On fields of totally $\mathcal{S}$-adic numbers
— With an appendix by Florian Pop —

Lior Bary-Soroker and Arno Fehm

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

2010 Mathematics Subject Classification. Primary 12E30; Secondary 12E25.

Keywords. totally $\mathcal{S}$-adic numbers, Hilbertian fields

1. Introduction

The field of totally real algebraic numbers $\mathbb{Q}^{tr}$, the field of totally $p$-adic algebraic numbers $\mathbb{Q}^p$, and, more generally, fields of totally $\mathcal{S}$-adic algebraic numbers $\mathbb{Q}^\mathcal{S}$, where $\mathcal{S}$ 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 $\mathbb{Q}^{tr}$ is not Hilbertian, it is less clear whether the same holds for $\mathbb{Q}^p$. For example, every finite group that occurs as a Galois group over $\mathbb{Q}^{tr}$ 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 $\mathbb{Q}^p$ every finite group occurs, see [2]. In fact, although (except in the case of $\mathbb{Q}^{tr}$) 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 $\mathbb{Q}^p$ 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 $\mathcal{S}$ of real archimedean or ultrametric discrete absolute values on a field $K$, the maximal extension $K^\mathcal{S}$ of $K$ in which every element of $\mathcal{S}$ 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
\[
\gamma(Y, T) = (Y^{-1} + T^{-1}Y)^{-1} = \frac{YT}{Y^2 + T}
\]
and
\[
f(X, Z) = X^2 + X - Z^2.
\]

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 $t \in F \setminus \{0, -1\}$. If $\text{char}(F) = 2$, assume in addition that $t$ is not a square in $F$. Then $f(X, \gamma(Y, t))$ is irreducible over $F(Y)$.

Proof. If $\text{char}(F) \neq 2$, 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 $\text{char}(F) = 2$, 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 $\mathcal{G} \neq \emptyset$ and that the absolute values in $\mathcal{G}$ are pairwise inequivalent. Let $F = K^\mathcal{G}$.

The weak approximation theorem gives an element $t \in K \setminus \{0, -1\}$ that is a uniformizer for each of the ultrametric absolute values in $\mathcal{G}$. Clearly, if $\mathcal{G}$ contains an ultrametric discrete absolute value (in particular if $\text{char}(K) = 2$), 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 $|\cdot| \in \mathcal{G}$. If $|\cdot|$ is archimedean (this means we are in the case $\text{char}(K) \neq 2$), 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

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

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 $f(X, \gamma(y, t))$.

\[\square\]

Appendix: The totally \(\mathcal{G}\)-adic is not Hilbertian

Florian Pop*

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

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

In particular, if $K_{v_0} = K^{\text{sep}}$ for some $v_0 \in \mathcal{G}$, then $K^\mathcal{G}$ does not depend on $v_0$.

Thus without loss of generality, we suppose that $K_v \neq K^{\text{sep}}$ for all $v \in \mathcal{G}$. Further, for polynomials $r(X) \in K^\mathcal{G}[X]$ and their $G_K$-conjugates $r^\sigma(Y) \in K^\mathcal{G}[X]$ one has:

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

Let $L|K$ be all the finite Galois subextensions of $K^{\text{sep}}|K$. Then $K^{\text{sep}} = \cup_L L$, and since $K_v \subset K^{\text{sep}}$ is a strict inclusion, there exists $L|K$ 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 $K_v$, $v \in \mathcal{G}$. 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 \( \deg(p(X)) = [L : K] \). Then \( L = k[\alpha] \) for every root \( \alpha \) of \( p(X) \). Hence the fact that \( L \) is not contained in \( K_\nu \) translates into:

3) There exist non-constant \( p(X) \in K[X] \) having no roots in \( K_\nu, \nu \in \mathcal{S} \).

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

4) If \( v(t) < v(t_\nu), \nu \in \mathcal{S} \), then \( v(t) < v(p(x)) \) for all \( x \in K_\nu, \nu \in \mathcal{S} \).

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 \( y_1, \ldots, y_n \) in \( K \). For polynomials \( q_n(Y) \in K_n[Y] \), we define \( v(q_n - q) := \max\{v(a_{ij} - a_{ij})\}_{i,j} \), where \( (a_{ij}) \) are the coefficients of \( q_n(Y) \), respectively \( q(Y) \). Then for every \( \nu \in \mathcal{S} \) there exists \( \delta_\nu \in K^\times \) such that all polynomials \( q_n(Y) \in K_\nu[Y] \) of degree \( n \) satisfy: If \( v(q_n - q) < v(\delta_\nu) \), then the roots \( y_{\nu 1}, \ldots, y_{\nu n} \) of \( q_\nu(Y) \) are distinct and lie in \( K_\nu \).

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

5) Suppose that \( v(\delta) \leq v(\delta_\nu), \nu \in \mathcal{S}, \tilde{q}(Y) \in K^\nu[Y] \) satisfy \( v(\tilde{q}^\sigma - q) < v(\delta) \) for all \( \nu \in \mathcal{S}, \sigma \in G_K \). Then all the roots of \( \tilde{q}(Y) \in K^\nu[Y] \) lie in \( K^\delta \).

**Key Lemma.** Let \( \delta \in K^\times \) satisfy \( v(\delta) \leq v(\tilde{\delta}) \) if \( v \) is a valuation, and \( v(2\delta) \leq v(\tilde{\delta}) \) 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 \( x \in K^\nu \) the specialization \( f_x(Y) := f(x,Y) \in K^\nu[Y] \) splits in linear factors in \( K^\nu[Y] \). In particular, the field \( K^\nu \) is not Hilbertian.

**Proof.** Let \( x \in K^\nu \) be given. Then \( x^\sigma \in K_\nu \) for all \( \nu \in \mathcal{S}, \sigma \in G_K \), thus \( p(x^\sigma) \in p(K_\nu) \). Hence by the definition of \( t \) we have \( v(t) < v(p(x^\sigma)) \), 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 \( K^\delta \) and \( v(u^\sigma) < v(1) \) for all \( \nu \in \mathcal{S}, \sigma \in G_K \).

Set \( \tilde{q}(Y) := a f_x(Y) = q(Y) + u \delta \in K^\nu[Y] \). Then the \( G \)-conjugates of \( \tilde{q}(Y) \) are \( \tilde{q}^\sigma(Y) = \tilde{q}(Y) + u^\sigma \delta \in K^\nu[Y] \), thus \( \tilde{q}^\sigma - q = (u^\sigma - u) \delta \). On the other hand, one has that \( v(u^\sigma - u) \leq v(u^\sigma) + v(u) < v(1) + v(1) = v(2) \) if \( v \) is an absolute value, respectively \( v(u^\sigma - u) \leq \max\{v(u^\sigma), v(u)\} < v(1) \) if \( v \) is a valuation. Thus using the definition of \( \delta \), one has that \( v(\tilde{q}^\sigma - q) = v(u^\sigma - u) v(\delta) < v(\delta) \) for all \( \nu \in \mathcal{S}, \sigma \in G_K \). Therefore, by point 5) above it follows that \( \tilde{q}(Y) \) has all its roots in \( K^\nu \) 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 \( K \), \( v \in \mathcal{S} \), 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