $K_\infty = R$. Observe that for every $n \in \mathbb{N}$,

$$\mathrm{id}, \kappa \in \mathrm{Gal}(\overline{K}|K_\infty) \subset \mathrm{Gal}(\overline{K}|K_n) = S_n,$$

and in fact $\bigcap_{n\in\mathbb{N}} S_n = \{\mathrm{id}, \kappa\}$. Given $\sigma \in (G \setminus \{\mathrm{id}, \kappa\})$ both $\sigma \neq \mathrm{id}$ and $\kappa\sigma \neq \mathrm{id}$ and, by Lemma 2.5, $\bigcap_{n\in\mathbb{N}} H_n = \{\mathrm{id}\}$. Thus, there exist $n, m \in \mathbb{N}$ such that $\sigma \notin H_n$ and $\kappa\sigma \notin H_m$. Hence $\sigma, \kappa\sigma \notin H_{mn}$, that is, $\sigma \notin (H_{mn} \cup \kappa H_{mn}) = S_{mn}$. Consequently,

$$\mathrm{Gal}(\overline{K}|K_\infty) = \{\mathrm{id}, \kappa\} = \mathrm{Gal}(\overline{K}|R),$$

and $R = K_\infty$.

Next, let us prove that $K_1$ is a subfield of $R$ containing $K$ and $[R : K_1] = \aleph_0$. First, each $K_n$ is a finite dimensional $K_1$-vector space, so there exists a finite subset $\Sigma_n$ of $K_n$ generating it as $K_1$-vector space. Thus, $\Sigma := \bigcup_{n\in\mathbb{N}} \Sigma_n$ is a countable subset of $R = K_\infty$ generating it as $K_1$-vector space, which shows that $[R : K_1] \leq \aleph_0$. Thus, we must just prove that the extension $R|K_1$ is not finite. Otherwise, by the transitivity of degree,

$$[\overline{K_1} : K_1] = [\overline{K} : K_1] = [\overline{R} : K_1] = [\overline{R} : R] \cdot [R : K_1] = 2 \cdot [R : K_1]$$

is finite too and, by Proposition 2.2, $[R : K_1] = 1$, that is, $K_\infty = K_1$. Hence,

$$\gamma \in G_1 \subset H_1 \subset S_1 = \mathrm{Gal}(\overline{K}|K_1) = \mathrm{Gal}(\overline{K}|K_\infty) = \{\mathrm{id}, \kappa\},$$

a contradiction.

To finish, note that each index $[K_n : K_1]$ is finite, so $[R : K_n] = \aleph_0$ for every $n \geq 1$. □

## 3. Some consequences

Along this section we will use the notations employed in the previous ones; in particular those introduced in the proof of Theorem 2.6.

**Corollary 3.1.** *Each real closed field $R$ contains a countable family of subfields of countable codimension. In addition, this family is a directed system with respect to inclusion and $R$ is its direct limit.*

*Proof.* Let $R$ be a real closed field and let $f \in \mathbb{Q}[\mathtt{t}]$ be an irreducible polynomial of odd degree. Hence there exists a root $\alpha \in R$ of $f$ and, by Zorn's Lemma, there exists a subfield $K$ of $R$ which is maximal among those subfields of $R$ not containing $\alpha$. Since $R|K$ is a proper extension because $\alpha \in R \setminus K$, the result follows from Theorem 2.6 once we see that the extension $R|K$ is algebraic. Otherwise there exists a an element $\zeta \in R$ transcendental over $K$ and, since $K \subsetneq K(\zeta) \subset R$, the maximality of $K$ implies that $\alpha \in K(\zeta)$. Notice also that $\zeta$ is transcendental over $K(\alpha)$.

Therefore, there exist coprime polynomials $g, h \in K[\mathtt{t}]$ such that $\alpha := g(\zeta)/h(\zeta)$ or, equivalently, $\zeta$ is a root of the polynomial $p(\mathtt{t}) := g(\mathtt{t}) - \alpha h(\mathtt{t}) \in K(\alpha)[\mathtt{t}]$. Thus $p$ is the zero polynomial and, in particular, $0 = p(0) = g(0) - \alpha h(0)$. Since $\alpha \notin K$ this implies that $g(0) = h(0) = 0$, and this is a contradiction because $g$ and $h$ are coprime. □

Recall that an *euclidean field* is an ordered field $F$ such that for every positive element $x \in F$ there exists $y \in F$ such that $x = y^2$. Real closed fields are euclidean fields, but the converse is not true as it follows from our next remark.

**Remarks 3.2.** (1) We have proved in Theorem 2.6 that $R := \bigcup_{n\in\mathbb{N}} K_n$ and $K_n|K_1$ is, for every positive integer $n$ a finite extension. As $[R : K_1]$ is not finite, the proper extension $R|K_n$ is algebraic. In particular no $K_n$ is a real closed field because real closed fields do not admit proper formally real algebraic extensions.

(2) For every $n \in \mathbb{N}$ the field $K_n$ endowed with the ordering inherited from the ordering in $R$ is euclidean. In fact, let $x \in K_n$ be positive. Then there exists $y \in R$ such that $x = y^2$, and all reduces to check that $y$ belongs to $K_n = \mathrm{Fix}(S_n)$. Let $f \in S_n = H_n \cup \kappa H_n$. We must prove that $f(y) = y$.

Suppose first that $f \in H_n = \mathrm{Gal}(\overline{K}|\,\mathrm{Fix}(\langle\gamma^n\rangle))$, i.e., $\mathrm{Fix}(\langle\gamma^n\rangle) \subset \mathrm{Fix}(f)$. Since $x \in K_n$ we have $\gamma^n(x) = x$, that is, $\gamma^n(y^2) = y^2$. Thus $y^2 \in \mathrm{Fix}(\langle\gamma^n\rangle) \subset \mathrm{Fix}(f)$, so $y^2 = f(y^2) = f(y)^2$. After changing $y$ by $-y$ if necessary we may assume that $y > 0$ and, since $R$ is real closed, there exists $z \in R$ such that $y = z^2$.

Write $f(z) = a + b\mathtt{i}$ with $a, b \in R$. Then $y = f(z)^2 = (a + b\mathtt{i})^2 = (a^2 - b^2) + 2ab\mathtt{i}$ and $y = a^2 - b^2$ with $ab = 0$. If $a = 0$, then $y = -b^2$, which is false because $y > 0$ and $-b^2 \leq 0$. Thus $b = 0$ and $f(z) = a \in R$.

Consequently $f(y) = f(z)^2 = a^2 > 0$. Hence $y$ and $f(y)$ are positive elements of $R$ and we have proved that $y^2 = f(y)^2$. Thus, $y = f(y)$, as claimed.

Suppose now that $f \in \kappa H_n$. Then $\kappa f \in H_n$ and we have just seen that $y = (\kappa f)(y)$. But $y = \kappa(y)$ because $y \in R$, so

$$y = \kappa(y) = \kappa((\kappa f)(y)) = (\kappa^2 f)(y) = f(y),$$

as wanted.

Let $R$ be a real closed field. Possibly there exist many subfields $E \subset R$ such that $[R : E] = \aleph_0$ which are distinct to the ones found in Theorem 2.6. We are going to prove that it does not exist a maximal one among them. For the sake of the reader let us recall some notions and results introduced in [4] and [5].

**Definition 3.3.** Let $K(\mathtt{t})$ be the field of rational functions over a field $K$. It is said that $K$ enjoys the *extension property* if every automorphism $\varphi : K(\mathtt{t}) \to K(\mathtt{t})$ satisfies the equality $\varphi(K) = K$.

It was proved in Proposition 3.7 in [4] or, in a different way, in Proposition 3.1 in [5], that real closed fields enjoy the extension property. On the other hand, let $E$ be a field and let $u$ be transcendental over $E$. Then, the field $K := E(u)$ does not enjoy the extension property because the automorphism $\psi : K(\mathtt{t}) \to K(\mathtt{t})$ defined by $\psi|_E = \mathrm{id}$, $\psi(u) = \mathtt{t}$ and $\psi(\mathtt{t}) = u$ satisfies $\psi(K) \neq K$.

**Corollary 3.4.** Let $R$ be a real closed field. It does not exist a maximal subfield of $R$ of countable codimension.

*Proof.* Assume, by the way of contradiction, that there exists a maximal subfield $E$ among those subfields of $R$ with countable codimension. Pick $u \in R \setminus E$. As $E \subsetneq E(u) \subset R$ the maximality of $E$ implies that $[R : E(u)]$ is finite. As real closed fields admit no proper subfields of finite codimension, we get $R = E(u)$. In addition, since $[R : E]$ is not finite it follows that $u$ is transcendental over $E$, and this is impossible because $R$ has the extension property whereas $E(u)$ does not enjoy it. □

Next we shall try to understand the intersection of all subfields of a real closed field with countably codimension. First we need to introduce some terminology and to prove a technical lemma.

**Definition 3.5.** Let $R$ be a real closed field and let $R|K$ be a proper field extension. We say that an element $\alpha \in R \setminus K$ is not *totally real* with respect to $K$, if either it is transcendental over $K$ or its minimal polynomial over $K$ has a root in $R(\mathtt{i}) \setminus R$.

**Lemma 3.6.** *Let $R$ be a real closed field and let $\alpha \in R \setminus \mathbb{Q}$ be such that it is not totally real with respect to $\mathbb{Q}$. Then, there exists a subfield $K$ of $R$ which is maximal among those subfields $F$ of $R$ such that $\alpha$ is not totally real with respect to $F$. In addition, $R|K$ is an algebraic extension.*

*Proof.* The family $\Sigma$ consisting of those subfields $F$ of $R$ such that $\alpha$ is not totally real with respect to $F$ is nonempty because it contains $\mathbb{Q}$. Let $\{K_i : i \in I\} \subset \Sigma$ be a chain. Then, its union $K := \bigcup_{i\in I} K_i$ belongs to $\Sigma$ because, if $\alpha$ is algebraic over $K$, then there exists an index $i \in I$ such that the minimal polynomial of $\alpha$ over $K$ coincides with the minimal polynomial of $\alpha$ over $K_i$. Thus, Zorn's lemma guarantees the existence of a maximal element $K$ of $\Sigma$. To finish let us prove that $R|K$ is an algebraic extension. Otherwise there would exist an element $\zeta \in R$ transcendental over $K$. Since $K \subsetneq K(\zeta) \subset R$, the maximality of $K$ implies that $K(\zeta) \notin \Sigma$, hence $\alpha$ is algebraic over $K(\zeta)$ and its minimal polynomial over $K(\zeta)$ splits completely in $R[\mathtt{t}]$. This is false because, as $\zeta$ is transcendental over $K$, the minimal polynomials of $\alpha$ over $K$ and over $K(\zeta)$ coincide. □

**Proposition 3.7.** *Let $R$ be a real closed field, and let $\mathcal{F}$ be the non-empty family consisting of those subfields of $R$ with countable codimension. Then $\bigcap_{E\in\mathcal{F}} E = \mathbb{Q}$.*

*Proof.* We must prove that for every $\alpha \in R \setminus \mathbb{Q}$ there exists $E \in \mathcal{F}$ such that $\alpha \notin E$. By Lemma 3.6 there exists a subfield $K$ of $R$ which is maximal among those subfields $F$ of $R$ such that $\alpha$ is not totally real with respect to $F$ and, in addition, $R|K$ is an algebraic extension. Let $f \in K[\mathtt{t}]$ be the minimal polynomial of $\alpha$ over $K$ and pick a root $\beta \in R(\mathtt{i}) \setminus R$ of $f$.

In the proof of Theorem 2.6 we proved the existence of an automorphism $\sigma : R(\mathtt{i}) \to R(\mathtt{i})$ satisfying $\sigma(\alpha) = \beta$. We denoted

$$\kappa : R(\mathtt{i}) \to R(\mathtt{i}),\ x + \mathtt{i}y \mapsto x - \mathtt{i}y,$$

and distinguished two cases. Firstly, if $\kappa \circ \sigma = \sigma \circ \kappa$ then $\gamma := \sigma$ satisfies $\gamma(\alpha) = \beta \neq \alpha$.

Suppose now that $\kappa\circ\sigma \neq \sigma\circ\kappa$. Then the automorphism $\gamma := \kappa\circ\sigma^{-1}\circ\kappa\circ\sigma$ satisfies $\gamma(\alpha) \neq \alpha$. Otherwise $(\sigma^{-1}\circ\kappa\circ\sigma)(\alpha) = \kappa(\alpha) = \alpha$, i.e., $\kappa(\beta) = \kappa(\sigma(\alpha)) = \sigma(\alpha) = \beta$, and this is false because $\beta \in R(\mathtt{i}) \setminus R$. Thus $\gamma(\alpha) \neq \alpha$ in both cases and, with the notations in Theorem 2.6,

$$E := K_1 := \mathrm{Fix}(S_1) \in \mathcal{F} \quad \text{and} \quad \gamma \in G_1 \subset H_1 \subset S_1,$$

so $\alpha \notin E$. □

## References


[1] E. Artin, O. Schhreier: Algebraische Konstruction reeller Körper der reellen algebraische Zahlen. *Hamb. Abh.* **5**, 85-99, (1926).

[2] J. Bochnak, M. Coste, M.F. Roy: Real algebraic geometry. Translated from the 1987 French original. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **36**. Springer-Verlag, Berlin, (1998).

[3] J. Dieudonné: *History of Algebraic Geometry. An Outline of the History and Development of Algebraic Geometry.* Wadsworth Advanced Books, Monterey, CA.

[4] J.M. Gamboa: Some new results on ordered fields. *Journal of Algebra* bf 110, 1-12, (1987).

[5] J.M. Gamboa, T. Recio: Ordered fields with the dense orbits property. *Journal of Pure and applied Algebra* bf 30, 237-246, (1983).

[6] N. Jacobson: *Lectures in Abstract Algebra.* III. *Theory of fields and Galois Theory.* Springer Verlag. **4**. (1971).

[7] H. Kestelman: Automorphisms of the field of complex numbers. *Proc. London Math. Soc.* (2), **53**, 1-12, (1951).

[8] S. Lang: *Algebra.* Addison-Wesley. Third printing. (1971).
[9] D. Marker: *Model theory. An introduction.* Graduate Texts in Mathematics, **217** Springer-Verlag, New York. (2002).
[10] P. J. Morandi: *Field and Galois Theory.* Graduate Texts in Mathematics, **167**, Springer-Verlag, New York. (1996)
[11] I. Shafarevich: *Basic Algebraic Geometry.* Springer-Verlag, Berlin. (1977)

Departamento de Álgebra, Geometría y Topología, Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, 28040 MADRID (SPAIN)

*Email address*: jmgamboa@ucm.es