

INVERSES OF POLYNOMIAL FUNCTIONS IN TOPOLOGICAL FIELDS¹

JOHN O. KILTINEN

Let (K, \mathfrak{J}) be a (commutative) topological field. (We do not require that multiplicative inversion be continuous, i.e. \mathfrak{J} is a ring topology. See [1, p. 274] for the definition of the latter.) Throughout this paper, \mathfrak{U} will denote a basic system of neighborhoods of zero for \mathfrak{J} . Let $P(X)$ be a polynomial in $K[X]$ of degree $n \geq 2$, and let $S = \{P(a) \mid a \in K\}$. We will be concerned with suitably defining a multiple-valued inverse P^\leftarrow for P on S , and then considering questions of continuity and uniform continuity for P^\leftarrow . We will be particularly interested in polynomials which are monic and of degree 2, or of the form $P(X) = X^n$. For $P(X) = X^n$, P^\leftarrow will be called the *n*th root function.

We will show that the uniform continuity of P^\leftarrow is sometimes related to \mathfrak{J} being type V . Indeed, if $\deg P = 2$ and $\text{char } K \neq 2$, then P^\leftarrow is uniformly continuous if and only if \mathfrak{J} is type V . The hypothesis that $\text{char } K \neq 2$ cannot be eliminated, as will be demonstrated by exhibiting nontrivial topological fields of characteristic 2 which are not type V , but in which the (single-valued) square root function is uniformly continuous. In greater generality, for each prime p , we will exhibit topological fields of characteristic p which are not of type V , but in which the p th root function is uniformly continuous.

Finally, we will show that inverses of polynomials need not be continuous at all. Specifically, we will exhibit topological fields of arbitrary characteristic other than 2 in which the square root function is discontinuous.²

1. Inverses for polynomials. Let $\mathcal{K} = \{F \mid F \subseteq K, F \text{ finite}\}$. For $P \in K[X]$, we define P^\leftarrow from S into \mathcal{K} by $P^\leftarrow(y) = \{a \in K \mid P(a) = y\}$ for all $y \in S$. In order to talk about continuity for P^\leftarrow , as in [1, Exercise 5, p. 206], we will consider a natural uniform structure on \mathcal{K} . For each U in \mathfrak{U} , let \bar{U} be the subset of $\mathcal{K} \times \mathcal{K}$ defined by $\bar{U} = \{(F_1, F_2) \mid \text{for all } a \in F_i \text{ there exists } b \in F_j \text{ such that } a - b \in U, \text{ for } (i, j) = (1, 2) \text{ and } (i, j) = (2, 1)\}$. Let \mathfrak{V} be the filter generated by all the sets \bar{U} . One may easily check that $(\mathcal{K}, \mathfrak{V})$ is a uniform structure. It will be this

Received by the editors May 5, 1969.

¹ This research has been supported in part by NSF Grant GP-8496.

² It was a consideration of this question of whether the square root function is necessarily continuous in a topological field, which was raised by Hansjoachim Groh in the problems section of the Amer. Math. Monthly 75 (1968), 912, which led the author to the results in this paper.

uniformity with which we will work. S will of course have the relative topology.

2. Type V topologies. A subset B of K is *bounded* if for all $U \in \mathfrak{U}$ there is a $V \in \mathfrak{U}$ such that $V \cdot B \subseteq U$. B is *bounded away from zero* if its complement $K \sim B$ is a neighborhood of zero. \mathfrak{I} is of *type V* if for any set B bounded away from zero, B^{-1} is bounded.³ \mathfrak{I} is *locally bounded* if there is a bounded neighborhood of zero. Type V topologies are locally bounded [1, Exercise 22, p. 321].

A proof of the following lemma may be found in [3, Lemma 4, p. 911]. The corollary follows easily.

LEMMA 1. \mathfrak{I} is of type V if and only if for any two sets A and B bounded away from zero, $A \cdot B$ is also bounded away from zero.

COROLLARY. \mathfrak{I} is of type V if and only if:

- (1) For all $U \in \mathfrak{U}$ there is a $V \in \mathfrak{U}$ such that if $a \cdot b \in V$, then $a \in U$ or $b \in U$.

We first observe that a topology being type V assures that the n th root function is uniformly continuous in very many cases.

THEOREM 1. Let (K, \mathfrak{I}) be a type V topological field over which the polynomial $X^n - 1$ factors into linear polynomials. Then the n th root function, P^\leftarrow , (where $P(X) = X^n$) is uniformly continuous.

PROOF. Let

$$\begin{aligned} m &= 1 && \text{if char } K = 0, \\ &= p^k, && \text{where } n = p^k r, \quad (r, p) = 1, \quad \text{if char } K = p. \end{aligned}$$

Then $X^n - 1 = (X^r - 1)^m$, where $r = n/m$, and by looking at its derivative, one can see that $X^r - 1$ has no multiple roots. Then since $X^n - 1$ factors into linear polynomials, there are r distinct n th roots of unity, $w_1 = 1, w_2, \dots, w_r$.

Now for any b in K , $X^n - b^n = (X^r - b^r)^m$. Since $X^r - b^r$ has the r distinct roots $b, w_2 b, \dots, w_r b$, we have over K the factorization

$$X^n - b^n = (X - b)^m (X - w_2 b)^m \cdots (X - w_r b)^m.$$

To see that P^\leftarrow is uniformly continuous, we must show that for all U in \mathfrak{U} there is a V in \mathfrak{U} such that for all a and b in K , if $a^n - b^n \in V$,

³ Bourbaki calls such topologies *locally retrobounded* [1, Exercise 22, p. 321]. The terminology used here is due to I. Kaplansky [3, p. 910].

then $(P^{\leftarrow}(a^n), P^{\leftarrow}(b^n)) \in \overline{U}$. Let $U \in \mathfrak{U}$ be given. There is a U' in \mathfrak{U} such that $\{1, w_2, \dots, w_r\} U' \subseteq U$. Extending (1) of the corollary to Lemma 1 by induction, we assert that there is a set V in \mathfrak{U} such that if $c_1 \cdot c_2 \cdot \dots \cdot c_n \in V$, then $c_i \in U'$ for some i , $1 \leq i \leq n$.

Now let $a^n - b^n$ be in V for some a and b in K . Since

$$a^n - b^n = (a - b)^m (a - w_2 b)^m \dots (a - w_r b)^m,$$

for some i , $1 \leq i \leq r$, we have $a - w_i b \in U'$.

Suppose that $c \in P^{\leftarrow}(a^n)$. Then $c = aw_j$ for some j , $1 \leq j \leq r$. Also, $w_i b w_j \in P^{\leftarrow}(b^n)$, and $c - w_i b w_j = (a - w_i b) w_j \in U' w_j \subseteq U$. Similarly, for $c \in P^{\leftarrow}(b^n)$, we may find a $d \in P^{\leftarrow}(a^n)$ such that $c - d \in U$. Thus, we have shown that if $a^n - b^n \in V$, then $(P^{\leftarrow}(a^n), (P^{\leftarrow}(b^n))) \in \overline{U}$, and the proof is complete.

COROLLARY. *For any topological field (K, \mathfrak{I}) of type V , the square root function is uniformly continuous.*

PROOF. The polynomial $X^2 - 1$ factors over K , so this result follows from the theorem.

We are able to prove the converse for this corollary if we restrict attention to fields of characteristic other than 2. In fact, we have the following somewhat more general theorem.

THEOREM 2. *If (K, \mathfrak{I}) is a topological field, if $\text{char } K \neq 2$, and if $P(X) = X^2 + \alpha X + \beta$, $\alpha, \beta \in K$, then P^{\leftarrow} is uniformly continuous if and only if \mathfrak{I} is type V .*

PROOF. Note that for $y = P(a) \in S$, $P^{\leftarrow}(y) = \{a, -a - \alpha\}$. Clearly P^{\leftarrow} is uniformly continuous if and only if:

- (2) *For all $U \in \mathfrak{U}$ there is a $V \in \mathfrak{U}$ such that if $P(a) - P(b) \in V$, then $a - b \in U$ or $a + b + \alpha \in U$.*

Now $P(a) - P(b) = (a - b)(a + b + \alpha)$. Thus, (2) clearly follows from (1) of the corollary to Lemma 1.

Conversely, we may deduce (1) from (2). Let $U \in \mathfrak{U}$ be given. Assuming that (2) is true, let V be a set in \mathfrak{U} satisfying $P(a) - P(b) \in V$ implies $a - b \in U$ or $a + b + \alpha \in U$. Now suppose that $c \cdot d \in V$. Since $\text{char } K \neq 2$, the system of linear equations

$$\begin{aligned} a - b &= c \\ a + b + \alpha &= d \end{aligned}$$

has a solution $a = (c + d - \alpha)/2$, $b = (d - c - \alpha)/2$. But then $P(a) - P(b) = (a - b)(a + b + \alpha) = c \cdot d \in V$, so by (2), $c = a - b \in U$ or $d = a + b + \alpha$

$\in U$. Thus, (1) is proven.

Note that if the property in Lemma 1 were taken as the defining property for a type V topology, thus removing dependence on multiplicative inverses, then Theorem 2 clearly generalizes to any topological integral domain in which 2 is invertible.

3. Inverses of linear polynomials. Over a field K of nonzero characteristic p , there are many polynomials $P(X)$ which are *linear* in the sense that $P(a+b) = P(a) + P(b)$ for all a and b in K . For example, take P to be of the form $P(X) = \sum_{i=0}^n \alpha_i X^{pi}$. Uniform continuity for inverses of polynomials of this type is equivalent to a simpler condition.

LEMMA 2. *Let (K, \mathfrak{J}) be a topological field, and let P be a linear polynomial over K . P^\leftarrow is uniformly continuous if and only if P^\leftarrow is continuous at y for some y in S .*

PROOF. Let $y = P(c)$. Note that P^\leftarrow is continuous at y if and only if:

For all $U \in \mathfrak{U}$ there is a $V \in \mathfrak{U}$ such that for all $a \in K$, if $P(a) - P(c) \in V$, then $(P^\leftarrow(P(a)), P^\leftarrow(P(c))) \in \overline{U}$.

P^\leftarrow is uniformly continuous if and only if:

For all $U \in \mathfrak{U}$ there is a $V \in \mathfrak{U}$ such that for all a and $b \in K$, if $P(a) - P(b) \in V$, then $(P^\leftarrow(P(a)), P^\leftarrow(P(b))) \in \mathfrak{U}$.

The equivalence of these two conditions follows from the facts that $P(a) - P(b) = P(a - b + c) - P(c)$, and

$(P^\leftarrow(P(a)), P^\leftarrow(P(b))) \in \overline{U}$ if and only if $(P^\leftarrow(P(a - b + c)), P^\leftarrow(P(c))) \in \overline{U}$.

To see that this last assertion is true, suppose

$$(P^\leftarrow(P(a - b + c)), P^\leftarrow(P(c))) \in \overline{U}.$$

Let d be in $P^\leftarrow(P(a))$. We must find an $e \in P^\leftarrow(P(b))$ such that $d - e \in U$. Now $P(d - b + c) = P(a - b + c)$. Hence,

$$d - b + c \in P^\leftarrow(P(a - b + c)),$$

so there is an $e' \in P^\leftarrow(P(c))$ such that $d - b + c - e' \in U$. Let $e = b - c + e'$. Then $d - e \in U$, and $P(e) = P(b) - P(c) + P(e') = P(b)$, so $e \in P^\leftarrow(P(b))$. Similarly, one shows that for all $c \in P^\leftarrow(P(b))$ there is a $d \in P^\leftarrow(P(a))$ such that $d - e \in U$. Thus, $(P^\leftarrow(P(a)), P^\leftarrow(P(b))) \in \overline{U}$. The implication in the other direction is proven similarly.

4. Inductive c.p.r. ring topologies. In this section we will develop a technique for exhibiting topologies on fields of prime characteristic p which are not type V but in which the p th root function is uniformly continuous. The technique will be a modification of the method of inductive ring topologies introduced in [2] and developed in §§1–5 of [4]. Since the proofs of the theorems are virtually the same as the corresponding ones in [4], we will state them without proof here.

If K has characteristic p , then the function $P(X) = X^p$ is a monomorphism, so $P^\leftarrow: S \rightarrow \mathcal{K}$ takes elements a^p of S to singletons $\{a\}$. Since the subset of \mathcal{K} consisting of the singletons is homeomorphic with K , we may regard P^\leftarrow as a function from S into K in this case. We will restrict our attention for the remainder of this section to *perfect* fields of characteristic p . These are precisely the fields for which P is an automorphism [5, p. 64], and hence P^\leftarrow is also an automorphism. Thus, if K is perfect of characteristic p , then every element a of K has a unique p th root in K , which we will denote by $a^{1/p}$.

To get a topology on K for which P^\leftarrow is uniformly continuous, by Lemma 2, we need only assure that P^\leftarrow is continuous at zero. The method of [4] gives rise to ring topologies without specific further properties. However, by modifying the method, we can develop topologies with this latter property.

To begin, let $(B_n)_{n \geq 1}$ be a sequence of subsets of K such that $B_1 \subseteq B_2 \subseteq \dots$, and $\bigcup_{n=1}^{\infty} B_n = K$. Let $K[(X_n)]$ denote the ring of polynomials over K in a countable set $\{X_1, X_2, \dots\}$ of indeterminates. As in [4, p. 150], we define inductively a double sequence of subsets of $K[(X_n)]$:

$$\begin{array}{lll} W_0^0, & W_0^1, & W_0^2, \dots \\ & W_1^1, & W_1^2, \dots \\ & & W_2^2, \dots \\ & & \vdots \\ & & \vdots \end{array}$$

Let $W_0^0 = \{0\}$. Suppose now that the sets W_n^m have been defined for all n and m such that $0 \leq n \leq m \leq k$ in such a way that:

- (3) For all $Q \in W_n^m$, each monomial $\alpha X_1^{r_1} \cdot X_2^{r_2} \cdot \dots \cdot X_s^{r_s}$ of Q with a nonzero coefficient α is such that $p^n \mid r_i$, $1 \leq i \leq s$.

Then set $W_{k+1}^{k+1} = \{0, X_{k+1}^{k+1}, -X_{k+1}^{k+1}\}$. Then clearly W_{k+1}^{k+1} also satisfies (3). Suppose now that W_j^{k+1} has been defined for each j such that $k+1 \geq j \geq r+1$, and such that (3) holds for $m = k+1$ and $n = j$ for

each j . We then define W_r^{k+1} by

$$(4) \quad W_r^{k+1} = \left[\left(W_{r+1}^{k+1} + \bigcup_{s=r+1}^{k+1} W_{r+1}^s \right) \cup \left(W_{r+1}^{k+1} \cdot \bigcup_{s=r+1}^{k+1} W_{r+1}^s \right) \right. \\ \left. \cup (B_{r+1} \cdot W_{r+1}^{k+1}) \cup \{Q^{1/p} \mid Q \in W_{r+1}^{k+1}\} \right] \sim \left[\bigcup_{s=r}^k W_r^s \right].$$

Note that condition (3), the fact that all elements of K have p th roots, and that the function $y \rightarrow y^p$ is a monomorphism in any integral domain of characteristic p assure that every polynomial Q in W_{r+1}^{k+1} has a unique p th root $Q^{1/p}$ in $K[(X_n)]$. Also, one may check that W_r^{k+1} satisfies (3) for $m = k+1$, $n = r$.

By induction, we have W_n^m defined and (3) true for all n and m , $n \leq m$. Now, let W_n be the union of the sets in the n th row of the array, i.e.,

$$W_n = \bigcup_{m=n}^{\infty} W_n^m.$$

One may verify that we have built into the collection $\{W_n \mid n \geq 0\}$ the following properties for all $n \geq 0$:

$$\begin{aligned} 0 &\in W_n \\ W_n &= -W_n \\ W_{n+1} + W_{n+1} &\subseteq W_n \\ W_{n+1} \cdot W_{n+1} &\subseteq W_n \\ B_{n+1} \cdot W_{n+1} &\subseteq W_n \\ W_{n+1}^{1/p} &\subseteq W_n. \end{aligned}$$

If we let $(a_k)_{k \geq 1}$ denote a sequence of elements of K , and let $\sigma_{(a_k)}$ be the substitution homomorphism from $K[(X_n)]$ to K defined by $Q(X_1, X_2, \dots) \rightarrow Q(a_1, a_2, \dots)$ for all Q in $K[(X_n)]$, then the sets $V_n = \sigma_{(a_k)}(W_n)$ will satisfy the corresponding conditions with the W_n 's replaced by V_n 's. The first five conditions assure that $\mathfrak{V} = \{V_n \mid n \geq 0\}$ is a basic system of neighborhoods for a ring topology on K , [1, p. 275]. The last one clearly assures that the p th root function is continuous at zero.

DEFINITION. Call the topology just defined on K the *inductive c.p.r. ring topology* (the c.p.r. for continuous p th root) on K determined by the sequences (a_k) and (B_k) . Denote it by $\mathfrak{I}_{c.p.r.}((a_k), (B_k))$.

The only ways that the definition of $\mathfrak{I}_{c.p.r.}((a_k), (B_k))$ differs from that of an inductive ring topology $\mathfrak{I}((a_k), (B_k))$ defined in [4] is the

inclusion of $\{Q^{1/p} \mid Q \in W_{r+1}^{k+1}\}$ in W_r^{k+1} , and the fact that for an ordinary inductive topology, W_{k+1}^{k+1} would have been defined to be $\{0, X_{k+1}, -X_{k+1}\}$ instead of what we took it to be here. What is important is that in spite of these changes, the two basic lemmas for inductive topologies which enabled us to prove the existence of Hausdorff ones still remain valid.

LEMMA 3. *Let Q be in W_n^m . If $n < m$, then Q_m^* is in W_n^j for some j such that $n \leq j < m$.*

Here Q_m^* denotes the sum of all the monomials of Q which are not divisible by X_m . The proof of this lemma is like that of Lemma 2.1 [4, p. 153]. The only additional fact needed here is that $(Q^{1/p})_m^* = (Q_m^*)^{1/p}$.

LEMMA 4. *Let Q be a nonzero element of W_n^m . Then Q is a polynomial in X_m with coefficients in $K[X_1, \dots, X_{m-1}]$ such that $1 \leq \deg_m(Q) \leq p^m \cdot 2^{m-n}$.*

$\deg_m(Q)$ denotes the degree of Q in the indeterminate X_m . This lemma corresponds to Lemma 2.2 [4, p. 153].

On the strength of these two lemmas, the development in §§3–5 of [4] could be copied almost verbatim with, however, attention restricted to perfect fields of characteristic p . From this would come the following analog of Theorem 5.2 [4, p. 159].

THEOREM 3. *If K is an infinite perfect field of characteristic p , then there are nondiscrete, Hausdorff inductive c.p.r. ring topologies on K .*

We now look at a class of fields on which the inductive c.p.r. topologies cannot be type V . These will be the *absolutely algebraic* fields of prime characteristic, i.e., fields K which are algebraic over their finite prime subfield Z_p .

Let K be an infinite absolutely algebraic field of characteristic p . Then clearly K is perfect. By Theorem 3, there is an inductive c.p.r. ring topology \mathfrak{I} on K which is nondiscrete and Hausdorff. Now \mathfrak{I} is not type V , for as we observed in §2, a type V topology is locally bounded, and it is known [4, Theorem 6.1, p. 159] that the only locally bounded ring topologies on K are the discrete and indiscrete topologies. Since we have made certain that the p th root function is uniformly continuous for \mathfrak{I} , we have the following result.

THEOREM 4. *For any prime p , there are topological fields (K, \mathfrak{I}) of characteristic p which are not type V but for which the p th root function is uniformly continuous.*

It is unknown to the author under what conditions, if any, the uniform continuity of P^ϵ for P a polynomial of degree 3 or more implies that the topology is type V . Theorem 4 shows, however, that if results in this direction are to be obtained, restrictions on the characteristic of the field appear necessary, as was the case in Theorem 2.

5. Discontinuous square roots. Let D be a principle ideal domain of characteristic other than 2, and let K be its quotient field. Then D is also a unique factorization domain [5, Theorem 32, p. 243]. Suppose that D has at least two relatively prime irreducible elements, π and χ , which do not divide 2. Let $\mathfrak{U} = \{(b) \mid b \in D, b \neq 0\}$, where (b) denotes the principle ideal in D generated by b . One may check that \mathfrak{U} is a basic system of neighborhoods of zero for a ring topology \mathfrak{J} on K [1, p. 275]. We will show that the square root function P^ϵ is discontinuous at one for this topology.

To do this, we will show that for every a in D , $a \neq 0$, there is a b in D such that $b^2 - 1 \in (a)$, but $b - 1 \notin (\pi\chi)$ and $b + 1 \notin (\pi\chi)$. Thus, there is no (a) in \mathfrak{U} such that for all b in K , if $b^2 - 1 \in (a)$, then $(P^\epsilon(b^2), P^\epsilon(1)) \in (\overline{\pi\chi})$.

Let a in D be given, $a \neq 0$.

Case 1. a is not a multiple $\pi\chi$. Then $a \notin (\pi\chi)$. Since neither π nor χ divides 2, either $a + 2 \notin (\pi\chi)$ or $a - 2 \notin (\pi\chi)$. In these respective cases, let $b = a + 1$ and $b = a - 1$. In either case, we have $b^2 - 1 = (b - 1)(b + 1) \in (a)$, but $b - 1 \notin (\pi\chi)$ and $b + 1 \notin (\pi\chi)$.

Case 2. a is a multiple of $\pi\chi$. Let $a = (\pi\chi)^i a'$, where $a' \in D$ and $\pi\chi$ does not divide a' in D . Since π^i and χ^i are relatively prime in D , clearly there are r and s in D such that $\pi^i r - \chi^i s = -2$ [5, Theorem 32, p. 243]. Then for all y in D , $\pi^i(r + y\chi^i) - \chi^i(s + y\pi^i) = -2$. Since $\pi\chi$ does not divide a' in D , either $(\pi, a') = 1$ or $(\chi, a') = 1$. Assume the former. Then there exist c and d in D such that $a'c - \pi^i d = 1$. Let $b' = ds$, and let $b = \pi^i(r + b'\chi^i) + 1$. Then $b^2 - 1 = (b - 1)(b + 1) = \pi^i(r + b'\chi^i)\chi^i(s + b'\pi^i) = \pi^i(r + b'\chi^i)\chi^i s(1 + d\pi^i) = \pi^i(r + b'\chi^i)\chi^i s a'c = a(r + b'\chi^i)sc$. Thus, $b^2 - 1 \in (a)$.

However, neither $b - 1$ nor $b + 1$ is in $(\pi\chi)$. Suppose to the contrary that $b - 1 \in (\pi\chi)$. Then χ divides $b - 1 = \pi^i(r + b'\chi^i)$, so χ must divide $r + b'\chi^i$. Since $i \geq 1$, this implies that χ divides r , but then by one of the equations above, χ divides 2, a contradiction. One similarly shows that $b + 1 = \chi^i(s + b'\pi^i) \notin (\pi\chi)$.

One may check that continuity of the square root function P^ϵ at any nonzero square of a topological field implies continuity at any other nonzero square. Thus, for this topology, P^ϵ is discontinuous at

every nonzero square. Note, however, that P^ϵ is continuous at zero. From these observations, we have the following theorem.

THEOREM 5. *There are topological fields for which the square root function is discontinuous at every nonzero point.*

We remark that virtually this same proof shows that P^ϵ is discontinuous at one for the topology determined by a basic system of neighborhoods of zero $\mathfrak{U}' = \{ (a)/1 + (a) \mid a \in D, a \neq 0 \}$. This topology renders multiplicative inversion continuous, indicating that continuous inversion does not necessarily have any influence on the continuity of the square root function.

REFERENCES

1. N. Bourbaki, *Elements of mathematics*. Part I: General topology, Hermann, Paris and Addison-Wesley, Reading, Mass., 1966. MR 34 #5044a.
2. L. Hinrichs, *Integer topologies*, Proc. Amer. Math. Soc. 15 (1964), 991–995. MR 31 #2286.
3. I. Kaplansky, *Polynomials in topological fields*, Bull. Amer. Math. Soc. 54 (1948), 909–916. MR 10, 280.
4. J. Kiltinen, *Inductive ring topologies*, Trans. Amer. Math. Soc. 134 (1968), 149–169. MR 37 #4054.
5. O. Zariski and P. Samuel, *Commutative algebra*. Vol. I, The University Series in Higher Mathematics, Van Nostrand, Princeton, N. J., 1958. MR 19, 833.

UNIVERSITY OF MINNESOTA