Rendiconti del Seminario Matematico della Università di Padova

Paulo Ribenboim

Remarks on existentially closed fields and diophantine equations

Rendiconti del Seminario Matematico della Università di Padova, tome 71 (1984), p. 229-237

<http://www.numdam.org/item?id=RSMUP_1984__71__229_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 71 (1984)

Remarks on Existentially Closed Fields and Diophantine Equations.

PAULO RIBENBOIM (*)

Introduction.

We begin with a simple proposition: an infinite field is always existentially closed in any purely transcendental extension. This leads to the consideration of solutions of diophantine equations in fields $K(t)$. In this respect, we extend a result of Natanson about Catalan's equation, to a much wider class of diophantine equations.

In the last section, we show that a field K, with a non-henselian valuation and algebraically closed residue field $\bar{K}$ cannot be existentially closed in any henselian valued field extension $\tilde{K}$. This leads to the conclusion that (whatever be $\bar{K}$), $\tilde{K}/K$ is not a purely transcendental extension. As corollaries, we obtain anew: $K((X))$ is not a purely transcendental extension of $K(X)$ and the p-adic field $\mathbf{Q}_p$ is not a purely transcendental extension of $\mathbf{Q}$.

1. Let S be a commutative ring with identity, let R be a subring of S. We say (see [1]) that R is *existentially closed* in S when every system of polynomial equations and inequations

$$f_1(X_1, \dots, X_n) = 0, \dots, f_k(X_1, \dots, X_n) = 0\,,$$
$$g_1(X_1, \dots, X_n) \neq 0, \dots, g_l(X_1, \dots, X_n) \neq 0$$
$$(\text{where } n \geqslant 1,\ f_i, g_j \in R[X_1, \dots, X_n])$$

which has a solution in S^n has also a solution in R^n.

(*) Indirizzo dell'A.: Queen's University, Kingston, Ontario, Canada.

It is immediate that is $R \subset S \subset T$ are rings and subrings, if R is existentially closed in S and S is existentially closed in T, then R is existentially closed in T.

It is also easy to see ([1]): Let S be an integral domain, let R be a subring of S, let K be the field of quotients of R and L the field of quotients of S. If R is existentially closed in S then K is existentially closed in L.

The following proposition is practically trivial:

PROPOSITION 1. If K is an infinite field then K is existentially closed in every purely transcendental extension of K.

PROOF. By transfinite induction and transitivity of the property of being existentially closed, it suffices to show that K is existentially closed in the purely transcendental extension $K(t)$. By the above remark, it suffices to show that K is existentially closed in $K[t]$.

Let $n \geqslant 1$, $f_1, \ldots, f_k, g_1, \ldots, g_l \in K[X_1, \ldots, X_n]$, and assume that there exist $u_1(t), \ldots, u_n(t) \in K[t]$ such that

$$P_i(t) = f_i(u_1(t), \ldots, u_n(t)) = 0 \qquad (i = 1, \ldots, k)$$

and

$$Q_j(t) = g_j(u_1(t), \ldots, u_n(t)) \neq 0 \qquad (j = 1, \ldots, l)\,.$$

Since K is infinite, there exists an element $a \in K$ such that $Q_j(a) \neq 0$ (for $j = 1, \ldots, l$). Moreover, since $P_i(t) = 0$ then $P_i(a) = 0$ (for $i = 1, \ldots, k$). Thus, $(u_1(a), \ldots, u_n(a)) \in K^n$ is a solution of the given system of equations and inequations, proving that K is existentially closed in $K[t]$. □

We deduce:

COROLLARY 1. Let K be any infinite field. If $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ has a non-trivial solution $(u_1, \ldots, u_n)$ (with each $u_i \neq 0$) in a purely transcendental extension of K, then it has already a non-trivial solution in K.

PROOF. Let $g(X_1, \ldots, X_n) = X_1 X_2, \ldots, X_n$. We need only to apply the proposition to the system

$$\begin{cases} f(X_1, \ldots, X_n) = 0\,, \\ g(X_1, \ldots, X_n) \neq 0\,. \end{cases} \qquad \square$$

For example, we may take $f(X, Y, Z) = X^n + Y^n - Z^n$. Noting that this polynomial is homogeneous, we deduce that if Fermat's equation with the exponent n has only the trivial solution in $\mathbb{Z}$, then it has only the trivial solution in any purely transcendental extension of $\mathbb{Q}$.

2. In this respect, much more is known concerning Fermat's equation.

In 1879, Liouville ([3]) proved that if $K = \mathbb{C}$ (the field of complex numbers), if $\mathbb{C}(t)|\mathbb{C}$ is a purely transcendental extension, if $n > 2$ and if $f(t), g(t), h(t) \in \mathbb{C}[t]$ satisfy $f(t)^n + g(t)^n = h(t)^n$ and $gcd(f(t), g(t), h(t)) = 1$ then $f(t), g(t), h(t) \in \mathbb{C}$.

This result was generalized by Greenleaf [2], who showed that it holds when K is any field whose characteristic does not divide the exponent n of Fermat's equation.

Concerning Catalan's equation, Natanson proved in [4] the following result:

Proposition 2. Let m, n be integers greater than 2 and not divisible by the characteristic of the field K. If $f, g \in K(t)$ (purely transcendental extension of K) and $f^m - g^n = 1$ then $f, g \in K$.

We use the very same method to extend Natanson's result to a wider class of equations.

Proposition 3. Let m, n be integers greater than 2 and n not divisible by the characteristic of the field K. Let $P(X) \in K[X]$ have degree m and distinct roots. If $f, g \in K(t)$ (purely transcendental extension of K) and $g^n = P(f)$ then $f, g \in K$.

Proof. We may assume without loss of generality that K is algebraically closed. Indeed, assuming the proposition true for such fields, if $\bar{K}$ is the algebraic closure of K, then $f, g \in \bar{K} \cap K(t) = K$.

If $f \in K$ then $g^n = c \in K$; since K is algebraically closed, there exists $d \in K$ such that $c = d^n$, hence $g \in K$, because K contains the n-th roots of 1. Similarly, if $g = c \in K$ and $Q(X) = P(X) - c^n$ then f is a root of $Q(X)$; since K is algebraically closed then $f \in K$.

Let

$$P(X) = a_0 X^m + a_1 X^{m-1} + \ldots + a_m = a_0 \prod_{i=1}^{m} (X - r_i) ,$$

where $a_i, r_i \in K$ $(i = 1, \ldots, m)$, all the r_i are distinct and $a_0 \in K$, $a_0 \neq 0$.

Let $f = f_1/f_0$, $g = g_1/g_0$ with $f_0, f_1, g_0, g_1 \in K[t]$ and

$$gcd(f_0, f_1) = 1 \,, \qquad gcd(g_0, g_1) = 1 \,.$$

Then

$$g_1^m f_0^m = (a_0 f_1^m + a_1 f_1^{m-1} f_0 + \ldots + a_{m-1} f_1 f_0^{m-1} + a_m f_0^m) g_0^n \,.$$

From $gcd(f_0, a_0 f_1^m + a_1 f_1^{m-1} f_0 + \ldots + a_m f_0^m) = 1$ it follows that

$$g_0^n = h f_0^m \,, \qquad \text{with } h \in K[t] \,.$$

From $gcd(g_0, g_1) = 1$ it follows that

$$a_0 f_1^m + a_1 f_1^{m-1} f_0 + \ldots + a_m f_0^m = h' g_1^n \,, \qquad \text{with } h' \in K[t] \,.$$

Hence $hh' = 1$, in particular $h, h' \in K$.

Let $d \in K$ be such that $d^n = h'$. Then

$$(dg_1)^n = a_0 \prod_{i=1}^{m} (f_1 - r_i f_0) \,.$$

Since the roots r_i are all distinct then the polynomials $f_1 - r_i f_0$ are pairwise relatively prime, hence each is a n-th power:

$$f_1 - r_i f_0 = h_i^n \ (i = 1, \ldots, m) \,, \qquad \text{with } h_i \in K[t] \,.$$

Since $m \geqslant 3$ the elements $f_1 - r_1 f_0$, $f_1 - r_2 f_0$, $f_1 - r_2 f_0$, which are in the K-subspace of $K[t]$ generated by f_0, f_1, must be linearly dependent. So there exist $b_i \in K$ $(i = 1, 2, 3)$ not all equal to 0, such that

$$\sum_{i=1}^{3} b_i (f_1 - r_i f_0) = 0 \,.$$

Actually b_1, b_2, b_3 are all not zero, since $gcd(f_0, f_1) = 1$.

Let $c_i \in K$ be such that $c_i^n = b_i$ $(i = 1, 2, 3)$. Then

$$(c_1 h_1)^n + (c_2 h_2)^n + (c^r h^r)^n = 0 \,.$$

By Greenleaf's result on Fermat's equation, quoted above,

$$h_1, h_2, h_3 \in K, \qquad \text{that is } f_1 - r_i f_0 \in K \ (i = 1, 2, 3).$$

This implies that $(r_1 - r_2) f_0 \in K$ hence $f_0, f_1 \in K$ and this is against the hypothesis. □

It is quite easy to provide many applications of the above proposition.

If $P(X) = X^m - 1$ and m is not divisible by the characteristic of K, we have Natanson's result.

If $P(X) = 1 - X^n$ we have Greenleaf's result.

If $P(X) = 1 + X + X^2 + \ldots + X^{m-1} + X^m$ and $n, m+1$ are not divisible by the characteristic of K, we may apply the proposition. Etc. ....

3. In this section, we shall indicate some results about valued fields; the valuations are not required to be of height 1.

PROPOSITION 4. *Let (K, v) be a valued field which is not henselian, having algebraically closed residue field. If $(\tilde{K}, \tilde{v})$ is a henselian valued field, extension of (K, v), then K is not existentially closed in $\tilde{K}$.*

PROOF. Let A_v denote the valuation ring of v, let $\bar{K}$ be the residue field of (K, v). For each polynomial $f \in A_v[X]$ let $\bar{f}$ denote its canonical image in $\bar{K}[X]$.

Since (K, v) is not henselian, there exist monic polynomials $f, g, h \in A_v[X]$ such that $\bar{f} = \bar{g}\bar{h}$, $gcd(\bar{g}, \bar{h}) = 1$, $\deg(g) > 0$, $\deg(h) > 0$, and such that there does not exist polynomials $g', h' \in A_v[X]$ such that $f = g'h'$, $\bar{g}' = \bar{g}$, $\bar{h}' = \bar{h}$, $\deg(g') = \deg(g)$. We choose f of minimal degree with the above property.

We show that f has no roots in K. Indeed, if $b \in K$ and $f(b) = 0$ then b is integral over A_v, hence $b \in A_v$. So $f = (X - b)^r f_1$, with $r \geqslant 1$, $f_1 \in K[X]$ and $f_1(b) \neq 0$; in particular, f_1 is monic. Let v^* be the natural extension of v to $K(X)$, defined by

$$v^*(a_0 X^m + a_1 X^{m-1} + \ldots + a_m) = \min_{0 \leqslant i \leqslant m} \{v(a_i)\}.$$

Then $v^*(f) = 0$, $v^*(X - b) = 0$ so $v^*(f_1) = 0$, thus $f_1 \in A_v[X]$. We have therefore $\bar{g}\bar{h} = \bar{f} = (X - \bar{b})^r \bar{f}_1$ and, say, $\bar{h}(\bar{b}) = 0$, hence $\bar{g}(\bar{b}) \neq 0$. So $\bar{h} = (X - \bar{b})^r \bar{k}$ where $k \in A_v[X]$ is a monic polynomial. Therefore $\bar{f}_1 = \bar{g}\bar{k}$, with $gcd(\bar{g}, \bar{k}) = 1$.

We have $\deg \bar{k} > 0$. Indeed if $\deg \bar{k} = 0$ then $k = 1$ so

$$f = (X - b)^r f_1 , \qquad \text{with } (X - \bar{b})^r = \bar{h} ,\ \bar{f}_1 = \bar{g} ,$$

which is against the hypothesis. By the minimality of f, there exist polynomials g_1', $k_1' \in A_v[X]$, such that

$$f_1 = g_1' k_1' , \quad \bar{g}_1' = \bar{g} , \quad \bar{k}_1' = \bar{k} , \quad \deg(g_1') = \deg(g) .$$

It follows that $f = g_1(X - b)^r k_1'$ with g_1',

$$(X - b)^r k_1' \in A_v[X] ,\ \bar{g}_1' = \bar{g} ,\ (X - \bar{b})^r \bar{k}_1' = \bar{h} ,\ \deg(g_1') = \deg(g) ,$$

which is a contradiction. So f has no roots in K.

On the other hand, the residue field $\bar{\tilde{K}}$ contains $\bar{K}$, which is algebraically closed. Since $\bar{f}$ has a root in $\bar{K} \subseteq \bar{\tilde{K}}$ and $(\tilde{K}, \tilde{v})$ is henselian, then f has a root in $\tilde{K}$.

This shows that K is not existentially closed in $\tilde{K}$. □

PROPOSITION 5. Let (K, v) be a valued field which is not henselian. If $(\tilde{K}, \tilde{v})$ is a henselian valued field, extension of (K, v), then $\tilde{K}|K$ is not a purely transcendental extension.

PROOF. We assume first that the residue field $\bar{K}$ is algebraically closed. By Proposition 4, K is not existentially closed in $\tilde{K}$. Since K is not finite (otherwise v is trivial and (K, v) would be henselian), by Proposition 1, $\tilde{K}|K$ is not a purely transcendental extension.

Now we assume that $\bar{K}$ is not algebraically closed. Let $\bar{K}^a$ denote the algebraic closure of $\bar{K}$. We claim:

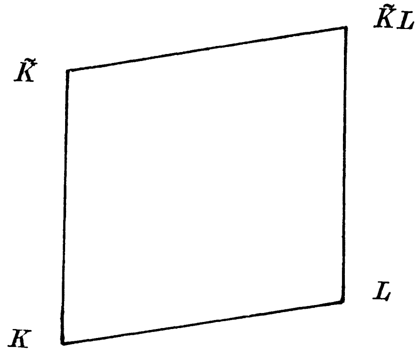
(*) There exists an algebraic extension $L|K$ such that:

1) v has a unique extension w to L,

2) $\bar{L} = \bar{K}^a$.

Assuming (*), we continue the proof. If $\tilde{K}|K$ is a purely transcendental extension, then $\tilde{K}L|L$ is purely transcendental and $\tilde{K}L|\tilde{K}$

is algebraic. Let $\tilde{w}$ be the unique extension of $\tilde{v}$ to $\tilde{K}L$, so $(\tilde{K}L, \tilde{w})$ is again a henselian valued field. Moreover, the restriction of $\tilde{w}$ to L must be equal to w, which is the only extension of v to L.



Now we observe that (L, w) is not henselian. Indeed, since (K, v) is not henselian, there exist at least two distinct extensions v_1^*, v_2^* of v to the algebraic closure K^a of K; we may assume $K^a \supseteq L$. Since the restrictions of v_1^*, v_2^* must be equal to w then (L, w) is not henselian.

Since $\bar{L}$ is algebraically closed, by Proposition 4 L is not existentially closed in $\tilde{K}L$, hence by Proposition 1 $\tilde{K}L/L$ is not purely transcendental, which is a contradiction.

It remains to establish the claim (*), which is in fact well-known. We include the proof for completeness.

Consider the family of all algebraic extensions L of K (contained in a given algebraic closure K^a), such that

1) v has a unique extension w to L,

2) $\bar{L} \subseteq \overline{K^a}$.

It is immediate that this family has a maximal element, which we still denote by L. We show that $\bar{L} = \overline{K^a}$.

If there exists $\gamma \in \overline{K^a}$, $\gamma \notin \bar{L}$, let $f \in A_w[X]$ be a monic polynomial such that $\bar{f} \in \bar{L}[X]$ is the minimal polynomial of γ over $\bar{L}$; let $n = \deg(\bar{f}) > 1$. Therefore f is irreducible in $A_w[X]$, and since A_w is a Bézout domain, f is also irreducible in $L[X]$.

Let $c \in L^a$ (algebraic closure of L) be a root of f, let $L' = L(c)$ and let w' be any extension of w to L'. Then $w'(c) \geq 0$, because $f \in A_w[X]$ and f is monic. Thus the residue field $\bar{L}'$ contains $\bar{L}(\bar{c})$. From $\bar{f}(\bar{c}) = 0$, it follows that $[\bar{L}(\bar{c}):\bar{L}] = n$ so $[\bar{L}':\bar{L}] \geqslant n$. This implies that $\bar{L}' = \bar{L}(\bar{c})$ and w' is the only extension of w to L'.

From the decomposition of f into linear factors (in its splitting field L''), $f = \prod_{i=1}^{n} (X - c_i)$ if w'' is a valuation of L'' extending v, then each $c_i \in A_{w''}$. Hence $\bar{f} = \prod_{i=1}^{n} (X - \bar{c}_i)$, so $\bar{c}_1, \ldots, \bar{c}_n$ are all the roots of $\bar{f}$, hence there exists i such that $\bar{c}_i = \gamma$. The above consideration (with $c = c_i$) shows that $\bar{L}' = \bar{L}(\gamma) \subseteq \bar{K}^a$, against the maximality of L. This concludes the proof. □

As corollaries, we have the following results already established in [6]:

COROLLARY 1. If K is any field, then $K((X))$ is not a purely transcendental extension of $K(X)$.

PROOF. The field $K(X)$ is not henselian with respect to the X-adic valuation. On the other hand, $K((X))$ is the completion of $K(X)$, relative to the X-adic valuation. So it is a henselian field, with respect to the natural extension of the X-adic valuation. By the proposition, $K((X))$ is not a purely transcendental extension of $K(X)$. □

COROLLARY 2. If p is any prime number, the field $\mathbf{Q}_p$ of p-adic numbers is not a purely transcendental extension of $\mathbf{Q}$.

PROOF. $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$, with respect to the p-adic valuation. Since $\mathbf{Q}$ is not henselian, while $\mathbf{Q}_p$ is henselian (with respect to the p-adic valuation), then $\mathbf{Q}_p$ is not a purely transcendental extension of $\mathbf{Q}$. □

BIBLIOGRAPHY

[1] L. VAN DEN DRIES, *Model Theory of Fields, Decidability and Bounds for Polynomial Ideals*, Thesis, University of Utrecht, 1978.

[2] N. GREENLEAF, *On Fermat's equation in* $\mathbf{C}(t)$, Amer. Math. Monthly, **76** (1969), pp. 808-809.

[3] R. LIOUVILLE, *Sur l'impossibilité de la relation algébrique* $X^n + Y^n + Z^n = 0$, C. R. Acad. Sci. Paris, **87** (1879), pp. 1108-1110.

[4] M. NATANSON, *Catalan's equation in* $K(t)$, Amer. Math. Monthly, **81** (1974), pp. 371-373.
[5] P. RIBENBOIM, *Théorie des Valuation,* Presses Université de Montréal, 1964.
[6] P. RIBENBOIM, *On the completion of a valuation ring,* Math. Annalen, **155** (1964), pp. 392-396.

Manoscritto pervenuto in redazione il 7 ottobre 1982.