FIELDS ON THE BOTTOM

*

by

Moshe Jarden**

School of Mathematics, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

e-mail: jarden@post.tau.ac.il

and

Carlos Videla

Mount Royal University

Calgary, Alberta, Canada

e-mail: cvidela@mtroyal.ca,

MR Classification: 12E30

Directory: \Jarden\Diary\Bottom

26 December 2013

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

** Research suppoerted by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation.

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 $\mathbb{F}_p$ lie 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 [Lan93, 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 [Lan93, 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, the Henselian closure $\mathbb{Q}_{p,\mathrm{alg}}$ of $\mathbb{Q}$ with respect to a prime number p lies on the bottom (e.g. [Jar91, Cor. 15.3]).

By the "Bottom Theorem" [Jar08, 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 $\tilde{\mathbb{Q}}(\sigma_1, \ldots, \sigma_e)$ lies on the bottom. Here $\tilde{\mathbb{Q}}(\sigma_1, \ldots, \sigma_e)$ is the fixed field of $\sigma_1, \ldots, \sigma_e$ in the algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$. The clause "almost all" means "all but a subset of $\mathrm{Gal}(\mathbb{Q})^e$ of Haar measure 0".

We mention that Lior Bary-Soroker [BaS08] 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 [BSo08, 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 least 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 [Rbn72, 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 $\mathbb{Q}$ whoes images under all embeddings into $\mathbb{C}$ lie in $\mathbb{R}$. It is also the intersection of all real closures of $\mathbb{Q}$ in $\tilde{\mathbb{Q}}$. Since the absolute Galois group of a real closed field has order two, $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tr}})$ is generated by involutions. Florian Pop proved in [Pop92] that $\mathbb{Q}_{\mathrm{tr}}$ 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. Michael Fried, Dan Haran, and Helmut Völklein proved in [FHV94] that $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tr}})$ is a free profinite group (in the sense of Melnikov) generated by involutions. They also proved that the elementary theory of $\mathbb{Q}_{\mathrm{tr}}$ is effectively decidable [FHV94, Thm. 10.1].

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

THEOREM A: *The field $\mathbb{Q}_{\mathrm{tr}}$ of all totally real algebraic numbers lies on the bottom.*

Our second result involves the notion of an "S-closure" of a field, where S is a set of prime numbers. Given a field K, we let $K^{(S)}$ be 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. We prove:

THEOREM B: *Let S be a set of primes.*

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

(b) *If $2 \in S$, then $\mathbb{Q}_{\mathrm{tr}}^{(S)} = \mathbb{Q}^{(S)} \cap \mathbb{Q}_{\mathrm{tr}}$ lies on the bottom.*

The proofs of both theorems use information about Pythagorean fields, an old theorem of George Whaples, and an older theorem of Edmund Landau.

1. The Field $\mathbb{Q}_{\mathrm{tr}}$ QTR input, 9

We present a few facts and results that enter the proof of Theorems A and B.

LEMMA 1.1: *Let F/K be a Galois extension. Suppose that there exists no field $K \subseteq M \subset F$ such that $[F:M]$ is a prime number. Then F is a proper finite extension of no field that contains K.* QTRa input, 13

Proof: Assume that M is an extension of K in F such that $1 < [F:M] < \infty$. Then F/M is a finite proper Galois extension. Let p be a prime divisor of $[F:M]$. By a theorem of Cauchy, $\mathrm{Gal}(F/M)$ has an element σ of degree p. Let M' be the fixed field of σ in F. Then, $[F:M'] = p$, in contrast to the assumption of the Lemma. ∎

LEMMA 1.2: *If F/M is a cyclic extension of an odd prime degree p, then F has a cyclic extension of degree p.* QTRb input, 32

Proof: By a result of Whaples from 1957 [FrJ08, 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 [FrJ08, 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 [Rbn72]. It is a corollary of a theorem of Diller and Dress.

PROPOSITION 1.3: *If a finite extension of a field P_0 is Pythagorean, then P_0 itself is Pythagorean.* QTRd input, 53

Finally we use a result of Landau from 1919 proved in [Lan19, p. 392, II]. To this end recall that an algebraic number a is **totally real** if $\varphi(a) \in \mathbb{R}$ for every embedding $\varphi\colon \mathbb{Q} \to \mathbb{C}$. 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 1.4: *Q_{tr} is a Pythagorean field.* QTRe input, 68

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 ∎

The following result is due to Landau [Lnd19].

PROPOSITION 1.5: *Every totally positive algebraic number a is a sum of finitely many squares of elements of $\mathbb{Q}(a)$.* QTRf input, 82

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 $\mathbb{Q}(a)$ [Sie21].

Proof of Theorem A: Assume that $\mathbb{Q}_{\mathrm{tr}}$ is a cyclic extension of degree p of a field M for some prime number p. By Lemma 1.1, it suffices to prove that this assumption leads to a contradiction.

There are two cases to consider.

CASE A: $p \neq 2$. By Proposition 1.2, $\mathbb{Q}_{\mathrm{tr}}$ has a finite cyclic extension N_0 of degree p. However, since as mentioned in the introduction, $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tr}})$ is generated by involutions, so is $\mathrm{Gal}(N_0/\mathbb{Q}_{\mathrm{tr}})$. This contradicts the assumption that $p \neq 2$.

CASE B: $p = 2$. Then, $\mathbb{Q}_{\mathrm{tr}}/M$ is a quadratic extension. Thus, there exists a non-square element $a \in M$ with $\mathbb{Q}_{\mathrm{tr}} = M(\sqrt{a})$.

Observe that a is totally positive, since otherwise $\sqrt{a}$ would not lie in $\mathbb{Q}_{\mathrm{tr}}$. By Proposition 1.5, a is a sum of squares in $\mathbb{Q}(a)$. Hence, a is a sum of squares in M. By Proposition 1.4, $\mathbb{Q}_{\mathrm{tr}}$ is Pythagorean. Hence, by Proposition 1.3, M is also Pythagorean. Hence, $\sqrt{a} \in M$, in contrast to the preceding paragraph.

Thus, in both cases we achieve a contradiction. ∎

2. The Fields $\mathbb{Q}^{(S)}$ and $\mathbb{Q}_{\mathrm{tr}}^{(S)}$ PROOFB input, 9

Starting with a set S of prime numbers, we prove Theorem B about the fields that appear in the title. We start with a few observations:

(1) For each $p \in S$ the field $\mathbb{Q}^{(S)}$ has no cyclic extension of degree p.

Otherwise, there exist a finite Galois extension K of $\mathbb{Q}$ in $\mathbb{Q}^{(S)}$ and a cyclic extension L of K of degree p such that $\mathbb{Q}^{(S)}L$ is a cyclic extension of degree p and $\mathbb{Q}^{(S)} \cap L = K$. Let $\hat{L}$ be the compositum of all conjugates of L over $\mathbb{Q}$. In particular,

(2) $L \not\subseteq \mathbb{Q}^{(S)}$.

On the other hand, $\hat{L}$ is a Galois extension of $\mathbb{Q}$ and each prime number that divides $[\hat{L} : \mathbb{Q}]$ belongs to S. Hence, $\hat{L} \subseteq \mathbb{Q}^{(S)}$, so $L \subseteq \mathbb{Q}^{(S)}$, in contrast to (2). This concludes the proof of (1).

The second observation is:

(3) If M'/M is a finite extension of fields and $\mathbb{Q} \subseteq M \subseteq M' \subseteq \mathbb{Q}^{(S)}$, then every prime divisor of $[M' : M]$ belongs to S.

Indeed, $\mathbb{Q}$ has a finite Galois extension K in $\mathbb{Q}^{(S)}$ such that $M' \subseteq MK$ [FrJ08, Lemma 1.2.5(a)]. The field K is contained in the compositum of finitely many Galois extensions of $\mathbb{Q}$ with degrees whose prime divisors belong to S. Hence, every prime divisor of $[K : \mathbb{Q}]$ belongs to S, Therefore, every prime divisor of $[M' : M]$ belongs to S.

(4) If M is a Galois extension of $\mathbb{Q}$ in $\mathbb{Q}^{(S)}$ and N is a Galois extension of M such that the degree of each finite Galois subextension N_0/M of N/M is divisible only by prime numbers that belong to S, then $N \subseteq \mathbb{Q}^{(S)}$.

Indeed, it suffices to prove that each N_0 as above is contained in $\mathbb{Q}^{(S)}$. To this end we take a finite Galois extension K of $\mathbb{Q}$ in M and a finite Galois extension L_0 of K such that $M \cap L_0 = K$ and $ML_0 = N_0$ [FrJ08, Lemma 1.2.5(a)]. In particular, every prime divisor of $[L_0 : K] = [N_0 : M]$ belongs to S. Let L be the compositum of all conjugates of L_0 over $\mathbb{Q}$. Then, every prime divisor of $[L : \mathbb{Q}]$ divides $[L_0 : \mathbb{Q}]$, hence belongs to S. Therefore, L is contained in $\mathbb{Q}^{(S)}$. It follows that $L_0 \subseteq \mathbb{Q}^{(S)}$, so $N_0 = ML_0 \subseteq \mathbb{Q}^{(S)}$, as claimed.

Now we break up the rest of the proof of Theorem B into three parts.

Part A: *If $2 \notin S$, then $\mathbb{Q}^{(S)}$ lies on the bottom.* By Lemma 1.1, it suffices to prove that F is a cyclic extension of no subfield M such that $p = [\mathbb{Q}^{(S)} : M]$ is a prime number. Assume that there exists such an M. By (3), $p \in S$, hence by our assumption $p \neq 2$. By Lemma 1.2, $\mathbb{Q}^{(S)}$ has a cyclic extension of degree p. But this contradicts (1).

Part B: *If $2 \in S$, then $\mathbb{Q}^{(S)}$ does not lie on the bottom.* Indeed, in this case $\sqrt{-1} \in \mathbb{Q}^{(S)}$. Hence, after embedding $\tilde{\mathbb{Q}}$ into $\mathbb{C}$, we find that $\mathbb{Q}^{(S)} \not\subseteq \mathbb{R}$, Therefore, $\mathbb{Q}^{(S)}$ is a quadratic extension of $\mathbb{Q}^{(S)} \cap \mathbb{R}$. This proves our claim.

The combination of Parts A and B proves Theorem B(a).

Part C: *In each case $\mathbb{Q}_{\mathrm{tr}}^{(S)}$ lies on the bottom.* As before, we have to derive a contradiction from the assumption that $\mathbb{Q}_{\mathrm{tr}}^{(S)}$ is a cyclic extension of some prime degree p of a field M. By (3), $p \in S$. Again, we have to consider two cases.

Case C1: $p \neq 2$. By Lemma 1.2, $\mathbb{Q}_{\mathrm{tr}}^{(S)}$ has a cyclic extension N of degree p. By (4), $N \subseteq \mathbb{Q}^{(S)}$. Since $\mathbb{Z}/p\mathbb{Z}$ is not generated by involutions, $N \subseteq \mathbb{Q}_{\mathrm{tr}}$. Hence, $N = \mathbb{Q}_{\mathrm{tr}}^{(S)}$, which is a contradiction.

Case C2: $p = 2$. In this case $\mathbb{Q}_{\mathrm{tr}}^{(S)} = M(\sqrt{a})$ for some non-square element a of M. In particular,

(5) a is not a square in M.

On the other hand, $\mathbb{Q}^{(S)}$ is in our case a Pythagorean field. Otherwise there exist $x, y \in \mathbb{Q}^{(S)}$ such that $x^2 + y^2$ is not a square in $\mathbb{Q}^{(S)}$. Therefore, $\mathbb{Q}^{(S)}(\sqrt{x^2 + y^2})$ is a quadratic extension of $\mathbb{Q}^{(S)}$, in contrast to (1). Since $\mathbb{Q}_{\mathrm{tr}}$ is Pythagorean (Lemma 1.4) so is the intersection $\mathbb{Q}_{\mathrm{tr}}^{(S)} = \mathbb{Q}^{(S)} \cap \mathbb{Q}_{\mathrm{tr}}$. By Lemma 1.3, M is also Pythagorean.

Since $\sqrt{a} \in \mathbb{Q}_{\mathrm{tr}}$, the element a of M is totally positive. By Lemma 1.5, a is a sum of squares in M. Hence, by the preceding paragraph, a is a square in M. This contradiction to (5) ends the proof of Part C and the proof of Theorem B. ∎

References

[BaS08] L. Bary-Soroker, *Pseudo Algebraic Closed Extensions,* Ph.D Thesis, Tel Aviv University, 2008.

[FHV94] M. D. Fried, D. Haran, H. Völklein, *Real hilbertianity and the field of totally real numbers,* Contemporary Mathematics **174** (1994), 1–34.

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic, Third Edition, revised by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008.

[Jar91] M. Jarden, *Intersection of local algebraic extensions of a Hilbertian field,* in "Generators and Relations in Groups and Geometries" (A. Barlotti et al., eds), NATO ASI Series C **333**, 343–405, Kluwer, Dordrecht, 1991.

[Lnd19] E. Landau, Über die Zerlegung total positiver Zahlen in Quadrate, Nachrichten von der Gesselschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse (1919), 392–396.

[Lan93] S. Lang, *Algebra, Third Edition,* Addison-Wesley, Reading, 1993.

[Pop92] F. Pop, *Fields of totally Σ-adic numbers,* manuscript, Heidelberg, 1992

[Rbn72] P. Ribenboim, *L'Arithmétique des corps,* Hermann, Paris, 1972.

[Sie21] C. Siegel, *Darstellung total positiver Zahlen durch Quadrate,* Mathematische Zeitschrift **11** (1921), 246-275.