ISRAEL JOURNAL OF MATHEMATICS 105 (1998), 323–335

VALUES OF RATIONAL FUNCTIONS ON NON-HILBERTIAN FIELDS AND A QUESTION OF WEISSAUER

BY

P. CORVAJA

Dip. Mat. Inf., Università di Udine, 33100 Udine, Italy
e-mail: corvaja@dimi.uniud.it

AND

U. ZANNIER

Ist. Univ. Arch. D.C.A., S. Croce, 191, 30135 Venezia, Italy
e-mail: zannier@iuav.unive.it

ABSTRACT

We answer in the negative a question raised by Fried and Jarden, asking whether the quotient field of a unique factorization domain with infinitely many primes is necessarily hilbertian. This implies a negative answer to a related question of Weissauer. Our constructions are simple and take place inside the field of algebraic numbers. Simultaneously we investigate the relation of hilbertianity of a field K with the structure of the value sets of rational functions on K: we construct a non-hilbertian subfield K of $\bar{\mathbb{Q}}$ such that, given any $f_1, \dots, f_h \in K(x)$, each of degree ≥ 2, the union $\bigcup_{i=1}^{h} f_i(K)$ does not contain K.

Introduction

Let K be a field and $f \in K(x)$ have degree ≥ 2. A general question concerning the arithmetic of K, which seems to be fairly natural, is to establish how large the image $f(K)$ (a subset of $K \cup \{\infty\}$) can be with respect to the whole K; e.g. when can we have $f(K) \supset K$? Plainly this cannot happen when K is, say, hilbertian*: in that case no finite union of sets $f(K)$ as above is sufficient to cover K.

* See e.g. [FrJ], [L1], [L2], [Sch], [Se1], or [Se2] for the classical theory of hilbertian fields.

Received June 9, 1996 and in revised form November 11, 1996

Though hilbertianity may seem too restrictive in this context (and Theorem 2 below will show that in a sense it is!), we remark that value sets of rational functions have played somewhat a special role in the theory of hilbertian fields. For instance, it follows easily from Siegel's theorem on integral points on curves, that an infinite set S of natural numbers is a *universal Hilbert subset of* $\mathbb{Q}$ if and only if $S \cap f(\mathbb{Q})$ is finite for every $f \in \mathbb{Q}(x)$ of degree > 1 [DZ]*. Value sets of rational functions on hilbertian fields are considered, from different points of view, also in [Fr1, 2,3].

Actually, value sets of rational functions appear in the very definition of hilbertian fields, as given in [Se1], Remark 5 to Definition at p. 129 or in [Se2], Ch. 3, remark following Def. 3.1.3 and Exercise 1. We may rephrase those definitions as follows: *a field K is hilbertian if it is not contained in a finite union of sets of the form $f(C(K))$, where $C(K)$ is the set of K-rational points of a curve C defined over K and $f: C \to \mathbb{P}^1$ is a rational map of degree ≥ 2.*

Both in view of the mentioned *special role* of value sets of functions in $K(x)$ and in view of the fact that curves of high genus tend to have few rational points, it makes sense to ask if we can replace C with $\mathbb{P}^1$ in this definition. Namely, can we test hilbertianity using only the value sets on K of rational functions $f \in K(x)$, of degree ≥ 2? In Theorem 1 below we shall show that this is not the case, producing a certain field of algebraic numbers as a counterexample.

A condition on K which turns out to be relevant in the context of value sets was introduced by Weissauer; the condition, which we shall denote by (W) in the sequel, requires that

(W) *K is equipped with an infinite set S of inequivalent discrete valuations such that, for each $a \in K^*$, the set $\{v \in S: v(a) \neq 0\}$ is finite.*

In Theorem 6 below we show very simply that, if (W) is satisfied, then K is not contained in any finite union of sets $f(K)$, where $f \in K(x)$ has degree ≥ 2 *and* satisfies a certain additional condition (always verified by polynomials).

Actually, Weissauer asked whether (W) implies hilbertianity [FrJ, Problem 14.20, p. 180 and p. 443]. Weissauer himself proved in his thesis that the implication is true provided (W) is supplemented with a product formula (see e.g. [Ws] or [FrJ, Ch. 14]). (Below we work mainly inside $\overline{\mathbb{Q}}$, where Weissauer's deep theorem has little influence, since the only product formulas are the classical ones

* If S is only assumed to consist of rational numbers this is no longer true, as shown in [Fr1], Prop. 3.4.

which arise in number fields).

With Theorem 1 below we give a negative answer to Weissauer's problem. In fact, we answer in the negative to the following question raised by Fried and Jarden ([FrJ, Problem 14.21, p. 180 and p. 443]*), analogous to Weissauer's, but with more restrictive assumptions: *let K be the quotient field of a unique factorization domain R with infinitely many primes. Is K necessarily hilbertian?* (Plainly a negative answer to this question implies the same answer for Weissauer's one.) The question by Fried and Jarden was motivated by an analogous problem raised implicitly by Lang, asking about the hilbertianity of R in place of K (see [L1, p. 142], [L2, p. 226]). Lang's question was answered negatively by Harbater [Har].

Finally, in Remark 7 we sketch two constructions which show that the assertion of Theorem 6 cannot hold unconditionally, namely Weissauer's (or Lang's) assumptions do not even imply that non-invertible rational functions are not surjective. The first construction takes place over the algebraic closure of $\mathbb{Q}(z)$ and works with a rational function of exact degree 2. In the second construction, we give an analogous example inside $\overline{\mathbb{Q}}$ with a rational function of degree 3. Of course such examples provide alternative proofs for Theorem 1.

Summing up we state our main results as follows.

THEOREM 1: *There exists a unique factorization domain $R \subset \bar{\mathbb{Q}}$ with quotient field K, satisfying the following properties.*

(i) *There exists an absolutely irreducible polynomial $h \in \mathbb{Q}[t,x]$ such that $h(t_0,x)$ is reducible in $K[x]$ for every $t_0 \in K$, so K is not hilbertian.*

(ii) *R has infinitely many prime ideals.*

(iii) *Given any rational functions $f_1 \ldots, f_h \in K(x)$, there exist infinitely many $t_0 \in K$ such that, writing $f_i(x) = r_i(x)/s_i(x)$ with coprime $r_i, s_i \in K[x]$, all the polynomials $r_i(x) - t_0 s_i(x)$, $i = 1, \ldots, h$, are irreducible in $K[x]$.*

In particular, if each f_i has degree ≥ 2, $K \not\subset \bigcup_{i=1}^{h} f_i(K)$.

Note that in part (iii) we could assume $f_i \in \bar{\mathbb{Q}}(x)$ as well. In fact, if $f \in \bar{\mathbb{Q}}(x) \setminus K(x)$, the set $f(K) \cap K$ is finite.

The field K and the polynomial h will be constructed explicitly. It will turn out that K is normal over $\mathbb{Q}$ (see Lemma 2), a condition which seems relevant in this context, as pointed out in the final considerations of the present paper.

* The question has been rephrased in [Fr1, p. 349].

Actually the principles of the proof furnish several different constructions. We have chosen to work with the polynomial $h(t,x) = x^2 - t^6 + 2$.

Proofs: To construct K, define inductively fields $K_n \subset \overline{\mathbf{Q}}$, $n = 0, 1, 2, \ldots$ as follows: set $K_0 = \mathbb{Q}$ and, having defined K_n, let K_{n+1} be the field obtained by adjoining to K_n all the algebraic numbers $\sqrt{a^6 - 2}$, for $a \in K_n$. Define $K := \bigcup_{n=0}^{\infty} K_n$. K is plainly a field, since $K_n \subset K_{n+1}$ for all n.

Let $h(t,x) := x^2 - t^6 + 2$. By construction, for each $t_0 \in K_n$, the roots of $h(t_0, x) = 0$ lie in K_{n+1}. So, for all $t_0 \in K$, $h(t_0, x)$ is reducible in $K[x]$. This proves assertion (i) of Theorem 1.

We continue by proving a simple but crucial lemma about K. For a field $L \subset \overline{Q}$, we denote by $\hat{L}$ its normal closure over $\mathbb{Q}$.

LEMMA 2: *K_n is normal over $\mathbb{Q}$ for each n.*

Proof: We have to show, for every $\mathbb{Q}$ embedding σ: $K_n \to \overline{\mathbb{Q}}$, that $\sigma(K_n) \subset K_{n+1}$. We argue by induction on n, the assertion being evident for $n = 0$. Assuming $\sigma(K_{n-1}) \subset K_n$, let $a \in K_{n-1}$; then $\sigma(a) \in K_{n-1}$. Therefore $\sigma(\sqrt{a^6 - 2}) = \sqrt{\sigma(a)^6 - 2} \in K_n$. By the definition of K_n we have $\sigma(K_n) \subset K_n$. ∎

Consider now the field $F := \mathbb{Q}(\theta, \sqrt[3]{2})$, where θ is a primitive cubic root of unity. F is normal over $\mathbb{Q}$ with group G, say, of order 6, with an automorphism σ of order 3 fixing θ and such that $\sigma(\sqrt[3]{2}) = \theta\sqrt[3]{2}$. The conjugacy class of σ in G, denoted $[\sigma]$, consists of σ and σ^2. We denote by $\mathcal{P}$ the set of prime numbers $p > 3$ such that the Artin class of p in F is precisely $[\sigma]$. Such primes split in the fixed field of σ, which is $\mathbb{Q}(\theta)$, but do not split completely in F. In other words, $p \in \mathcal{P}$ if and only if $p \equiv 1 \bmod 3$ and 2 is not a cubic residue modulo p. By the theorem of Cebotarev such primes constitute an infinite set with Dirichlet density equal to $1/3$.

LEMMA 3: *Let $p \in \mathcal{P}$. Then p does not ramify in any number field $L \subset K$.*

Proof: We may assume that $L \subset K_n$ for some n and argue by induction on n, the claim being trivial for $n = 0$. Let $n \geq 1$ and assume the assertion true up to $n-1$. We may assume that $L \subset L'$, where $L' = \mathbb{Q}(a_1, \ldots, a_r, \sqrt{a_1^6 - 2}, \ldots \sqrt{a_r^6 - 2})$, where $a_1, \ldots, a_r \in K_{n-1}$. Plainly it suffices to prove that p does not ramify in L'. By induction we may assume that p does not ramify in $L_* := \mathbb{Q}(a_1, \ldots, a_r)$, which is a subfield of K_{n-1}. If p ramifies in L', then it must ramify in a field $L_*(\sqrt{a_s^6 - 2})$, for some s, $1 \leq s \leq r$. Let π be a prime ideal of L_* lying above

p. We show that π does not ramify in $L_*(\sqrt{a_s^6-2})$. Assume first that a_s has negative order $-m<0$ at π. Then $p^m a_r$ has order 0 at π, since p does not ramify in L_*. We have $L_*(\sqrt{a_s^6-2}) = L_*(\sqrt{(p^m a_s)^6 - 2p^{6m}})$. Since $(p^m a_s)^6 - 2p^{6m}$ has order 0 at π, we see that π does not ramify in $L_*(\sqrt{(p^m a_s)^6 - 2p^{6m}})$, by a well known criterion, namely *let L be a number field and π be a prime ideal of L not lying above 2. If π ramifies in $L(\sqrt{\alpha})$, where α is an integer in L, then $\alpha \in \pi$* [CF, p. 91, Lemma 5]. If a_s is π-integral, then p can ramify in $L_*(\sqrt{a_s^6-2})$ only if $a_s^6 - 2 \in \pi$, by the same criterion. If this were the case, then in particular 2 would be a cube in the residue field of π. Let $\hat{L}_*$ be the normal closure of L_* over $\mathbb{Q}$. Then, by Lemma 2, $\hat{L}_*$ is contained in K_{n-1}, so its degree over $\mathbb{Q}$ is a power of 2 (because $\mathrm{Gal}(K/\mathbb{Q})$ is a pro-2 group). Let $\hat{\pi}$ be a prime ideal of $\hat{L}_*$ lying above π. Then 2 would be a cube also in the residue field $\mathbb{F}$ of $\hat{\pi}$. However $[\mathbb{F}\colon \mathbb{F}_p]$ divides $[\hat{L}_*\colon \mathbb{Q}]$, so $[\mathbb{F}\colon \mathbb{F}_p]$ is a power of 2. But then 2 would be a cube already in $\mathbb{F}_p$, contrary to assumptions. This concludes the proof. ∎

The last step of the proof of (ii) of Theorem 1 is the following

LEMMA 4: *Let K be a field equipped with a set S of inequivalent discrete valuations satisfying (W). Assume that for each $v \in S$ there exists $p_v \in K$ such that $v(p_v) = 1$ and $v'(p_v) = 0$ if $v' \neq v$. Then*

$$R := \{x \in K\colon v(x) \geq 0 \quad \forall v \in S\}$$

is a unique factorization domain whose set of primes (up to units) is $\{p_v\colon v \in S\}$.

Proof: Let $x \in R$. Then $v_p(x) > 0$ for finitely many $p \in S$. Let $p_1, \ldots, p_r$ be such primes and set $h_i := v_{p_i}(x)$. Then, plainly, we may write $x = \mu \prod_{i=1}^r p_i^{h_i}$, where $v_p(\mu) = 0$ for all $p \in S$, so μ is a unit of R. It remains to show that, for $p \in S$, p generates a prime ideal in R. For this, let $xy = pz$, with $x, y, z \in R$. We have $v_p(xy) \geq 1$ and we may assume by symmetry that $v_p(x) > 0$. Then $v_p(x) \geq 1$, as remarked above, so $x/p \in R$, concluding the proof. ∎

Proof of (ii) of Theorem 1: For each prime $p \in \mathcal{P}$ pick just one extension to K of the p-adic valuation on $\mathbb{Q}$. Denote by v_p this extension. Since p does not ramify in any number field contained in K, the value group of each v_p is $\mathbb{Z}$ and, for p, q distinct primes in $\mathcal{P}$ we have $v_p(p) = 1$, $v_p(q) = 0$. Define

$$R := \{x \in K\colon v_p(x) \geq 0 \quad \forall p \in \mathcal{P}\}.$$

By Lemma 4 the ring R is a unique factorization domain whose primes are the prime numbers in $\mathcal{P}$, and their associates. Plainly, its quotient field is K, which is not hilbertian, as we have already remarked. ∎

To prove (iii) of Theorem 1 we shall first deal with quadratic functions in the following lemma, which holds for all subfields of $\overline{\mathbb{Q}}$ satisfying Weissauer's condition (W), defined in the Introduction. Since these assumptions hold for the previously constructed field K, we denote by K even the more general field.

To state the result we first give the following

Definition: An **arithmetic progression** in a field K is a set of the form $\{x \in K: v_i(x - x_i) \geq a_i,\ i = 1, \dots r\}$, where $x_1, \dots, x_r$ are elements in K, $a_1, \dots, a_r$ are positive integers, and $v_1, \dots, v_r$ are inequivalent discrete valuations of K.

By the approximation theorem of Artin–Whaples [La2, Thm. 1.2, p. 4], such sets are always infinite.

LEMMA 5: *Let K be any subfield of $\overline{\mathbb{Q}}$ satisfying condition (W). Let $q_1, \dots, q_r \in K[t]$ be each of degree 1 or 2, each without multiple roots. Then there exists an arithmetic progression A in K such that, for each $m \in A$, none of the numbers $\sqrt{q_j(m)}$ belongs to K.*

Proof: Let $L \subset K$ be a number field containing all the coefficients of the q_i's. We select inequivalent discrete valuations $v_1, \dots, v_r$ of K with the property that they are trivial on all the coefficients of the q_i's and on their discriminants (assumed to be nonzero). Their existence is clear by the finiteness condition in (W). Also, by the same condition only a finite number of valuations may lie over a given prime, so we may assume that the characteristic of the residue field of any of the v_i is > 3.

It suffices to show that, for each i, $1 \leq i \leq r$ there exists $x_i \in K$ such that $q_i(x)$ is not a square in K for all $x \in K$ satisfying $v_i(x - x_i) \geq 2$.

Fix i, $1 \leq i \leq r$ and assume the contrary, that is: *for all $\eta \in K$ there exists $x \in K$ with $v_i(x - \eta) \geq 2$ such that $q_i(x)$ is a square in K.* We proceed to derive a contradiction. From now on, we omit the subscript i, since we have fixed it.

Let Φ be the residue field of L relative to v. We show that, enlarging L if necessary to a finite extension still contained in K, we may assume that the reduction of q modulo v, denoted $\bar{q} \in \Phi[t]$, has its roots in Φ. Suppose this is not already true for L . By our choice of v, we know that $\deg \bar{q} \leftarrows \deg q \geq 1$ and we

certainly cannot have $\deg \bar{q} = 1$, whence we may assume $\deg \bar{q} = 2$. Also, $\bar{q}$ has no multiple roots, since we are assuming that v is trivial on the discriminant of q. Consider then the plane curve of genus zero over Φ defined by the absolutely irreducible equation $y^2 = \bar{q}(x)$. It is a well known elementary fact that it has $\leq \phi + 1$ points on the affine plane over Φ [FrJ, p. 41, exer. 2], where $\phi := \#\Phi$. Every $a \in \Phi$ such that $\bar{q}(a)$ is a nonzero square in Φ gives rise to two solutions. So the number of such a's is at most $(\phi+1)/2 < \phi$ for $\phi > 3$, as we are assuming. So we may pick $\eta \in L$, $v(\eta) \geq 0$, such that the reduction of $q(\eta)$ is not a square in Φ. By what we have assumed we may find $x \in K$, $v(x - \eta) \geq 2$, such that $q(x) = u^2$ where $u \in K$. Consider the field $L(x, u) \subset K$. Since the reduction of $q(x)$ modulo v equals $\bar{q}(\bar{\eta})$, the reduction is not a square in Φ, so the residue field of $L(x, u)$ modulo v contains a quadratic extension of Φ (i.e. $\Phi(\bar{u})$). Since there exists only one quadratic extension of any given finite field, this extension must contain the roots of $\bar{q}$ as wanted. We can now reach the desired contradiction. Pick $\xi \in K$ which reduces to a root of q, i.e. such that $v(q(\xi)) \geq 1$. If $v(q(\xi)) = 1$ we are done; in fact $v(q(x)) = v(q(\xi)) = 1$ for all x such that $v(x - \xi) \geq 2$, so $q(x)$ cannot be a square in K. If, on the other end, $v(q(\xi)) \geq 0$, let $\pi \in K$ satisfy $v(\pi) = 1$ and consider $q(\xi + \pi) = q(\xi) + \pi q'(\xi) + \pi^2 q''(\xi)/2$. Certainly $v(q(\xi + \pi)) \geq 1$. If equality holds we are done. Otherwise $v(q'(\xi)) \geq 1$. But then the reduction of q modulo v would have a double root, contrary to assumptions. ∎

Before going on we recall some facts from Hilbert's Irreducibility Theorem and specializations of Galois groups. Let L be a number field and $f \in L[t, x]$ a polynomial irreducible over L. Let ξ be a primitive element for the splitting field Σ of f over $L(t)$ and let $g(t, \xi) = 0$ be its minimal equation over $L(t)$. Each field Γ intermediate between $L(t)$ and Σ can be written as $\Gamma = L(t, \gamma)$, for a suitable $\gamma \in L(t)[\xi]$.

Consider now any $t_0 \in L$ such that $g(t_0, X)$ is defined and irreducible over L and pick a root x_0 of $g(t_0, X) = 0$. Each conjugate $\sigma(\xi)$ of ξ over $L(t)$ is expressed as an element $\sigma(\xi) \in L(t)[\xi]$, since Σ is Galois over $L(t)$. If t_0 does not belong to the finite set of elements such that some such $\sigma(\xi)$ is (possibly) not defined at t_0, then we see that the Galois group $\mathrm{Gal}(\Sigma/L(t))$ is isomorphic to $\mathrm{Gal}(L(x_0)/L)$ under the correspondence $\sigma \to \sigma^*$ such that $\sigma^*(x_0) := (\sigma(\xi))(t_0, x_0) = \rho(t_0, x_0)$. In this correspondence the lattice of the intermediate fields (which are the fixed fields of the possible subgroups) is preserved. If we exclude the finite set of t_0

such that some γ as above is not defined, we have that the intermediate fields between L and $L(x_0)$ are of the type $L(\gamma(t_0, x_0))$. (See [Se1, 9.2, p. 122] for a somewhat different formulation of these facts.)

Now, we know from Hilbert's Irreducibility Theorem that, given any polynomials $f_1, \dots, f_h$ as above, we may find a t_0 which works for them all. We may even pick t_0 in any given arithmetic progression in L, and even in $\mathbb{Z}$. The more precise result for $\mathbb{Z}$ is proved in [L2, chap. 9, §2] or in [Sch], first for $L = \mathbb{Q}$, then for general L by means of reduction steps. Another approach comes from ideas which go back to M.Eichler and S. D. Cohen; see e.g. [FrJ, Ch. 12] or [Se1, Ch. 13, Corollary to Thm. 5, p. 180]. See also Ex. 4, 5 in [FrJ, pp. 159–160].

End of the proof of Theorem 1: We retain the above notation concerning K, K_n etc.

Part (i) has already been proved. Put $u_i(t, x) = r_i(x) - ts_i(x)$ and let L be a number field such that $L \subset K$ and $u_i \in L[t, x]$ for $i = 1, \dots, h$. Let Σ_i be a splitting field of u_i over $L(t)$ and let $S_i \subset \Sigma_i$ be the set of all roots of the equation in x, $u_i(t, x) = 0$.

Consider now the set of all fields Ω such that $L(t) \subset \Omega \subset L(t, \alpha)$, for some $\alpha \in \bigcup_{i=1}^{h} S_i$ and such that Ω has degree 2 over $L(t)$. We may write each such Ω in the form $L(t, y)$, where $y^2 = q(t)$, for some $q \in L[t]$, without square factors of positive degree. Now, all the polynomials u_i are absolutely irreducible, so Ω is not a constant field extension, namely $\deg q > 0$. Also, the fields $L(t, \alpha) = L(\alpha)$ are of genus zero over L, so also Ω/L must be of genus zero. It is well known [A, p. 302] that this implies $\deg q \leq 2$ (here we could have equivalently used Luroth's theorem for the field $L(\alpha)$ - see [Sch, Thm. 2, p. 6]). Let $q_1(t), \dots, q_r(t)$ be all the polynomials obtained in this way. To them we may plainly apply Lemma 5, obtaining an arithmetic progression A in K such that, for all $m \in A$, none of the values $q_i(m)$ can be a square in K.

Let $g_i(t, x)$ be the minimal polynomial of a primitive element ξ_i for Σ_i over $L(t)$. As in the discussion above, we may find an infinite set $A' \subset A$ such that for all $m \in A'$ each $g_i(m, x)$ is irreducible over L and the specialisation $t \mapsto m$ extends to preserve the structure of Galois groups and the lattices of intermediate fields, as described previously, after the proof of Lemma 5.

We contend that for $m \in A'$ each $u_i(m, x)$ is irreducible over K.

Assume the contrary and, omitting the subscript in the discussion which follows, let $u(t, x)$ be some of the u_i's, such that $u(m, x)$ is reducible over K,

for a certain $m \in A'$.

Recall now the following fact from simple Galois theory: *Let M, N be subfields of a same field, both of finite degree over $M \cap N$. Suppose that $N/M \cap N$ is Galois. Then $[MN\colon N] = [M\colon M \cap N]$.*

Let α_m be a root of $u(m,x) = 0$. Apply this statement taking $M := L(\alpha_m)$ and N as a number field normal over $\mathbb{Q}$ such that $L \subset N \subset K$ and such that $u(m,t)$ is reducible over N. That N exists follows from our assumption and from Lemma 2. Then $[MN\colon N] < [M\colon L] = \deg_x u$ (since $u(m,x)$ is by construction irreducible over L). So $J := M \cap N$ contains L strictly. Since $\mathrm{Gal}(K/\mathbb{Q})$ is a pro-2 group, the Galois group $\mathcal{G}$ of N over L is a 2-group and $\mathcal{H} := \mathrm{Gal}(N/J)$ is a subgroup. By well known properties of finite p-groups we may find a group $\mathcal{H}'$, intermediate between $\mathcal{H}$ and $\mathcal{G}$, such that $[\mathcal{G}\colon \mathcal{H}'] = 2$. This subgroup corresponds to a field $J' \subset J \subset K \cap M$, with $[J'\colon L] = 2$. By the above discussion and the choice of A', the field J' is obtained from a subfield Ω of $L(t,\alpha)$, where $u(t,\alpha) = 0$, by extending the specialization $t \mapsto m$, as described above. Write as above Ω as $L(t,y)$, where $y^2 = Q(t)$, $Q \in L[t]$, $1 \leq \deg Q \leq 2$. Then $J' = L(\sqrt{Q(m)})$. On the other hand, by our definition of A and the fact that $A' \subset A$, $Q(m)$ cannot be a square in K, a contradiction which proves our contention and Theorem 1. ∎

We observe that the proof could be simplified if one wanted just the final conclusion of Theorem 1.

As announced in the introduction, we observe that Weissauer's condition implies rather severe restrictions on value sets of rational functions. More precisely, we prove the following

THEOREM 6: *Let K be a field satisfying (W) and let $f_1, \ldots, f_h \in K(x)$ be rational functions such that for every $i \in \{1, \ldots, h\}$ there exists a rational point $c_i \in \mathbb{P}^1(K)$ such that all the fibers of the cover $f_i\colon \mathbb{P}^1 \to \mathbb{P}^1$ at c_i are ramified. Then K is not contained in $\bigcup_{i=1}^h f_i(K)$.*

Observe that the assumption on the f_i's is satisfied by non-linear polynomials (with $c_i = \infty$).

Proof: We first notice that we can always reduce to the case when c_i is different from ∞ for every $i \in \{1, \ldots, h\}$, by composing all the functions f_i with an automorphism sending $\{c_1, \ldots, c_h\} \to \mathbb{P}^1(K) \setminus \{\infty\}$. Moreover, we can also suppose that ∞ is not a pole for any f_i. Write $f_i(x) - c_i = r_i(x)/s_i(x)$, where $r_i, s_i \in K[x]$

are coprime polynomials. By assumption we have $r_i(x) = \prod_j u_{i,j}(x)^{a_{i,j}}$, where $u_{i,j} \in K[x]$ are distinct irreducible polynomials and $a_{i,j} > 1$ for all i, j. Moreover $\deg r_i = \deg s_i$ or $\deg s_i - \deg r_i > 1$.

Let $v_1, \dots, v_h$ be inequivalent discrete valuations of K trivial on the c_i's on every nonzero coefficient of any r_i or s_i. We shall require that the v_i are trivial also on certain other quantities, dependent only on the f_i's, which, for simplicity, we introduce later. The existence of such v_i's is guaranteed by (W). Let p be a prime number larger than $\max\{a_{i,j}, \deg s_i - \deg r_i\}$ and let $t_0 \in K$ satisfy $v_i(t_0 - c_i) = p$ for $i = 1, \dots, h$. The existence of t_0 is guaranteed by the approximation theorem.

We contend that, for all i, $t_0 \notin f_i(K)$. Assume the contrary, and put $t_0 = f_i(x_0)$. To ease notation, omit the subscript i in what follows. First assume $v(x_0) < 0$. Then, since the coefficients of both $r(x)$ and $s(x)$ have order 0 at v, we easily see that $v(r(x_0)) = (\deg r)v(x_0)$, $v(s(x_0)) = (\deg s)v(x_0)$, so $p = v(f(x_0) - c) = (\deg r - \deg s)v(x_0)$. Then $\deg s - \deg r > 0$, so by hypothesis it is ≥ 2. The contradiction follows from the fact that p is prime and $p > \deg s - \deg r$. Suppose now $v(x_0) \geq 0$. Then $v(r(x_0)) \geq 0$, so we must have $v(u_j(x_0)) = q > 0$, say, for some j. Then $v(u_j(x_0)^{a_j}) = a_j q$ cannot be equal to p, so we must have either $v(s(x_0)) > 0$ or $v(u_\ell(x_0)) > 0$ for some $\ell \neq j$. Say the first case holds. Since $s(x)$ and $u_j(x)$ are coprime we have a Bezout equation $g(x)s(x) + h(x)u_j(x) = 1$ with $g, h \in K[x]$. We may assume to have chosen v such that all the coefficients of g, h have order 0 at v. Then we have a contradiction. Similarly in the other case. Observe that only finitely many Bezout equations may arise, so $v_1, \dots, v_h$ may in fact be chosen from the beginning to satisfy what is needed. ∎

Notice that our proof shows that the complementary set $\mathbb{P}^1(K) \setminus (\bigcup_i f_i(K))$ contains the image of an arithmetic progression under a K-automorphism of $\mathbb{P}^1$.

Remark 7: We sketch the constructions announced in the introduction. They show that some condition on the f_i beyond $\deg f_i > 1$ is needed in order to obtain the conclusion of the previous remark. Both of them answer negatively the question of Fried and Jarden. The principles are similar to those used in Theorem 1.

First example: Similarly to the construction used for Theorem 1, define fields K_n as follows: put $K_0 = \mathbb{Q}(z)$, where z is transcendental over $\mathbb{Q}$ and, having defined K_n, let K_{n+1} be obtained by adjoining to K_n all the elements $\sqrt{t^2 + 1}$,

for t running through K_n. Define K as the union of all K_n.

Let v be a valuation of $K_0/\mathbb{Q}$, corresponding to an irreducible polynomial $f(z) \in \mathbb{Q}[z]$ and extend v to K in some way. We contend that if f has at least one real root, v does not ramify in K. In fact, let n be the minimal integer such that v ramifies in K_n. Then, as in the proof of Lemma 3, some element $t_0^2 + 1$, $t_0 \in K_{n-1}$, would have positive order at v. However, since f has a real root, it is easy to see that the residue field of any extension of v to some field $L \subset K$, finite over K_0, may be embedded in $\mathbb{R}$ (it is obtained by adjoining successively square roots of positive elements), so -1 cannot be equal to the square of the reduction of t_0.

Since there are infinitely many such valuations, K satisfies (W) (and even the assumptions of the question of Fried and Jarden). On the other hand, by construction we plainly have $f(K) \supset K$ with $f(x) = (x-1)/x$, because each equation $x^2 - ax - 1 = 0$ with $a \in K$ is solvable in K.

Second example: Put $f(x) := (x^3+1)/x$, a rational function of degree 3. Let, for $p > 3$, v_p denote the p-adic valuation on $\mathbb{Q}$. Similarly to previous constructions, we define inductively a tower of fields K_n and extensions of the valuations v_p to K_n with the property that each v_p is unramified in K_n. We put $K_0 = \mathbb{Q}$ and proceed as follows. Assume K_n to be defined with the above properties and let $t_1, t_2, \ldots$ be a listing of its elements. Define $K_{n,\ell}$ as follows. Put $K_{n,0} = K_n$ and, having defined $K_{n,\ell-1}$, consider the polynomial $x^3 + 1 - t_\ell x$. In case this is reducible over $K_{n,\ell-1}$ put $K_{n,\ell} = K_{n,\ell-1}$. Otherwise, let x_ℓ be any root and define $K_{n,\ell} := K_{n,\ell-1}(x_\ell)$. Finally, define $K_{n+1} := \bigcup_{\ell=0}^{\infty} K_{n,\ell}$. We show that we can extend the valuations v_p to K_{n+1} such that none of them ramifies. Arguing with a single v_p and a field $K_{n,\ell}$ each time, it is plainly sufficient to show the following: *let L be a field with a discrete valuation v such that $v(6) = 0$. Let $t_0 \in L$ and assume $x^3 + 1 - t_0 x$ is irreducible over L. Then, letting x_0 be a root of $x^3 + 1 - t_0 x$, v may be extended to $L(x_0)$ as to be unramifed.*

To prove the contention, let first t_0 be a v-integer. Denote by $\bar{L}$ the residue field of L and by $\hat{L}$ its completion at v. If v were totally ramified in $L(x_0)$ the reduction of $h(x) := x^3 + 1 - t_0 x$ modulo v would have a triple root. This would imply that $v(6) > 0$, against the assumptions. Then the reduction of $h(x)$ either remains irreducible over $\bar{L}$ or has a simple root in $\bar{L}$. By well known facts related to Hensel's lemma, $h(x)$ remains irreducible over $\hat{L}$ or resp. splits into at least two relatively prime factors: in the first case v admits precisely one unramified

extension to $L(x_0)$, in the second one there are at least two extensions, the one corresponding to a factor of degree 1 being unramified.

Secondly, let $v(t_0) = -m$, where m is a positive integer. Let $\pi \in L$ have order 1 at v and put $t^* := \pi^m t_0$, a v-integer in L with nonzero reduction $\bar{t}^*$. Use the substitution $x = \pi^m/u$ in the equation $x^3 + 1 - t_0 x$. After multiplying by u^3 we get a monic irreducible cubic equation over L, with π^m/x_0 as a root, which reduces in $\bar{L}$ to $u^3 - u^2\bar{t}^*$. This has the simple root $\bar{t}^*$ in $\bar{L}$, whence there exists an unramified extension of v to $L(x_0)$.

This completes the verification that the v_p's can be extended to K_{n+1} in the desired way. Defining now K as the union of the K_n we have that K satisfies (W), but the equation $f(x) = t_0$ has a solution in K for all $t_0 \in K$.

Lemma 5 proves that there is no example of a subfield K of $\bar{\mathbb{Q}}$ satisfying (W), and an $f \in K(x)$, of degree 2, such that $f(K) \supset K$. The second construction shows that this is false if we allow degree 3. It seems likely that for a field $K \subset \bar{\mathbb{Q}}$ satisfying (W) and being moreover normal over $\mathbb{Q}$, the above phenomenon cannot any longer occur. In view of the above examples this would be in a sense best possible concerning the influence that condition (W) may have on the structure of value sets of rational functions on fields of algebraic numbers.

References

[A] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon & Breach, London, 1965.

[CF] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, New York, 1990.

[DZ] P. Dèbes and U. Zannier, *Universal Hilbert subsets*, Mathematical Proceedings of the Cambridge Philosophical Society, to appear.

[Fr1] M. Fried, *On the Sprindzuk-Weissauer approach to universal Hilbert subsets*, Israel Journal of Mathematics **51** (1985), 347–363.

[Fr2] M. Fried, *Arithmetical properties of value sets of polynomials*, Acta Arithmetica **15** (1969), 91–115.

[Fr3] M. Fried, *On Hilbert's irreducibility theorem*, Journal of Number Theory **6** (1974), 211–231.

[FrJ] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, 1986.

[Har] D. Harbater, *Galois coverings of the arithmetic line,* in *Number Theory — New York, 1984–85* (D. V. and G.V. Chudnovsky, eds.), Lecture Notes in Mathematics **1240**, Springer-Verlag, Berlin, 1987, pp. 165–195.

[L1] S. Lang, *Diophantine Geometry,* Interscience Publishers, New York, 1962.

[L2] S. Lang, *Fundamentals of Diophantine Geometry,* Springer-Verlag, Berlin, 1983.

[Sch] A. Schinzel, *Selected Topics on Polynomials,* The University of Michigan Press, Ann Arbor, 1983.

[Se1] J. P. Serre, *Lectures on the Mordell–Weil Theorem,* Vieweg, 2nd ed., Braunschweig, 1990.

[Se2] J. P. Serre, *Topics in Galois Theory,* Jones and Bartlett, Boston, 1992.

[Ws] R. Weissauer, *Der Hilbertsche Irreduzibilitätssatz,* Journal für die reine und angewandte Mathematik **334** (1982), 203–220.