JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Moshe JARDEN et Carlos VIDELA

Fields on the Bottom

Tome 28, n^o^ 1 (2016), p. 213-219.

<http://jtnb.cedram.org/item?id=JTNB_2016__28_1_213_0>

Journal de Théorie des Nombres
de Bordeaux **28** (2016), 213–219

Fields on the Bottom

par Moshe JARDEN et Carlos VIDELA

Résumé. Nous notons $\mathbb{Q}_{\mathrm{tr}}$ le corps des nombres totalement réels. Etant donné un ensemble S de nombres premiers, nous notons $\mathbb{Q}^{(S)}$ l'extension galoisienne maximale de $\mathbb{Q}$ de degré seulement divisible par des nombres premiers dans S. Nous démontrons que le corps $\mathbb{Q}_{\mathrm{tr},S} = \mathbb{Q}_{\mathrm{tr}} \cap \mathbb{Q}^{(S)}$ n'a pas de sous corps propre M avec $[\mathbb{Q}_{\mathrm{tr},X} : M] < \infty$.

Abstract. We denote the field of totally real numbers by $\mathbb{Q}_{\mathrm{tr}}$. For a set S of prime numbers we let $\mathbb{Q}^{(S)}$ be the maximal Galois extension of $\mathbb{Q}$ whose degree is divisible only by prime numbers in S. We prove that the field $\mathbb{Q}_{\mathrm{tr},S} = \mathbb{Q}_{\mathrm{tr}} \cap \mathbb{Q}^{(S)}$ has no proper subfield M with $[\mathbb{Q}_{\mathrm{tr},S} : M] < \infty$.

Introduction

We say that a field F *lies on the bottom* if F contains no field E with $1 < [F : E] < \infty$. By definition, each of the prime fields $\mathbb{Q}$ and $\mathbb{F}_p$ lies on the bottom. By a theorem of Artin, every separably closed field of positive characteristic lies on the bottom (see for example the proof of [7, Cor. 9.3]). In particular, the absolute Galois group $\mathrm{Gal}(K)$ of a field K of positive characteristic is torsion free.

The same theorem combined with another theorem of Artin [7, p. 452, Prop. 2.4] implies that every real closed field lies on the bottom. Again, this implies that the only torsion elements of the absolute Galois group of a field K are involutions.

By a theorem of F. K. Schmidt, each Henselian closure of $\mathbb{Q}$ with respect to a prime number p lies on the bottom (e.g. [5, Cor. 15.3]).

By the "Bottom Theorem" [4, Thm. 18.7.7], for every positive integer e and almost all $(\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(\mathbb{Q})^e$ the field $\tilde{Q}(\sigma_1, \ldots, \sigma_e)$ lies on the bottom. Here $\tilde{Q}(\sigma_1, \ldots, \sigma_e)$ is the fixed field of $\sigma_1, \ldots, \sigma_e$ in the algebraic closure $\tilde{Q}$ of $\mathbb{Q}$. The clause "almost all" means "all but a subset of $\mathrm{Gal}(\mathbb{Q})^e$ of Haar measure 0".

Manuscrit reçu le 27 décembre 2013, révisé le 15 mars 2014, accepté le 11 avril 2014.

Mathematics Subject Classification. 12E30.

Mots-clefs. Bottom theorem, Pythagorean field, totally real number.

Research initiated in a working team during a conference on Definability and decidability problems in number theory, in the American Institute for Mathematics, Palo Alto, California, September 2013.

We mention that Lior Bary-Soroker [1] strengthened the bottom theorem in the following way: Let K be a finitely generated extension of $\mathbb{Q}$ and let $e \geq 2$ be an integer. Then, for almost all $(\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ the field $\tilde{K}(\sigma_1, \ldots, \sigma_e)$ lies on the bottom [1, Thm. 8.2.2].

Next, we recall that a field F is *pythagorean* if every sum of two squares in F is a square in F. It follows that every sum of finitely many squares in F is a square in F. It also follows that the intersection of pythagorean subfields of a field Ω (which we assume to be algebraically closed) is pythagorean. Note that every algebraically closed field is pythagorean. Hence, the intersection of all pythagorean field extensions of a given field K in Ω is the smallest algebraic extension of K which is pythagorean. We denote it by K_{pyt}. If $\mathrm{char}(K) \neq 2$, then K_{pyt} is a Galois extension of K. Indeed, K_{pyt} is the smallest algebraic extension of K closed under extensions with elements of the form $\sqrt{x^2+y^2}$. By [12, p. 176], $\mathbb{Q}_{\mathrm{pyt}}$ lies on the bottom.

In order to present our results, we consider the field $\mathbb{Q}_{\mathrm{tr}}$ of all totally real algebraic numbers. It is the union of all finite extensions K of $\mathbb{Q}$ whose images under all embeddings into $\mathbb{C}$ lie in $\mathbb{R}$. It is also the intersection of all real closures of $\mathbb{Q}$ in $\tilde{Q}$. Since the absolute Galois group of a real closed field has order two, $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tr}})$ is generated by involutions.

By a result of Florian Pop ([10] and [11, p. 25]), $\mathbb{Q}_{\mathrm{tr}}$ is *PRC*. This means that every absolutely irreducible variety defined over $\mathbb{Q}_{\mathrm{tr}}$ with a simple R–rational point for each real closure R of $\mathbb{Q}_{\mathrm{tr}}$ has a $\mathbb{Q}_{\mathrm{tr}}$–rational point. This result is a consequence of a local-global principle of Laurent Moret-Bailly [9, Thm. 1.3 and Rem. 1.7]. Michael Fried, Dan Haran, and Helmut Völklein proved in [2] that $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tr}})$ is a free profinite product (in the sense of Melnikov [8]) of groups of order 2. They also proved that the elementary theory of $\mathbb{Q}_{\mathrm{tr}}$ is effectively decidable [3, Thm. 10.1].

Our goal is to enrich the already rich collection of properties of $\mathbb{Q}_{\mathrm{tr}}$ with the following one:

Main Theorem. *For every set S of prime numbers, the field $\mathbb{Q}_{\mathrm{tr},S} = \mathbb{Q}_{\mathrm{tr}} \cap \mathbb{Q}^{(S)}$ lies on the bottom.*

To this end we define $K^{(S)}$ for a field K and a set S of prime numbers as the union of all finite Galois field extensions L of K whose degrees $[L : K]$ are divisible only by prime numbers that belong to S.

In particular, if S is the set of all prime numbers, then $\mathbb{Q}^{(S)} = \tilde{Q}$ and $\mathbb{Q}_{\mathrm{tr},S} = \mathbb{Q}_{\mathrm{tr}}$. In this case, the main theorem becomes the following result.

Corollary. *The field $\mathbb{Q}_{\mathrm{tr}}$ lies on the bottom*

The proof of the main theorem uses information about pythagorean fields, an old theorem of George Whaples, and an older theorem of Edmund Landau.

Remark. As the referee pointed out, if N is a Galois extension of $\mathbb{Q}$, then the statement "N lies on the bottom" is equivalent to "$\mathrm{Gal}(N/\mathbb{Q})$ is torsion-free". If N is an arbitrary algebraic extension of $\mathbb{Q}$ that lies on the bottom, then it is still true that $\mathrm{Aut}(N/\mathbb{Q})$ is torsion-free. But the converse is not true. For example, $\mathbb{Q}(\sqrt[3]{2})$ does not lie on the bottom although $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is trivial, so torsion-free.

Acknowledgement. The authors are indebted to the referee for comments that led to an improvement of the presentation of this note.

1. Basic facts

We present a few facts and results that enter the proof of the main theorem.

Lemma 1.1. *If F/M is a cyclic extension of odd prime degree p, then F has a cyclic extension of degree p.*

Proof. By a result of Whaples from 1957 [4, Thm. 16.6.6], M has a Galois extension N with $\mathrm{Gal}(N/M) \cong \mathbb{Z}_p$. The compositum FN is a Galois extension of F and $\mathrm{Gal}(FN/F) \cong \mathrm{Gal}(N/F \cap N)$. The latter group is isomorphic to an open subgroup of $\mathbb{Z}_p$, hence to $\mathbb{Z}_p$ itself [4, Lemma 1.4.2]. It follows that $\mathrm{Gal}(FN/F) \cong \mathbb{Z}_p$. Hence, F has a finite cyclic extension of degree p in FN. □

Next we need the following result about pythagorean fields which is proved on page 176 of [12]. It is a corollary of a theorem of Diller and Dress.

Proposition 1.2. *If a finite extension of a field P_0 is pythagorean, then P_0 itself is pythagorean.*

Finally recall that an algebraic number a is *totally real* if $\varphi(a) \in \mathbb{R}$ for every embedding $\varphi\colon \tilde{Q} \to \mathbb{C}$. If in addition $\varphi(a) > 0$ for each such φ, then a is *totally positive*. Note that if a is totally real and $a \neq 0$, then a^2 is totally positive.

Lemma 1.3. $\mathbb{Q}_{\mathrm{tr}}$ *is a pythagorean field.*

Proof. Given elements $x, y \in \mathbb{Q}_{\mathrm{tr}}$, not both zero, the sum $x^2 + y^2$ is totally positive. Hence, so is $z = \sqrt{x^2 + y^2}$. Therefore, $z \in \mathbb{Q}_{\mathrm{tr}}$ and $x^2 + y^2 = z^2$, as claimed □

Edmund Landau proved in 1919 the following result.

Proposition 1.4 ([6, p. 392, II])**.** *Every totally positive algebraic number a is a sum of finitely many squares of elements of $\mathbb{Q}(a)$.*

We mention that two years after Landau published his result, Carl Ludwig Siegel improved it by proving that every totally positive algebraic number a is a sum of four squares in $\mathbb{Q}(a)$ [13].

2. S–Extensions

In addition to the results described in Section 1, we introduce here the notion of S–extensions and the *maximal Galois S–extension* of a field.

Let S be a set of prime numbers. An algebraic extension M/L of fields is said to be an *S–extension*, if the degree $[M_0 : L]$ of every finite subextension M_0/L of M/L is divisible only by prime numbers that belong to S. In other words, the degree $[M : L]$ considered as a supernatural number [4, Remark 22.8.6] is divisible only by prime numbers that belong to S.

For the rest of this section we fix a field K and an algebraic closure $\tilde{K}$ of K. All of the fields that appear in the rest of this section lie between K and $\tilde{K}$.

Lemma 2.1.

(a) *If M/K is an S–extension and L/K is a subextension, then both M/L and L/K are S–extensions.*
(b) *If L/K and M/L are S–extensions, then so is M/K.*
(c) *If M/K is an S–extension and M' is a K–conjugate of M, then M'/K is an S–extension.*
(d) *If L/K is an S–extension and L'/K is a Galois S–extension, then LL'/K is an S–extension.*
(e) *The compositum of arbitrary family of Galois S–extensions of K is a Galois S–extension of K.*
(f) *The compositum of arbitrary S–extensions need not be an S–extension.*

Proof of (a) and (b). Statement (a) follows from the relation $[M : L] \cdot [L : K] = [M : K]$ which holds for finite as well as for infinite algebraic extensions [4, Remark 8.2.6 (4a)]. The same relation proves (b).

Proof of (c). Use that $[M : K] = [M' : K]$.

Proof of (d). By (a), $L \cap L'/K$, $L/L \cap L'$, and $L'/L \cap L'$ are S–extensions. Also, $\mathrm{Gal}(LL'/L) \cong \mathrm{Gal}(L'/L \cap L)$, so $[LL' : L] = [L' : L \cap L']$, hence LL'/L is an S–extension. Now apply (b) twice to conclude that LL'/K is an S–extension.

Proof of (e). We may assume without loss that the family is finite. Then, we use induction in order to reduce (e) to the case where the family contains two extensions. The latter case follows from (d).

Proof of (f). Consider $S = \{3\}$, let ω be a root of unity of order 3, and let $\sqrt[3]{2}$ be the unique real third root of 2. Then, $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$, $[\mathbb{Q}(\omega\sqrt[3]{2}):\mathbb{Q}] = 3$, but $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$. Thus, $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\omega\sqrt[3]{2})$ are S–extensions of $\mathbb{Q}$ but their compositum is not. □

Next we define $K^{(S)}$ to be the union of all finite Galois S–extensions of K.

Lemma 2.2.

(a) *$K^{(S)}$ is a Galois S–extension of K.*

(b) *Every Galois S–extension of K is contained in $K^{(S)}$.*

(c) *If M is an extension of K in $K^{(S)}$, then $M^{(S)} = K^{(S)}$. In particular, $K^{(S)}$ has no proper Galois S–extensions.*

(d) *If $2 \in S$, then $K^{(S)}$ is pythagorean.*

Proof of (a). Consider elements $x, x' \in K^{(S)}$. By definition, there exist finite Galois S–extensions L and L' of K that contain x and x', respectively. By Lemma 2.1(d), LL'/K is a finite Galois S–extension, so $LL' \subseteq K^{(S)}$. It follows that $x + x'$ and $xx' \in K^{(S)}$ and if $x \neq 0$ also $x^{-1} \in K^{(S)}$. Consequently, $K^{(S)}$ is a field. Moreover, $K^{(S)}$ is a Galois S–extension of K.

Proof of (b). If N/K is a Galois S–extension and $x \in N$, then x is contained in a finite subextension N_0 of N which is Galois over K. By Lemma 2.1(a), N_0/K is an S–extension. Hence, by definition, $x \in K^{(S)}$. Therefore, $N \subseteq K^{(S)}$.

Proof of (c). By Lemma 2.1(a), $K^{(S)}/M$ is a Galois S–extension. Hence, it suffices to prove that if N is a Galois S–extension of M, then $N \subseteq K^{(S)}$.

Indeed, let M' be the compositum of all K–conjugates of M. Then, M'/K is a Galois extension. By (a), $M' \subseteq K^{(S)}$. Moreover, $N' = M'N$ is a Galois extension of M'. By Lemma 2.1(d), N' is an S–extension of M, hence also of M' (Lemma 2.1(a)).

Now let $\hat{N}$ be the compositum of all K–conjugates of N'. Since M'/K is Galois, each of the above conjugates is a Galois extension of M'. Hence, by Lemma 2.1(e), $\hat{N}/M'$ is an S–extension. Therefore, by Lemma 2.1(b), $\hat{N}/K$ is a Galois S–extension, so by (b), $\hat{N} \subseteq K^{(S)}$. It follows that $N \subseteq K^{(S)}$, as claimed.

Proof of (d). Assume $K^{(S)}$ has elements x, y such that $\sqrt{x^2 + y^2} \notin K^{(S)}$. Then, $K^{(S)}(\sqrt{x^2 + y^2})$ is a quadratic extension of $K^{(S)}$, in contrast to (c). It follows from this contradiction that $z = \sqrt{x^2 + y^2} \in K^{(S)}$ and $x^2 + y^2 = z^2$, as desired. □

3. Main Theorem

We fix a set S of prime numbers and recall the main theorem:

Main Theorem. *The field $\mathbb{Q}_{\mathrm{tr},S} = \mathbb{Q}^{(S)} \cap \mathbb{Q}_{\mathrm{tr}}$ lies on the bottom.*

Proof. Assume that $\mathbb{Q}_{\mathrm{tr},S}$ does not lie on the bottom. Then, $\mathbb{Q}_{\mathrm{tr},S}$ is a finite proper extension of a field M_0. Since $\mathbb{Q}_{\mathrm{tr},S}/\mathbb{Q}$ is Galois, so is $\mathbb{Q}_{\mathrm{tr},S}/M_0$. By a lemma of Cauchy, $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tr},S}/M_0)$ has an element σ of prime degree p. Let M be the fixed field of σ in $\mathbb{Q}_{\mathrm{tr},S}$. Then, $\mathbb{Q}_{\mathrm{tr},S}/M$ is a cyclic extension of degree p. By Lemma 2.2(a), $\mathbb{Q}_{\mathrm{tr},S}/\mathbb{Q}$ is an S–extension, hence by Lemma 2.1(a), $p \in S$. We distinguish between two cases.

Case A. $p \neq 2$
By Lemma 1.1, $\mathbb{Q}_{\mathrm{tr},S}$ has a cyclic extension N of degree p. By Lemma 2.2(c), $N \subseteq \mathbb{Q}^{(S)}$. If $N \not\subseteq \mathbb{Q}_{\mathrm{tr}}$, then $N\mathbb{Q}_{\mathrm{tr}}/\mathbb{Q}_{\mathrm{tr}}$ is a Galois extension with Galois group isomorphic to $\mathbb{Z}/p\mathbb{Z}$. As mentioned in the introduction, $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tr}})$ is generated by involutions. Hence, so is $\mathbb{Z}/p\mathbb{Z}$, in contrast to the assumption $p \neq 2$. Thus, $N \subseteq \mathbb{Q}_{\mathrm{tr}}$. Hence, $N = \mathbb{Q}_{\mathrm{tr},S}$, which is a contradiction.

Case B. $p = 2$
In this case $\mathbb{Q}_{\mathrm{tr},S} = M(\sqrt{a})$ for some non-square element a of M. On the other hand, by Lemma 2.2(d), $\mathbb{Q}^{(S)}$ is a pythagorean field. Since $\mathbb{Q}_{\mathrm{tr}}$ is pythagorean (Lemma 1.3), so is the intersection $\mathbb{Q}_{\mathrm{tr},S} = \mathbb{Q}^{(S)} \cap \mathbb{Q}_{\mathrm{tr}}$. By Proposition 1.2, M is also pythagorean. Since $\sqrt{a} \in \mathbb{Q}_{\mathrm{tr}}$, the element a of M is totally positive. By Proposition 1.4, a is a sum of squares in M. Hence, by the preceding paragraph, a is a square in M, in contrast to the defining property of a. This ends the proof of Case B and the proof of the main theorem. □

Corollary 3.1. *The field $\mathbb{Q}^{(S)}$ lies on the bottom if and only if $2 \notin S$.*

Proof. Let R be a real closure of $\mathbb{Q}$ and consider a proper Galois extension N of $\mathbb{Q}$ which is not contained in R. Then, N does not lie on the bottom. Indeed, $\mathrm{Gal}(N/N \cap R) \cong \mathrm{Gal}(\tilde{Q}/R) \cong \mathbb{Z}/2\mathbb{Z}$. In particular, if $2 \in S$, then $\mathbb{Q}(\sqrt{-1}) \subset \mathbb{Q}^{(S)}$, so $\mathbb{Q}^{(S)} \not\subseteq R$. Therefore, $\mathbb{Q}^{(S)}$ does not lie on the bottom.

On the other hand, if $2 \notin S$, then $\mathbb{Q}^{(S)}$ is a quadratic extension of no subfield (Lemma 2.2(a) and Lemma 2.1(a)). Hence, the argument of the preceding paragraph proves that $\mathbb{Q}^{(S)}$ is contained in every real closure of $\mathbb{Q}$. Therefore, $\mathbb{Q}^{(S)} \subseteq \mathbb{Q}_{\mathrm{tr}}$, so $\mathbb{Q}^{(S)} = \mathbb{Q}_{\mathrm{tr},S}$. It follows from the main theorem that $\mathbb{Q}^{(S)}$ lies on the bottom. □

References

[1] L. BARY-SOROKER, "Pseudo Algebraically Closed Extensions", PhD Thesis, Tel Aviv University, 2008.

[2] M. D. FRIED, D. HARAN & H. VÖLKLEIN, "Absolute Galois group of the totally real numbers", *C. R. Acad. Sci. Paris Sér. I Math.* **317** (1993), no. 11, p. 995-999.

[3] ———, "Real Hilbertianity and the field of totally real numbers", in *Arithmetic geometry (Tempe, AZ, 1993)*, Contemp. Math., vol. 174, Amer. Math. Soc., Providence, RI, 1994, p. 1-34.

[4] M. D. FRIED & M. JARDEN, *Field arithmetic*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008, Revised by Jarden, xxiv+792 pages.

[5] M. Jarden, "Intersections of local algebraic extensions of a Hilbertian field", in *Generators and relations in groups and geometries (Lucca, 1990)*, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 333, Kluwer Acad. Publ., Dordrecht, 1991, p. 343-405.

[6] E. Landau, "Über die Zerlegung total positiver Zahlen in Quadrate", *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* **1919** (1919), p. 392-396 (ger).

[7] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002, xvi+914 pages.

[8] O. V. Mel′nikov, "Subgroups and the homology of free products of profinite groups", *Izv. Akad. Nauk SSSR Ser. Mat.* **53** (1989), no. 1, p. 97-120.

[9] L. Moret-Bailly, "Groupes de Picard et problèmes de Skolem. II", *Ann. Sci. École Norm. Sup. (4)* **22** (1989), no. 2, p. 181-194.

[10] F. Pop, "Fields of totally Σ-adic numbers", manuscript, Heidelberg, 1992.

[11] ———, "Embedding problems over large fields", *Ann. of Math. (2)* **144** (1996), no. 1, p. 1-34.

[12] P. Ribenboim, *L'arithmétique des corps*, Hermann, Paris, 1972, 245 pages.

[13] C. Siegel, "Darstellung total positiver Zahlen durch Quadrate", *Math. Z.* **11** (1921), no. 3-4, p. 246-275.

Moshe Jarden
School of Mathematics, Tel Aviv University
Ramat Aviv, Tel Aviv, 6997801
ISRAEL
E-mail: jarden@post.tau.ac.il
URL: http://www.tau.ac.il/~jarden/

Carlos Videla
Mount Royal University
Calgary, Alberta
CANADA
E-mail: cvidela@mtroyal.ca