On fields of totally $\mathfrak{S}$-adic numbers

— With an appendix by Florian Pop —

Lior Bary-Soroker and Arno Fehm*

Abstract. Given a finite set $\mathfrak{S}$ of places of a number field, we prove that the field of totally $\mathfrak{S}$-adic algebraic numbers is not Hilbertian.

2010 Mathematics Subject Classification. Primary 12E30; Secondary 12E25.
Keywords. totally $\mathfrak{S}$-adic numbers, Hilbertian fields

1. Introduction

The field of totally real algebraic numbers $\mathbb{Q}^{\mathrm{tr}}$, the field of totally p-adic algebraic numbers $\mathbb{Q}^{\mathrm{t}p}$, and, more generally, fields of totally $\mathfrak{S}$-adic algebraic numbers $\mathbb{Q}^{\mathfrak{S}}$, where $\mathfrak{S}$ is a finite set of places of $\mathbb{Q}$, play an important role in number theory and Galois theory, see for example [5, 9, 11, 7]. The objective of this note is to show that none of these fields is Hilbertian (see [3, Chapter 12] for the definition of a Hilbertian field).

Although it is immediate that $\mathbb{Q}^{\mathrm{tr}}$ is not Hilbertian, it is less clear whether the same holds for $\mathbb{Q}^{\mathrm{t}p}$. For example, every finite group that occurs as a Galois group over $\mathbb{Q}^{\mathrm{tr}}$ is generated by involutions (in fact, the converse also holds, see [4]) although over a Hilbertian field all finite abelian groups (for example) occur. In contrast, over $\mathbb{Q}^{\mathrm{t}p}$ every finite group occurs, see [2]. In fact, although (except in the case of $\mathbb{Q}^{\mathrm{tr}}$) it was not clear whether these fields are actually Hilbertian, certain weak forms of Hilbertianity were proven and used, both explicitly and implicitly, for example in [4, 6]. Also, any proper finite extension of any of these fields is actually Hilbertian, see [3, Theorem 13.9.1].

The non-Hilbertianity of $\mathbb{Q}^{\mathrm{t}p}$ was implicitly stated and proven in [1, Examples 5.2] but this result seems to have escaped the notice of the community and was forgotten. We give a short elementary proof (which is closely related to the proof in [1]) of the following more general result.

Theorem 1.1. *For any finite set $\mathfrak{S}$ of real archimedean or ultrametric discrete absolute values on a field K, the maximal extension $K^{\mathfrak{S}}$ of K in which every element of $\mathfrak{S}$ totally splits is not Hilbertian.*

*The authors are indebted to Pierre Dèbes for pointing out to them the result in [1]. They would also like to thank Sebastian Petersen for motivation to return to the subject of this note. This research was supported by the Lion Foundation Konstanz – Tel Aviv and the Alexander von Humboldt Foundation.

Note that $K^{\mathfrak{S}}$ is the intersection of all Henselizations and real closures of K with respect to elements of $\mathfrak{S}$. We would like to stress that $\mathfrak{S}$ does not necessarily consist of *local* primes in the sense of [7].

After this note was written, it turned out that there is an unpublished manuscript of Pop with a different proof of Theorem 1.1 (which is less explicit but works in a more general setting), see the Appendix at the end of this paper.

2. Proof

Let

$$\gamma(Y,T) \quad = \quad (Y^{-1}+T^{-1}Y)^{-1} \quad = \quad \frac{YT}{Y^2+T}$$

and

$$f(X,Z) \quad = \quad X^2+X-Z^2.$$

Lemma 2.1. *If (F,v) is a discrete valued field with uniformizer $t \in F$, then $v(\gamma(y,t)) > 0$ for each $y \in F$.*

Proof. If $v(y)=0$, then $v(t^{-1}y) < 0 = v(y^{-1})$, so $v(y^{-1}+t^{-1}y) < 0$. If $v(y) < 0$, then $v(y^{-1}) > 0$ and $v(t^{-1}y) < 0$, so $v(y^{-1}+t^{-1}y) < 0$. If $v(y) > 0$, then $v(y^{-1}) < 0$ and $v(t^{-1}y) \geq 0$ since t is a uniformizer, so again $v(y^{-1}+t^{-1}y) < 0$. Thus, in each case, $v(\gamma(y,t)) = -v(y^{-1}+t^{-1}y) > 0$. □

Lemma 2.2. *Let F be a field and $t \in F \smallsetminus \{0,-1\}$. If $\mathrm{char}(F)=2$, assume in addition that t is not a square in F. Then $f(X,\gamma(Y,t))$ is irreducible over $F(Y)$.*

Proof. If $\mathrm{char}(F) \neq 2$, then $f(X,\gamma(Y,t))$ is reducible if and only if the discriminant $1+4\gamma(Y,t)^2$ is a square in $F(Y)$. This is the case if and only if $(Y^2+t)^2+4(tY)^2$ is a square. Writing

$$(Y^2+t)^2+4(tY)^2 = (Y^2+aY+b)^2$$

and comparing coefficients we get that $a=0$, $b^2=t^2$, and $a^2+2b=2t(1+2t)$. Hence, $t=0$ or $t=-1$.

If $\mathrm{char}(F)=2$, then $f(X,\gamma(Y,t))$ is irreducible if and only if

$$g(X) := f(X+\gamma(Y,t),\gamma(Y,t)) = X^2+X+\gamma(Y,t)$$

is irreducible. If v denotes the normalized valuation on $F(Y)$ corresponding to the irreducible polynomial $Y^2+t \in F[Y]$, then $v(\gamma(Y,t)) = -1$. This implies that a zero x of $g(X)$ in $F(Y)$ would satisfy $v(x) = -\frac{1}{2}$, so $g(X)$ has no zero in $F(Y)$ and is therefore irreducible. □

Proof of Theorem 1.1. Without loss of generality assume that $\mathfrak{S} \neq \emptyset$ and that the absolute values in $\mathfrak{S}$ are pairwise inequivalent. Let $F = K^{\mathfrak{S}}$.

The weak approximation theorem gives an element $t \in K \smallsetminus \{0, -1\}$ that is a uniformizer for each of the ultrametric absolute values in $\mathfrak{S}$. Clearly, if $\mathfrak{S}$ contains an ultrametric discrete absolute value (in particular if $\mathrm{char}(K) = 2$), then t is not a square in F. Hence, by Lemma 2.2, $f(X, \gamma(Y, t))$ is irreducible over $F(Y)$.

Assume, for the purpose of contradiction, that F is Hilbertian. Then there exists $y \in F$ such that $f(X, \gamma(y, t))$ is defined and irreducible over F.

Let $|\cdot| \in \mathfrak{S}$. If $|\cdot|$ is archimedean (this means we are in the case $\mathrm{char}(K) \neq 2$), let $\leq$ be an ordering corresponding to an extension of $|\cdot|$ to F, and let E be a real closure of $(F, \leq)$. Since $\gamma(y, t)^2 \geq 0$, there exists $x \in E$ such that $f(x, \gamma(y, t)) = 0$ (note that the map $E_{\geq 0} \to E_{\geq 0}$, $\xi \mapsto \xi^2 + \xi$ is surjective). If $|\cdot|$ is ultrametric and v is a discrete valuation corresponding to an extension of $|\cdot|$ to F, let E be a Henselization of (F, v). Since $v(\gamma(y, t)) > 0$ by Lemma 2.1, $f(X, \gamma(y, t)) \in \mathcal{O}_v[X]$ and

$$\overline{f(X, \gamma(y, t))} = X(X + 1)$$

has a simple root, so by Hensel's Lemma there exists $x \in E$ with $f(x, \gamma(y, t)) = 0$.

Thus in each case, $f(X, \gamma(y, t))$ has a root in E, so since it is of degree 2 all of its roots are in E. Since F is the intersection over all such E, all roots of $f(X, \gamma(y, t))$ lie in F, contradicting the irreducibility of $f(X, \gamma(y, t))$.

□

Appendix: **The totally $\mathfrak{S}$-adic is not Hilbertian**

Florian Pop*

Let K be an arbitrary field, and $\mathfrak{S}$ be a **finite** set of orderings and/or non-trivial valuations of K. We denote by $K^{\mathfrak{S}} \,|\, K$ the maximal subextesion of a separable closure $K^{\mathrm{sep}}|K$ of K in which all $v \in \mathfrak{S}$ are totally split. For $v \in \mathfrak{S}$, let $K_v \subset K^{\mathrm{sep}}$ be a <u>fixed</u> real closure/Henselization of K with respect to v in the case v is an ordering, respectively a valuation. Recall that $K_v \subset K^{\mathrm{sep}}$ is unique up to G_K-conjugation, where G_K is the absolute Galois group of K. One has:

1) $K^{\mathfrak{S}} = \cap_{v \in \mathfrak{S}} \cap_{\sigma \in G_K} K_v^{\sigma}$.

In particular, if $K_{v_0} = K^{\mathrm{sep}}$ for some $v_0 \in \mathfrak{S}$, then $K^{\mathfrak{S}}$ does not depend on v_0. Thus without loss of generality, we suppose that $K_v \neq K^{\mathrm{sep}}$ for all $v \in \mathfrak{S}$. Further, for polynomials $r(X) \in K^{\mathfrak{S}}[X]$ and their G_K-conjugates $r^{\sigma}(X) \in K^{\mathfrak{S}}[X]$ one has:

2) *$r(X)$ has all its roots in $K^{\mathfrak{S}}$ iff $r^{\sigma}(X)$ has all its roots in K_v, $v \in \mathfrak{S}$, $\sigma \in G_K$.*

Let $L|K$ be all the finite Galois subextensions of $K^{\mathrm{sep}}|K$. Then $K^{\mathrm{sep}} = \cup_L L$, and since $K_v \subset K^{\mathrm{sep}}$ is a strict inclusion, there exits $L|K$ finite Galois such that L is not contained in K_v. In particular, since the family $(L|K)_L$ is filtered, there exists $L|K$ such that L is not contained in any K_v, $v \in \mathfrak{S}$. Translated into the language

* Variants of 1990/2013. Last supported by the NSF grant DMS-1101397.

of polynomials, we have the following: Let $p(X) \in K[X]$ be a monic polynomial having splitting field $L|K$ and degree $\deg\big(p(X)\big) = [L : K]$. Then $L = k[\alpha]$ for every root α of $p(X)$. Hence the fact that L is not contained in K_v translates into:

3) *There exist non-constant $p(X) \in K[X]$ having no roots in K_v, $v \in \mathfrak{S}$.*

Equivalently, by general decomposition theory for valuations and orderings, it follows that $p(K_v)$ is *bounded away from zero,* see e.g., [10], i.e., there exists a v-neighborhood U_v of $0 \in K_v$ such that $U_v \cap p(K_v)$ is empty. In particular, for every $v \in \mathfrak{S}$ there exists $t_v \in K^\times$ such that $v(t_v) < v\big(p(x)\big)$ for all $x \in K_v$.[1] Taking into account that the non-zero elements $t \in K^\times$ approximate $0 \in K_v$ simultaneously for $v \in \mathfrak{S}$, for every $t \in K^\times$ we get:

4) *If $v(t) < v(t_v)$, $v \in \mathfrak{S}$, then $v(t) < v\big(p(x)\big)$ for all $x \in K_v$, $v \in \mathfrak{S}$.*

We next recall the theorem on the continuity of roots in the following form, see e.g., [10] for details: Let $q(Y) \in K[Y]$ be a polynomial of degree $n > 0$ which has n distinct roots $y_1, \dots, y_n$ in K. For polynomials $q_v(Y) \in K_v[Y]$, we define $v(q_v - q) := \max\{v(a_{vi} - a_i)\}_i$, where $(a_{vi})_i$ and $(a_i)_i$ are the coefficients of $q_v(Y)$, respectively $q(Y)$. Then for every $v \in \mathfrak{S}$ there exists $\delta_v \in K^\times$ such that all polynomials $q_v(Y) \in K_v[Y]$ of degree n satisfy: If $v(q_v - q) < v(\delta_v)$, then the roots $y_{v1}, \dots, y_{vn}$ of $q_v(Y)$ are distinct and lie in K_v.

Finally, via $K^{\mathfrak{S}} \hookrightarrow K_v$, $v \in \mathfrak{S}$, we view polynomials $\tilde{q}(Y) \in K^{\mathfrak{S}}[Y]$ and their conjugates $\tilde{q}^\sigma(Y) \in K^{\mathfrak{S}}[Y]$ as polynomials in $K_v[Y]$. Then for $\tilde{\delta} \in K^\times$ one has:

5) *Suppose that $v(\tilde{\delta}) \le v(\delta_v)$, $v \in \mathfrak{S}$, and $\tilde{q}(Y) \in K^{\mathfrak{S}}[Y]$ satisfy $v(\tilde{q}^\sigma - q) < v(\tilde{\delta})$ for all $v \in \mathfrak{S}$, $\sigma \in G_K$. Then all the roots of $\tilde{q}(Y) \in K^{\mathfrak{S}}[Y]$ lie in $K^{\mathfrak{S}}$.*

Key Lemma. *Let $\delta \in K^\times$ satisfy $v(\delta) \le v(\tilde{\delta})$ if v is a valuation, and $v(2\delta) \le v(\tilde{\delta})$ if v is an ordering. Then $f(X,Y) := p(X)q(Y) - t\delta \in K[X,Y]$ is absolutely irreducible, and for all $x \in K^{\mathfrak{S}}$ the specialization $f_x(Y) := f(x,Y) \in K^{\mathfrak{S}}[Y]$ splits in linear factors in $K^{\mathfrak{S}}[Y]$. In particular, the field $K^{\mathfrak{S}}$ is not Hilbertian.*

Proof. Let $x \in K^{\mathfrak{S}}$ be given. Then $x^\sigma \in K_v$ for all $v \in \mathfrak{S}$, $\sigma \in G_K$, thus $p(x^\sigma) \in p(K_v)$. Hence by the definition of t we have $v(t) < v\big(p(x^\sigma)\big)$, and in particular, $p(x^\sigma) \neq 0$. Further, setting $a := 1/p(x)$ and $u := at$, it follows that $a^\sigma = 1/p(x^\sigma)$ and $u^\sigma = a^\sigma t$ lie in $K^{\mathfrak{S}}$ and $v(u^\sigma) < v(1)$ for all $v \in \mathfrak{S}$, $\sigma \in G_K$. Set $\tilde{q}(Y) := af_x(Y) = q(Y) + u\delta \in K^{\mathfrak{S}}[Y]$. Then the G-conjugates of $\tilde{q}(Y)$ are $\tilde{q}^\sigma(Y) = q(Y) + u^\sigma\delta \in K^{\mathfrak{S}}[Y]$, thus $\tilde{q}^\sigma - q = (u^\sigma - u)\delta$. On the other hand, one has that $v(u^\sigma - u) \le v(u^\sigma) + v(u) < v(1) + v(1) = v(2)$ if v is an absolute value, respectively $v(u^\sigma - u) \le \max\{v(u^\sigma), v(u)\} < v(1)$ if v is a valuation. Thus using the definition of δ, one has that $v(\tilde{q}^\sigma - q) = v(u^\sigma - u)\, v(\delta) < v(\tilde{\delta})$ for all $v \in \mathfrak{S}$, $\sigma \in G_K$. Therefore, by point 5) above it follows that $\tilde{q}(Y)$ has all its roots in $K^{\mathfrak{S}}$ and therefore, so does $f_x(Y)$. To conclude the proof of Key Lemma, notice that $t\delta \neq 0$, and $q(Y)$ is separable. Therefore $f(X,Y)$ is absolutely irreducible, see e.g., [8] for a proof. □

[1] We write $v(ab) = v(a)v(b)$ for valuations, and $v(a) = \max\{a, -a\}$ if v is an ordering.

Remarks.

1) With a virtually identical proof/method, one proves that the intersection of all the *v-topological Henselizations* of K, $v \in \mathfrak{S}$, is not Hilbertian.

2) One can "axiomatize" the above proof and make it work for infinite families of orderings and/or valuations, satisfying some obvious approximation conditions.

References

[1] P. Dèbes and D. Haran, Almost Hilbertian fields. *Acta Arith.* **88** (1999), 269–287.

[2] I. Efrat, Absolute Galois groups of p-adically maximal PpC fields. *Forum Math.* **3** (1991), 437–460.

[3] M. D. Fried and M. Jarden, *Field Arithmetic*. Ergebnisse der Mathematik III **11**. Springer, 2008. 3rd edition, revised by M. Jarden.

[4] M. D. Fried, D. Haran, and H. Völklein, The absolute Galois group of the totally real numbers. *C. R. Math. Acad. Sci. Paris* **317** (1993), 95–99.

[5] M. D. Fried, D. Haran, and H. Völklein, Real Hilbertianity and the field of totally real numbers. In N. Childress and J. W. Jones, editors, *Arithmetic Geometry*, Contemporary Mathematics 174, pages 1–34. American Mathematical Society, 1994.

[6] D. Haran, M. Jarden, and F. Pop, The absolute Galois group of the field of totally S-adic numbers. *Nagoya Math. J.* **194** (2009), 91–147.

[7] D. Haran, M. Jarden, and F. Pop, The absolute Galois group of subfields of the field of totally S-adic numbers. *Funct. Approx. Comment. Math.* **46** (2012), 205–223.

[8] B. Heinemann and A. Prestel, Fields regularly closed with respect to finitely many valuations and orderings. *Can. Math. Soc. Conf. Proc.* **4** (1984), pp. 297–336.

[9] F. Pop, Embedding problems over large fields. *Ann. of Math.* **144** (1996), 1–34.

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

[11] R. Taylor, Galois representations. *Ann. Fac. Sci. Toulouse Math.* **8** (2004), 73–119.

Lior Bary-Soroker, School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel

E-mail: barylior@post.tau.ac.il

Arno Fehm, Fachbereich Mathematik und Statistik, University of Konstanz, 78457 Konstanz, Germany

E-mail: arno.fehm@uni-konstanz.de

Florian Pop, Department of Mathematics, University of Pennsylvania, DRL, 209 S 33rd Street, Philadelphia, PA 19104, USA

E-mail: pop@math.upenn.edu *URL*: http://math.penn.edu/~pop