MATEMATIČKI VESNIK
МАТЕМАТИЧКИ ВЕСНИК
74, 4 (2022), 249–259
December 2022

research paper
оригинални научни рад
DOI: 10.57016/MV-ywug8949

CANTOR SETS AND FIELDS OF REALS

Gerald Kuba

Abstract. Our main result is a construction of four families $\mathcal{C}_1, \mathcal{C}_2, \mathcal{B}_1, \mathcal{B}_2$ which are equipollent with the power set of $\mathbb{R}$ and satisfy the following properties. (i) The members of the families are proper subfields K of $\mathbb{R}$ where $\mathbb{R}$ is algebraic over K. (ii) Each field in $\mathcal{C}_1 \cup \mathcal{C}_2$ contains a *Cantor set.* (iii) Each field in $\mathcal{B}_1 \cup \mathcal{B}_2$ is a *Bernstein set.* (iv) All fields in $\mathcal{C}_1 \cup \mathcal{B}_1$ are isomorphic. (v) If K, L are fields in $\mathcal{C}_2 \cup \mathcal{B}_2$ then K is isomorphic to some subfield of L only in the trivial case $K = L$.

1. Introduction

The cardinal number (the *size*) of a set S is denoted by $|S|$. So $|\mathbb{R}| = |\mathbb{D}| = \boldsymbol{c} = 2^{\aleph_0}$ where $\mathbb{D} = \{\sum_{n=1}^{\infty} a_n\, 3^{-n} \mid a_n \in \{0, 2\}\}$ is the *Cantor ternary set.*

As usual, a nonempty set $C \subset \mathbb{R}$ is a *Cantor set* if and only if C is compact and does not contain nondegenerate intervals or isolated points. Equivalently, C is a *Cantor set* if and only if there is a continuous bijection from $\mathbb{D}$ onto C.

A fundamental question in descriptive analysis of the reals is whether a set $X \subset \mathbb{R}$ contains a Cantor set. An answer to this question can be important for problems concerning size and measure. For example, if $X \subset \mathbb{R}$ contains a Cantor set then (due to $|\mathbb{D}| = \boldsymbol{c}$) the sets X and $\mathbb{R}$ are equipollent. This leads to the important observation that, while $\aleph_0 < |X| < \boldsymbol{c}$ cannot be ruled out for arbitrary sets X, we can be sure that $\aleph_0 < |A| < \boldsymbol{c}$ is impossible for *closed* subsets A of the real line. (Because it is well-known that every uncountable closed subset of $\mathbb{R}$ must contain a Cantor set.) Another important example is the following. As usual, $B \subset \mathbb{R}$ is a *Bernstein set* when neither B nor $\mathbb{R} \setminus B$ contains a Cantor set. (Equivalently, neither B nor $\mathbb{R} \setminus B$ contains an uncountable closed set.) It is well-known that a Bernstein set is never Lebesgue measurable, see [1, Theorem 6.3.8].

We are interested in the existence of Cantor subsets from a specific algebraic point of view. Let us call a proper subfield of $\mathbb{R}$ a *Cantor field* if and only if it contains some Cantor set. (Notice that a proper subfield of $\mathbb{R}$ cannot contain the Cantor ternary set

2020 Mathematics Subject Classification: 12F20, 54H05.
Keywords and phrases: Transcendental extensions; descriptive set theory.

$\mathbb{D}$ because it is well-known that $\{x + y \mid x, y \in \mathbb{D}\} = [0, 2]$.) Furthermore, a *Bernstein field* is a subfield of $\mathbb{R}$ which is a Bernstein set. Trivially, each Bernstein field is a proper subfield of $\mathbb{R}$ and it cannot be a Cantor field. A trivial consequence of $|\mathbb{D}| = \boldsymbol{c}$ is that $|K| = \boldsymbol{c}$ for every Cantor field K. We also have $|K| = \boldsymbol{c}$ for every Bernstein field K. Actually, the following is true.

$$|B| = \boldsymbol{c} \quad \text{for every Bernstein set } B \subset \mathbb{R}. \tag{1}$$

There are several ways to verify (1). For example, (1) is an immediate consequence of (2) below.

For abbreviation let us call fields (taken from some collection) *incomparable* if no field is isomorphic to a subfield of another field. In particular, incomparable fields are mutually non-isomorphic. Our first main result is the following theorem. Notice that the field $\mathbb{R}$ is an *algebraic extension* of a subfield K if $\overline{K} = \mathbb{C}$. (As usual, $\overline{K}$ denotes the *algebraic closure* of the field K.)

Theorem 1.1. *There exist four families $\mathcal{C}_1, \mathcal{C}_2, \mathcal{B}_1, \mathcal{B}_2$ of subfields K of $\mathbb{R}$ with $\overline{K} = \mathbb{C}$ such that $|\mathcal{C}_1| = |\mathcal{C}_2| = |\mathcal{B}_1| = |\mathcal{B}_2| = 2^{\mathfrak{c}}$ and all fields in $\mathcal{C}_1 \cup \mathcal{C}_2$ are Cantor fields and all fields in $\mathcal{B}_1 \cup \mathcal{B}_2$ are Bernstein fields and all fields in $\mathcal{C}_1 \cup \mathcal{B}_1$ are isomorphic, whereas the fields in $\mathcal{C}_2 \cup \mathcal{B}_2$ are incomparable.*

2. Preparation for the proof

For $a \in \mathbb{R}$ and $S \subset \mathbb{R}$ we write $a + S := \{a + x \mid x \in S\}$. The following observation implies (1) and is also important for the proof of Theorem 1.1.

$$\text{Every Cantor set can be partitioned into } \boldsymbol{c} \text{ Cantor sets.} \tag{2}$$

To verify (2) let C be a Cantor set and f be homeomorphism from $\mathbb{D}$ onto C. Now consider the subset $D := \{\sum_{n=1}^{\infty} a_n \, 3^{-2n} \mid a_n \in \{0, 2\}\}$ of $\mathbb{D}$ which is clearly a Cantor set. Consequently, $\mathcal{P} = \{x + 3 \cdot D \mid x \in D\}$ is a partition of $\mathbb{D}$ consisting of Cantor sets and $|\mathcal{P}| = |D| = \boldsymbol{c}$. Thus $\{f(P) \mid P \in \mathcal{P}\}$ is a partition of C as desired.

As a consequence of the following lemma, a proper subfield K of $\mathbb{R}$ is a Bernstein field if $K \cap C \neq \emptyset$ for every Cantor set C or, equivalently, if $\mathbb{R} \setminus K$ does not contain a Cantor set. (It is not necessary to check that K does not contain a Cantor set.)

Lemma 2.1. *If K is a proper subfield of $\mathbb{R}$ which contains a Cantor set then $\mathbb{R} \setminus K$ contains a Cantor set as well.*

Proof. Let K be a subfield of $\mathbb{R}$ and $\xi \in \mathbb{R} \setminus K$. Then $\xi + k_1 = k_2$ is impossible for all $k_1, k_2 \in K$ and hence the translate $\xi + K$ is disjoint from K. Consequently, if C is a Cantor set contained in K then $\xi + C$ is a Cantor set contained in $\mathbb{R} \setminus K$. □

From Lemma 2.1 we immediately derive the following useful observation.

$$\begin{aligned}&\text{If } B \text{ is a Bernstein set and } K \text{ is a proper subfield of } \mathbb{R} \text{ and } B \subset K\\ &\text{then } K \text{ is a Bernstein field.}\end{aligned} \tag{3}$$

Remark 2.2. In view of (3) Bernstein fields can be defined in complete analogy with Cantor fields. While a proper subfield K of $\mathbb{R}$ is a *Cantor field* if and only if K *contains a Cantor set*, K is a *Bernstein field* if and only if K *contains a Bernstein set.*

As usual, for $Y \subset \mathbb{R}$ let $\mathbb{Q}(Y)$ denote the smallest subfield of $\mathbb{R}$ containing the set Y. To cut short, a set $S \subset \mathbb{R}$ is *algebraically independent* if and only if for arbitrary $n \in \mathbb{N}$ one cannot find distinct numbers $t_1, \dots, t_n$ in S such that $p(t_1, \dots, t_n) = 0$ holds for some nonconstant polynomial $p(X_1, \dots, X_n)$ in n indeterminates with rational coefficients. It is well-known (see [6]) that this definition is equivalent to the condition that $t \notin \overline{\mathbb{Q}(S \setminus \{t\})}$ for every $t \in S$. Since $\mathbb{Q}(S) \neq \mathbb{R}$ for every algebraically independent $S \subset \mathbb{R}$, from Lemma 2.1 and (3) we derive

$$\begin{aligned}&\text{If } B \text{ is a Bernstein set and } S \subset \mathbb{R} \text{ is algebraically independent and } B \subset S\\ &\text{then } S \text{ is a Bernstein set and } \mathbb{Q}(S) \text{ is a Bernstein field.}\end{aligned} \tag{4}$$

Remark 2.3. The fact that $\mathbb{Q}(S) \neq \mathbb{R}$ for every algebraically independent $S \subset \mathbb{R}$ is crucial for (4) and for what follows. This fact can be verified by several arguments. For example, it is a nice exercise to verify that $\sqrt{2} \notin \mathbb{Q}(S)$. Moreover, $\mathbb{Q}(S)$ cannot contain any irrational algebraic number. This can be verified in the following way. Firstly, if θ is transcendental over a field K then every element of $K(\theta) \setminus K$ is transcendental over K. (This important basic fact is proved in detail in [6, §73].) Secondly and consequently by induction, for every *finite* algebraically independent set $S \subset \mathbb{R}$ the set $\mathbb{Q}(S) \setminus \mathbb{Q}$ cannot contain algebraic numbers. Thirdly, this is also true for *infinite* S because for arbitrary $A \subset \mathbb{R}$ the field $\mathbb{Q}(A)$ is the union of all fields $\mathbb{Q}(E)$ with E running through the finite subsets of A.

To cut short, an algebraically independent set $S \subset \mathbb{R}$ is a *transcendence base* if and only if for each real number $x \notin S$ the set $S \cup \{x\}$ is not algebraically independent. As an immediate (and important, well-known) consequence of this maximality condition, $\mathbb{R}$ must be an algebraic extension of $\mathbb{Q}(S)$. Therefore, we easily obtain the following observation.

$$\overline{K} = \mathbb{C} \text{ for a subfield } K \text{ of } \mathbb{R} \text{ if and only if } K \text{ contains some transcendence base.} \tag{5}$$

Clearly, $|\overline{\mathbb{Q}(T)}| < \boldsymbol{c}$ whenever $T \subset \mathbb{R}$ and $|T| < \boldsymbol{c}$. Thus in view of (5) and $|\mathbb{C}| = \boldsymbol{c}$ the size of a transcendence base must be $\boldsymbol{c}$. Furthermore, it is well-known (and easy to verify) that the fields $\mathbb{Q}(S_1)$ and $\mathbb{Q}(S_2)$ are always isomorphic for algebraically independent sets S_1, S_2 of equal size. Therefore, from (4) and (5) we derive the following statement which gives a hint how to find an appropriate family $\mathcal{B}_1$ in Theorem 1.1.

$$\begin{aligned}&\text{If } B \text{ is a Bernstein set and } T \text{ is a transcendence base and } B \subset T\\ &\text{then } T \text{ is a Bernstein set and } \mathbb{Q}(T) \text{ is a Bernstein field and } \overline{\mathbb{Q}(T)} = \mathbb{C}.\end{aligned} \tag{6}$$

Thus we obtain appropriate families $\mathcal{C}_1$ and $\mathcal{B}_1$ in Theorem 1.1 by applying the following theorem which is interesting in its own right.

Theorem 2.4. *There exist two families $\mathcal{Y}_1, \mathcal{Y}_2$ of transcendence bases with $|\mathcal{Y}_1| = |\mathcal{Y}_2| = 2^{\mathbf{c}}$ such that each member of $\mathcal{Y}_1$ is a nowhere dense Lebesgue null set containing* *a Cantor set, while each member of* $\mathcal{Y}_2$ *is a Bernstein set, and for* $i \in \{1,2\}$ *and for distinct* $R, S \in \mathcal{Y}_i$ *we have* $\mathbb{Q}(R) \not\subset \mathbb{Q}(S)$ *and in particular* $\mathbb{Q}(R) \neq \mathbb{Q}(S)$.

For the proof of Theorem 2.4 we need the following lemma, which can easily be verified, and two propositions we will prove in Sections 5 and 6.

LEMMA 2.5. *If* B *is a transcendence base and* θ *is an algebraic irrational number then* $(B \setminus X) \cup \{x\theta \mid x \in X\}$ *is a transcendence base for every* $X \subset B$.

PROPOSITION 2.6. *There exists an algebraically independent Cantor set lying in* $\mathbb{D}$.

PROPOSITION 2.7. *There exist disjoint Bernstein sets* A, B *such that* $A \cup B$ *is an algebraically independent Bernstein set.*

REMARK 2.8. There is a natural analogy between algebraically independent subsets of $\mathbb{R}$ and *linearly independent* subsets of $\mathbb{R}$ (as defined in the usual way, see [1,2]), between transcendence bases and *Hamel bases.* A Hamel basis is a basis of the vector space $\mathbb{R}$ over the field $\mathbb{Q}$ and hence a *maximal* linearly independent set, while a transcendence basis is a *maximal* algebraically independent set. Consequently, *both* the existence of Hamel bases and the existence of transcendence bases are guaranteed by *one* routine argument applying Zorn's Lemma. Notice that algebraically independent sets must be linearly independent, but the converse is not true in general. (For example, it is evident that $\{\pi, \pi^2\}$ is linearly independent but not algebraically independent. Moreover, if H is a Hamel basis then H cannot be algebraically independent because, trivially, $\mathbb{Q}(H) = \mathbb{R}$.)

3. Proof of Theorem 2.4

Fix four subsets S_1, T_1, S_2, T_2 of $\mathbb{R}$ of size $\mathbf{c}$ such that $S_1 \cap T_1 = S_2 \cap T_2 = \emptyset$ and both sets $S_1 \cup T_1$ and $S_2 \cup T_2$ are transcendence bases and S_2 is a Bernstein set while S_1 is a Cantor set and $S_1 \cup T_1$ is a subset of $\mathbb{D}$. In view of Propositions 2.6 and 2.7 a choice of such sets is possible since each algebraically independent set is contained in some transcendence base and since each Cantor set can be split into two Cantor sets and since $\mathbb{Q}(\mathbb{D}) = \mathbb{R}$. (We have $\mathbb{Q}(\mathbb{D}) = \mathbb{R}$ due to $\mathbb{D} + \mathbb{D} = [0,2]$, and for every Cantor set C both $C \cap]-\infty, t]$ and $C \cap [t, \infty]$ are Cantor sets for some real $t \notin C$.) We define for every set $U \subset T_i$, $g_i(U) := S_i \cup U \cup \{x\sqrt[3]{2} \mid x \in T_i \setminus U\}$.

By virtue of Lemma 2.5, $g_i(U)$ is always a transcendence base. (In view of (9) in the next section we use the factor $\sqrt[3]{2}$ instead of the simpler factor $\sqrt{2}$.) Trivially $g_1(U)$ contains a Cantor set. As a union of three nowhere dense null sets $g_1(U)$ is a nowhere dense null set. By (4), $g_2(U)$ is a Bernstein set. Therefore Theorem 2.4 is settled by defining $\mathcal{Y}_i := \{g_i(U) \mid U \subset T_i\}$ $(i \in \{1,2\})$, because in both cases $i \in \{1,2\}$ the following statement is true.

$$\text{For } V, W \subset T_i \text{ the equality } V = W \text{ follows from } \mathbb{Q}(g_i(V)) \subset \mathbb{Q}(g_i(W)). \tag{7}$$

In order to verify (7) we show a bit more in view of the next section and Section 7. If $Y \subset \mathbb{R}$ is algebraically independent, then every algebraic number in the field $\mathbb{Q}(Y)$

is rational and hence $\sqrt[3]{2} \notin \mathbb{Q}(Y)$. Therefore (7) is an immediate consequence of the following statement.

$$\text{Let } i, j \in \{1, 2\} \text{ and } V \subset T_i \text{ and } W \subset T_j. \text{ Furthermore, let } L \text{ be a subfield of } \mathbb{R} \text{ with } \sqrt[3]{2} \notin L \text{ and } g_j(W) \subset L. \text{ Then } g_i(V) \subset L \text{ implies } V = W. \tag{8}$$

In order to verify (8), first we point out that the inclusion $g_i(V) \subset L$ enforces the identity $i = j$. Indeed, due to $g_i(V) \subset L$ and $g_j(W) \subset L$, from $i \neq j$ we derive that L contains both a Cantor set and a Bernstein set which is impossible in view of Lemma 2.1 since $L \neq \mathbb{R}$. Thus we may assume $i = j \in \{1, 2\}$ and $g_i(V) \subset L$ and $g_i(W) \subset L$ and $\sqrt[3]{2} \notin L$. To conclude the proof of (8) by verifying $V = W$ assume indirectly that there is a real $x \in (V \setminus W) \cup (W \setminus V)$. Then the pair $(x, x\sqrt[3]{2})$ lies in $g_i(V) \times g_i(W)$ or in $g_i(W) \times g_i(V)$. Consequently the field L contains both reals $x, x\sqrt[3]{2}$ and hence also the quotient $\sqrt[3]{2}$ which is a contradiction.

4. Proof of Theorem 1.1

For every subfield K of $\mathbb{R}$ let K^* denote the intersection of all fields L satisfying $K \subset L \subset \mathbb{R}$ and the property that $\sqrt{|x|} \in L$ for every $x \in L$. Of course, $K \subset K^* \subset \mathbb{R} \cap \overline{K}$ and $\sqrt{|x|} \in K^*$ for all $x \in K^*$ or, equivalently, $K^{**} = K^*$. Alternatively, K^* is obtained from K by successively adjoining square roots. Define inductively $W_0 = K$ and $W_n = \mathbb{Q}(\{\sqrt{|x|} \mid x \in W_{n-1}\})$ for $n \in \mathbb{N}$ in order to finally obtain $K^* = \bigcup_{n=1}^{\infty} W_n$. (As usual in number theory, $0 \notin \mathbb{N}$.)

A fortiori $\overline{\mathbb{Q}(T)^*} = \mathbb{C}$ for every transcendence base T, where $\mathbb{Q}(T)^* \neq \mathbb{R}$ due to the following observation.

$$\text{If } Y \subset \mathbb{R} \text{ is an algebraically independent set then } \sqrt[3]{2} \notin \mathbb{Q}(Y)^*. \tag{9}$$

Obviously (9) is a consequence of the following two statements.

$$\text{If } K \text{ is a subfield of } \mathbb{R} \text{ then every number in } K^* \setminus K \text{ is algebraic over } K \text{ of degree } 2^n \text{ with } n \in \mathbb{N}. \tag{10}$$

$$\text{For every algebraically independent set } Y \subset \mathbb{R} \text{ the degree of } \sqrt[3]{2} \text{ over the field } \mathbb{Q}(Y) \text{ equals 3.} \tag{11}$$

We obtain (10) from the well-known fact that K^* is the field of all reals which are *constructible* over K by a finite sequence of *ruler and compass* constructions.

In order to verify (11) let $Y \subset \mathbb{R}$ be algebraically independent and consider distinct $y_1, \ldots, y_n \in Y$ for arbitrary $n \in \mathbb{N}$. Naturally the field $\mathbb{Q}(y_1, \ldots, y_n)$ is isomorphic with the quotient field $\mathbb{Q}(X_1, \ldots, X_n)$ of the polynomial ring $\mathbb{Z}[X_1, \ldots, X_n]$ which is a unique factorization domain and in which 2 is irreducible. Consequently, by Eisenstein's Criterion the polynomial $X^3 - 2$ is irreducibel over the field $\mathbb{Q}(X_1, \ldots, X_n)$. Thus $X^3 - 2$ is irreducibel over $\mathbb{Q}(y_1, \ldots, y_n)$ and hence $X^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over the field $\mathbb{Q}(Y)$ and (11) is proved.

Now we take the transcendence bases $g_i(\cdot)$ from the previous section and define $\mathcal{C}_2 := \{\mathbb{Q}(g_1(U))^* \mid U \subset T_1\}$ and $\mathcal{B}_2 := \{\mathbb{Q}(g_2(U))^* \mid U \subset T_2\}$.

Then all fields in $\mathcal{C}_2$ resp. $\mathcal{B}_2$ are Cantor fields resp. Bernstein fields. Furthermore, concluding the proof of Theorem 1.1, the following statement shows that $|\mathcal{C}_2| = |\mathcal{B}_2| = 2^{\mathfrak{c}}$ and the fields in $\mathcal{C}_2 \cup \mathcal{B}_2$ are incomparable.

$$\begin{array}{l}\text{For } i,j \in \{1,2\} \text{ and } V \subset T_i \text{ and } W \subset T_j \text{ the field } \mathbb{Q}(g_i(V))^* \\ \text{can be embedded into the field } \mathbb{Q}(g_j(W))^* \text{ only if } V = W.\end{array} \tag{12}$$

The following lemma shows that if $\mathbb{Q}(g_i(V))^*$ can be embedded into $\mathbb{Q}(g_j(W))^*$ then already $\mathbb{Q}(g_i(V))^* \subset \mathbb{Q}(g_j(W))^*$ holds. Consequently and in view of (9) we obtain (12) from (8) with $L := \mathbb{Q}(g_j(W))^*$.

Lemma 4.1. *If K is a subfield of $\mathbb{R}$ with $K^* = K$ and φ is a monomorphism from K to $\mathbb{R}$ then $\varphi(x) = x$ for all $x \in \mathbb{R}$.*

Proof. It goes without saying that $\varphi(r) = r$ for all $r \in \mathbb{Q}$. Due to $K^* = K$ we have $\sqrt{|a|} \in K$ for every $a \in K$. Now let $x \in K$ and $r \in \mathbb{Q}$. If $r < x$ then $\varphi(x)-\varphi(r) = \varphi(x-r) = \varphi(\sqrt{x-r})^2 > 0$, and if $r > x$ then $\varphi(r)-\varphi(x) = \varphi(r-x) = \varphi(\sqrt{r-x})^2 > 0$. Thus φ is strictly increasing and, since φ restricted to the domain $\mathbb{Q}$ is the identity, for all $r, s \in \mathbb{Q}$ and $x \in K$ the implication $r < x < s \Rightarrow r < \varphi(x) < s$ holds and this enforces $\varphi(x) = x$ for all $x \in K$. □

5. Proof of Proposition 2.6

As usual, ZF means ZFC set theory minus the Axiom of Choice. In this section we are going to prove Proposition 2.6 without applying the Axiom of Choice. This has the benefit that the following trivial consequence of Theorem 1.1 turns out to be a theorem in ZF.

Corollary 5.1. *There exist two families $\mathcal{C}_3, \mathcal{C}_4$ equipollent with the power set of $\mathbb{R}$ such that $\mathcal{C}_3$ consists of isomorphic Cantor fields while $\mathcal{C}_4$ consists of incomparable Cantor fields.*

Remark 5.2. There are two reasons why Theorem 1.1 is not a theorem in ZF. Firstly, the existence of a proper subfield K of $\mathbb{R}$ satisfying $\overline{K} = \mathbb{C}$ is unprovable in ZF because of (5) and the well-known fact that the existence of transcendence bases is unprovable in ZF. Secondly, the existence of a Bernstein set (and in particular the existence of a Bernstein field) cannot be derived from the axioms of ZF only. Additionally, equations like $|\mathcal{F}| = 2^{\mathfrak{c}}$ need to be interpreted in a specific way in ZF since $|X|$ is not defined in ZF for arbitrary sets X. (But notice that sets like $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{D}$ are well-defined objects in ZF. Notice also that in ZF the field $\overline{K} \cap \mathbb{R}$ is well-defined for each subfield K of $\mathbb{R}$ constructed in ZF.)

If C is an algebraically independent Cantor set in ZF then a ZF-proof of Corallary 5.1 can easily be obtained by adopting parts of the ZFC-proof of Theorem 1.1. Simply split C constructively into two disjoint Cantor sets C_1, C_2 and define the sets S_1 and T_1 in the proof of Theorem 1.1 via $S_1 = C_1$ and $T_1 = C_2$. Then, never considering transcendence bases, $C_1 \cup U \cup \{x\sqrt[3]{2} \mid x \in C_2 \setminus U\}$ is algebraically independent for all $U \subset C_2$ and this is enough. Alternatively, there is a direct and much shorter ZF-proof of Corollary 1 as follows. With C_1, C_2 as above put $\mathcal{C}_3 := \{\overline{\mathbb{Q}(C_1 \cup X)} \,|\, X \subset C_2\}$ and $\mathcal{C}_4 := \{\mathbb{R} \cap \overline{\mathbb{Q}(C_1 \cup X)} \,|\, X \in \mathcal{F}\}$ where $\mathcal{F}$ is a family equipollent with the power set of $\mathbb{R}$ such that $X \subset C_2$ for every $X \in \mathcal{F}$ and $X \not\subset Y$ whenever $X, Y \in \mathcal{F}$ are distinct. (Such a family $\mathcal{F}$ can easily be constructed in ZF. For example take a bijection f from $\mathbb{R}$ onto C_2 and put $\mathcal{F} := \{f(T \cup ([2,3] \setminus (2+T))) \,|\, T \subset [0,1]\}$.) The family $\mathcal{C}_3$ obviously fits and the family $\mathcal{C}_4$ does the job by virtue of Lemma 4.1.

There is a more algebraic way and a more topological way to prove Proposition 2.6 in ZF. The algebraic way is far from being elementary since an appropriate modification of the famous *von Neumann numbers* (see [5]) is used.

As usual, $[\xi]$ denotes the largest integer $k \leq \xi$ for $\xi \in \mathbb{R}$. We put $\psi(x,n) := 2^{n^2} - 2^{[nx]}$ and observe that $0 < \psi(x,n) < \psi(x,m)$ whenever $n, m \in \mathbb{N}$ and $0 < x < n < m$. Consequently, $\sigma(x) := 2 \cdot \sum_{n>x} 3^{-\psi(x,n)}$ defines a function from $]0,\infty[$ into $\mathbb{D}$ for all $x \in \mathbb{R}$. (Notice that the von Neumann numbers are not contained in $\mathbb{D}$.) In the same way as carried out in [5] one can verify that $\sigma(x) \notin \overline{\mathbb{Q}(\sigma(]0,x[))}$ for every $x > 0$. Hence σ is injective and the set $\sigma(]0,\infty[)$ is algebraically independent. It goes without saying that σ is continuous at each positive irrational. Now consider the uncountable partition $\mathcal{P}$ of $\mathbb{D}$ defined in the proof of (2) and obviously well-defined in ZF. Then $\mathcal{P}^* := \{X \in \mathcal{P} \,|\, X \cap \mathbb{Q} \neq \emptyset\}$ is a countable subfamily of $\mathcal{P}$ and hence the family $\mathcal{P} \setminus \mathcal{P}^*$ is not empty. Hence we can select an element C from this family. Automatically, C is a Cantor set containing only irrational numbers. Consequently, $\sigma(C)$ is a Cantor set lying in an algebraically independent set and this concludes the ZF-proof of Proposition 2.6.

Alternatively we now present an elementary ZF-proof of Proposition 2.6. (Notice that $\mathbb{D}$ is well-defined in ZF). In doing so we show a bit more, namely that the following statement (which cannot be verified using some modification of the von Neumann numbers) is a theorem in ZF.

$$\text{Every Cantor set } D \text{ contains an algebraically independent Cantor set.} \tag{13}$$

First of all recall the standard construction of the Cantor ternary set $\mathbb{D} = \bigcap_{k=1}^{\infty} \bigcup_{j=1}^{2^k} \mathcal{J}_{k,j}$ where $\mathcal{J}_{1,1} = [0, \frac{1}{3}]$ and $\mathcal{J}_{1,2} = [\frac{2}{3}, 1]$ and $\mathcal{J}_{2,1} = [0, \frac{1}{9}]$ and $\mathcal{J}_{2,2} = [\frac{2}{9}, \frac{1}{3}]$ and $\mathcal{J}_{2,3} = [\frac{2}{3}, \frac{7}{9}]$ and $\mathcal{J}_{2,4} = [\frac{8}{9}, 1]$ and so on.

For $n \in \mathbb{N}$ consider the ring $R_n = \mathbb{Z}[X_1, \ldots, X_n]$ of all integral polynomials in n indeterminates. Of course, R_n is a countable set. For every $n \in \mathbb{N}$ let g_n be a bijection from $\mathbb{N}$ onto $R_n \setminus \mathbb{Z}$. For $(n,m) \in \mathbb{N}^2$ let $A(n,m)$ denote the set of all n-tuples $(t_1, \ldots, t_n)$ of reals that are annihilated by the polynomial $g_n(m)$. Naturally, $A(n,m)$ is a *closed* subset of the space $\mathbb{R}^n$. Furthermore, $A(n,m)$ is *nowhere dense* because for an integral polynomial $p(X_1, \ldots, X_n)$ the equation $p(t_1, \ldots, t_n) = 0$ holds for all points $(t_1, \ldots, t_n)$ in a nonempty open subset of $\mathbb{R}^n$ only if $p(X_1, \ldots, X_n)$ is the zero polynomial.

For $a \leq b$ put $\lambda([a,b]) := b - a$. For every $k \in \mathbb{N}$ choose 2^k pairwise disjoint compact intervals $\mathcal{I}_{k,j} (1 \leq j \leq 2^k)$ such that $\mathcal{I}_{m,j} \supset \mathcal{I}_{m+1,2j} \cup \mathcal{I}_{m+1,2j-1}$ whenever $m, j \in \mathbb{N}$ and $j \leq 2^m$ and that $\lim_{k\to\infty} \max\{\lambda(\mathcal{I}_{k,j}) \,|\, 1 \leq j \leq 2^k\} = 0$. Certainly, in each parallelepiped of positive volume there lies a parallelepiped of positive volume disjoint with the closed, and nowhere dense point set $A(n,m)$. Therefore, step by step it can be accomplished that the following condition $\mathbf{B}[m]$ holds for all $m \in \mathbb{N}$ as well.

($\mathbf{B}[m]$) *$A(n,m) \cap \prod_{i=1}^{n} \varphi(i) = \emptyset$ whenever $n \in \mathbb{N}$ and φ is an injection from $\{1,\ldots,n\}$ into $\{\mathcal{I}_{m,1},\ldots,\mathcal{I}_{m,2^m}\}$.*

In comparison with the standard construction of the ternary Cantor set it is clear that $C := \bigcap_{k=1}^{\infty} \bigcup_{j=1}^{2^k} \mathcal{I}_{k,j}$ is a Cantor set. (Alternatively it is plain that C is compact, dense in itself and does not contain isolated points.) We claim that C is algebraically independent.

Assume indirectly that C is not algebraically independent. Then we can find distinct numbers $t_1, t_2, \ldots, t_n$ in C such that the n-tuple $(t_1, t_2, \ldots, t_n)$ is annihilated by some non-zero polynomial p in the ring $\mathbb{Z}[X_1,\ldots,X_n]$. Trivially, this n-tuple is also annihilated by the polynomial $k \cdot p(X_1,\ldots,X_n)$ for every $k \in \mathbb{N}$. Hence there is an infinite set $M \subset \mathbb{N}$ such that for all $m \in M$ the point $(t_1,\ldots,t_n)$ lies in the set $A(n,m)$. Now choose $m \in M$ sufficiently large such that each one of the 2^m intervals $\mathcal{I}_{m,j}$ contains at most one of the numbers $t_1,\ldots,t_n$. This provides us with an injection φ from $\{1,\ldots,n\}$ into $\{\mathcal{I}_{m,1},\ldots\mathcal{I}_{m,2^m}\}$ such that the point $(t_1,\ldots,t_n)$ lies in the parallelepiped $\prod_{i=1}^{n} \varphi(i)$. This is a contradiction to $\mathbf{B}[m]$ since $(t_1,\ldots,t_n) \in A(n,m)$.

So we have proved that C is algebraically independent. In doing so also Proposition 2.6 is settled because in choosing the intervals $\mathcal{I}_{k,j}$ we can take care that always $\mathcal{I}_{k,j} \subset \mathcal{J}_{k,j}$, which trivially implies $C \subset \mathbb{D}$. Moreover, an appropriate choice of the intervals $\mathcal{I}_{k,j}$ is also possible to accomplish $C \subset D$ for an arbitrary Cantor set D and hence (13) is settled. This is indeed true in view of the following proposition about Cantor sets and because $f\big(\bigcap_k \bigcup_j \mathcal{I}_{k,j}\big) = \bigcap_k \bigcup_j f(\mathcal{I}_{k,j})$ and $f([u,v]) = [f(u), f(v)]$ for every increasing bijection $f : \mathbb{R} \to \mathbb{R}$.

Proposition 5.3. *A nonempty set $C \subset \mathbb{R}$ is compact, totally disconnected and dense in itself if and only if $C = f(\mathbb{D})$ for some increasing bijection f from $\mathbb{R}$ onto $\mathbb{R}$.*

Proof. Naturally, every strictly increasing function f from $\mathbb{R}$ onto $\mathbb{R}$ is a homeomorphism. Hence as the topological space $\mathbb{D}$ the set $f(\mathbb{D})$ is compact, totally disconnected and dense in itself. Conversely let $D_1 = C$ similarly as $D_0 = \mathbb{D}$ be a compact, totally disconnected and dense-in-itself subspace of $\mathbb{R}$. In the following, $i \in \{0,1\}$.

The set D_i has a maximum and a minimum due to compactness. Let $a_i = \min D_i$ and $b_i = \max D_i$. (In particular, $a_0 = 0$ and $b_0 = 1$.) Since the set $[a_i,b_i] \setminus D_i$ is open, we can define a family $\mathcal{U}_i$ of pairwise disjoint open intervals such that $\bigcup \mathcal{U}_i \subset [a_i,b_i]$ and $D_i = [a_i,b_i] \setminus \bigcup \mathcal{U}_i$.

In a natural way the family $\mathcal{U}_i$ is linearly ordered by declaring $U \in \mathcal{U}_i$ *smaller than* $V \in \mathcal{U}_i$ if and only if $\sup U \le \inf V$. Since D_i is totally disconnected, $\bigcup \mathcal{U}_i$ is dense in $[a_i,b_i]$. And since D_i has no isolated point, between two intervals from $\mathcal{U}_i$ there always lie infinitely many intervals from $\mathcal{U}_i$. Finally, the linearly ordered set $\mathcal{U}_i$ has neither a smallest nor a largest element.

Taking all these observations into account, by virtue of a well-known classical theorem by Cantor, the linearly ordered set $\mathcal{U}_i$ is order-isomorphic to the naturally ordered set $\mathbb{Q}$. In particular the two families $\mathcal{U}_0$ and $\mathcal{U}_1$ are order-isomorphic. Since for $u < v$ and $r < s$ the interval $]u, v[$ can easily be mapped onto the interval $]r, s[$ by a strictly increasing function, with the help of an order-isomorphism from $\mathcal{U}_0$ onto $\mathcal{U}_1$ we obtain an increasing bijection g from $\bigcup \mathcal{U}_0$ onto $\bigcup \mathcal{U}_1$. This function g can be extented to a continuous function f from $\mathbb{R}$ to $\mathbb{R}$ by defining $f(t) := a_1 + t$ for $t \leq 0$ and $f(t) := b_1 + t - 1$ for $t \geq 1$ and $f(t) := \sup\{g(x) \,|\, x \in \bigcup \mathcal{U}_0 \wedge x \leq t\}$ for $0 < t < 1$. Obviously f is strictly increasing and surjective and $f(\mathbb{D}) = C$. $\square$

Remark 5.4. Proposition 5.3 can be regarded as a *purely algebraic* characterization of Cantor sets. Because firstly in the definition of $\mathbb{D}$ the series $\sum a_n 3^{-n}$ need not refer to the topological concept *convergency* but can be regarded as the depiction of a sequence of digits. And secondly, *monotonicity* of real functions can be characterized purely algebraically because a mapping f from $\mathbb{R}$ into $\mathbb{R}$ is increasing if and only if for arbitrary $u, v \in \mathbb{R}$ the equation $(u - v)(f(u) - f(v)) = x^2$ has a real solution x.

Remark 5.5. The existence of an algebraically independent Cantor set, which is a trivial consequence of (13), can be obtained by applying the Kuratowski-Mycielski theorem [2, 19.1]. However, this theorem is not elementary (since arguments using Vietoris topologies occur) and it does not imply (13), even not in ZFC. On the other hand, our proof of (13) is elementary and, since it is carried out in ZF, constructive as well. In view of [2, 19.2(i)] there exists a Hamel basis which contains a Cantor set. Even more, by applying (13) *there exist a Cantor set C and a transcendence basis T and a Hamel basis H such that $C \subset T \subset H \subset \mathbb{D}$.* (Inevitably, $T \neq H$ since H cannot be algebraically independent.)

6. Proof of Proposition 2.7

Let $\mathcal{D}$ be the family of all Cantor sets. We have $|\mathcal{D}| = \mathbf{c}$ since every set in $\mathcal{D}$ is compact and $\mathbb{R}$ contains precisely $\mathbf{c}$ closed sets and since the translate $x + \mathbb{D}$ is obviously a Cantor set for each one of the $\mathbf{c}$ real numbers x.

In the following we regard the cardinal $\mathbf{c}$ as an initial ordinal number and use the ordinal numbers $\alpha < \mathbf{c}$ for indexing real numbers and sets of real numbers. (Keep in mind the crucial estimate $|\{\beta \,|\, \beta < \alpha\}| < \mathbf{c}$ whenever $\alpha < \mathbf{c}$.) Since $|\{\alpha \,|\, \alpha < \mathbf{c}\}| = \mathbf{c}$, we can write $\mathcal{D} = \{D_\alpha \,|\, \alpha < \mathbf{c}\}$ (and we do not care whether the mapping $\alpha \mapsto D_\alpha$ is injective or not). Let ρ be a choice function defined on the nonempty subsets of $\mathbb{R}$. Thus $\rho(X) \in X$ for every nonempty set $X \subset \mathbb{R}$.

Now, by induction we define real numbers x_α and y_α for all $\alpha < \mathbf{c}$. Assume that for $\xi < \mathbf{c}$ real numbers x_α and y_α are already defined for all $\alpha < \xi$. (This assumption is vacuous if $\xi = 0$.) Then define necessarily distinct real numbers x_ξ and y_ξ in two steps. Put $x_\xi := \rho\big(D_\xi \setminus \overline{\mathbb{Q}(\{x_\alpha \,|\, \alpha < \xi\} \cup \{y_\alpha \,|\, \alpha < \xi\})}\big)$ and then, with respect to this definition of x_ξ, put $y_\xi := \rho\big(D_\xi \setminus \overline{\mathbb{Q}(\{x_\alpha \,|\, \alpha \leq \xi\} \cup \{y_\alpha \,|\, \alpha < \xi\})}\big)$.

Both definitions are correct since the choice function ρ is always applied to a nonempty set. Indeed, for arbitrary $Y, T \subset \mathbb{R}$ the set $Y \setminus \overline{\mathbb{Q}(T)}$ certainly is nonempty provided that $|Y| = \mathbf{c}$ and $|T| < \mathbf{c}$ because the field $\overline{\mathbb{Q}(T)}$ is either countable or equipollent with T. So in this way we have defined real numbers x_α and y_α for each $\alpha < \mathbf{c}$ such that $x_\alpha \neq x_\beta$ and $y_\alpha \neq y_\beta$ whenever $\alpha \neq \beta$ and that $\{x_\alpha \,|\, \alpha < \mathbf{c}\} \cap \{y_\alpha \,|\, \alpha < \mathbf{c}\} = \emptyset$. Moreover, the specific choices of the real numbers x_α, y_α immediately yield

$$\text{The set } \{x_\alpha \,|\, \alpha < \mathbf{c}\} \cup \{y_\alpha \,|\, \alpha < \mathbf{c}\} \text{ is algebraically independent.} \tag{14}$$

Finally, in view of (14) and (4) Proposition 2.7 is settled with the definitions $A := \{x_\alpha \,|\, \alpha < \mathbf{c}\}$ and $B := \{x_\alpha \,|\, \alpha < \mathbf{c}\}$ because A and B are disjoint and, due to $\{x_\alpha, y_\alpha\} \subset D_\alpha$ for every $\alpha < \mathbf{c}$, A meets every Cantor set and B meets every Cantor set.

7. Extremely large fields

Due to the condition $\overline{K} = \mathbb{C}$ the fields depicted in Theorem 1.1 are rather large. But in a certain sense they are not extremely large. Let K be a subfield of $\mathbb{R}$. Naturally, $\mathbb{R}$ is a vector space over the field K. As usual, $[\mathbb{R} : K]$ denotes the dimension of the K-vector space $\mathbb{R}$. Naturally, in the nontrivial case $K \neq \mathbb{R}$ the dimension $[\mathbb{R} : K]$ is always an infinite cardinal number not greater than $\mathbf{c} = |\mathbb{R}|$.

For every field K in the family $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{B}_1 \cup \mathcal{B}_2$ defined in the proof of Theorem 1.1 we have $[\mathbb{R} : K] = \mathbf{c}$ because if T is a transcendence base then $[\mathbb{R} : \mathbb{Q}(T)] = \mathbf{c}$ (see [3, Theorem 4]) and we have $[\mathbb{R} : \mathbb{Q}(T)^*] = \mathbf{c}$ as well. (Of course, $[\mathbb{R} : \mathbb{Q}(T)^*] = \mathbf{c}$ implies $[\mathbb{R} : \mathbb{Q}(T)] = \mathbf{c}$ and $[\mathbb{R} : \mathbb{Q}(T)^*] = \mathbf{c}$ can be proved by verifying that the $\mathbf{c}$ reals $\sqrt[3]{t}$ $(t \in T)$ are linearly independent vectors in the vector space $\mathbb{R}$ over the field $\mathbb{Q}(T)^*$.)

One may regard a subfield K of $\mathbb{R}$ *larger than* a subfield L of $\mathbb{R}$ when $[\mathbb{R} : K] < [\mathbb{R} : L]$. In this sense the following theorem provides extremely many mutually non-isomorphic *extremely large* Cantor fields and Bernstein fields, respectively. Notice that (as explained in [3]) we must have $\overline{K} = \mathbb{C}$ for a subfield K of $\mathbb{R}$ satisfying the condition $[\mathbb{R} : K] = \aleph_0$.

Theorem 7.1. *In Theorem 1.1 it can be accomplished that* $[\mathbb{R} : K] = \aleph_0$ *for every field* K *in the family* $\mathcal{C}_2 \cup \mathcal{B}_2$.

In order to settle Theorem 7.1 we consider the families $\mathcal{C}_2, \mathcal{B}_2$ defined in Section 4, expand each field K in $\mathcal{C}_2 \cup \mathcal{B}_2$ to an appropriate proper subfield $\hat{K}$, and replace $\mathcal{C}_2$ and $\mathcal{B}_2$ by $\{\hat{K} \,|\, K \in \mathcal{C}_2\}$ and $\{\hat{K} \,|\, K \in \mathcal{B}_2\}$. In view of (8) this is enough provided that for each subfield K of $\mathbb{R}$ with $\sqrt[3]{2} \notin K$ we can find a subfield $\hat{K}$ of $\mathbb{R}$ with $\sqrt[3]{2} \notin \hat{K}$ and $\hat{K} \supset K$ and $[\mathbb{R} : \hat{K}] = \aleph_0$.

So let K be a subfield of $\mathbb{R}$ with $\sqrt[3]{2} \notin K$. Then the family $\mathcal{F}$ of all subfields L of $\mathbb{R}$ with $\sqrt[3]{2} \notin L$ and $L \supset K$ is not empty. Clearly, $\bigcup \mathcal{G} \in \mathcal{F}$ for every chain $\mathcal{G}$ of fields in $\mathcal{F}$. Consequently, by applying Zorn's Lemma, the partially ordered family $(\mathcal{F}, \subset)$ has a maximal element $\hat{K}$. Such a field $\hat{K}$ is a subfield of $\mathbb{R}$ satisfying for the irrational number $\theta = \sqrt[3]{2}$ the property that $\theta \notin \hat{K}$ but $\theta \in L$ for every field L with $\hat{K} \subset L \subset \mathbb{R}$

and $L \neq \hat{K}$. By applying methods from infinite-dimensional Galois theory we can prove that every field $\hat{K}$ of this kind satisfies $[\mathbb{R} : \hat{K}] = \aleph_0$, see [4, Proposition 3]. This concludes the proof of Theorem 7.1.

References

[1] K. Ciesielski, *Set Theory for the Working Mathematician*, Cambridge 1997.

[2] A. Kechris, *Classical Descriptive Set Theory*, Springer 1995.

[3] G. Kuba, *Über den Grad unendlicher Körpererweiterungen*, Mitt. Math. Seminar, Univ. Hamburg **26** (2007), 117–124.

[4] G. Kuba, *Counting fields of complex numbers*, Am. Math. Monthly, **116(6)** (2009), 541–547.

[5] J. von Neumann, *Ein System algebraisch unabhängiger Zahlen*, Math. Ann., **99** (1928), 134–141.

[6] B.L. van der Waerden,*Algebra I.* Springer-Verlag, 1971.

(received 29.01.2021; in revised form 04.01.2022; available online 18.07.2022)

Institute of Mathematics, University of Natural Resources and Life Sciences, Vienna, Austria
E-mail: gerald.kuba@boku.ac.at