JOURNAL OF ALGEBRA 15, 417–428 (1970)

Zeros of Polynomials over Local Fields—The Galois Action*

JAMES AX†

Department of Mathematics, State University of New York at Stony Brook, Stony Brook, Long Island, New York 11790

Communicated by W. Feit

Received September 18, 1969

This paper will be devoted to investigating certain geometric properties of the zeros of polynomials over local field and some applications of these properties. Our main result generalizes (and simplifies the proof of) a theorem of Tate [1], Theorem 1, concerning the fixed field of the Galois action on the completion of the algebraic closure of a local field. This is an application of a geometric theory to be developed in a sequel; the special facts required are proved in an *ad hoc* fashion when they are used. We have chosen this approach because there is a gap between the geometric properties which can be neatly encompassed in a general theory and the actual properties required for the main result.

Throughout this paper k will denote a *local field*, a term which we use in a loose sense: a field with a non-trivial valuation ord (in an ordered abelian group) with respect to which k is henselian. It is convenient to introduce the following terminology:

$$
\begin{aligned}
\tilde{k} &= \text{algebraic closure of } k;\\
\tilde{k}^s &= \text{separable algebraic closure;}\\
\sqrt{}k &= \text{perfect closure, i.e., } k^{p^{-\infty}} \text{ if char } k = p;\\
\hat{k} &= \text{completion of } k;\\
\bar{k} &= \text{residue class field of } k;\\
k^t &= \hat{h} \text{ where } h = \tilde{k}.
\end{aligned}
$$

THEOREM. *Let K be a local field. If we let $G_k = \mathcal{G}(\tilde{k}/k)$, the galois group of k, operate on k^t by uniform continuity then the fixed field is $\widehat{\sqrt{}k}$. We have $k^t = k^{st}$.*

The first assertion is our main result. Tate proved it in the case where char $k = 0$ and the value group is archimedean. While the removal of this

* This work was partially done while the author was a summer faculty employee at the IBM T. J. Watson Research Center, Yorktown Heights, New York.

† Sloan Fellow.

last restriction is of no real interest it points out the relative simplicity of our methods: Tate's proof depends ultimately on class field theoretical information in ramification theory which is, therefore, applicable only in certain classical situations; our proof, relying as it does on very basic geometric properties of zeros of polynomials, works equally well for *big* value groups.

The removal of the restriction on the characteristic of k is of some interest. It is accomplished by another direct but different argument from that employed when char $k = 0$.

The idea behind the proof of our main result is quite simple (it is this idea to which Tate alludes in his third remark after Theorem 1 of [1]). If $\lambda \in k^t$ is fixed under G_k, then λ is the limit of $\lambda_i \in \tilde{k}$ which are *almost* fixed by G_k; hence, there is a *small* disk D_i such that $\sigma\lambda_i \in D_i$ for all $\sigma \in G_k$. Now a classical theorem[1] of Gauss [2], p. 112, states that a disk in the complex numbers containing all roots of a polynomial contains all roots of its derivative. We prove enough of an analogue of Gauss's theorem to establish that if f is the monic irreducible polynomial for λ_i over $\sqrt{k}$, then f' has *enough* zeroes in a *slightly* larger disk, E_i. An inductive argument now shows that λ_i must be *close* to $\sqrt{k}$. Hence, $\lambda = \lim \lambda_i$ is in $\sqrt{\hat{k}}$.

1. The Location of the Zeros of the Derivatives of a Polynomial

The main argument are those of a Newton-polygon type which is essentially contained in the following well-known fact. Let C denote an algebraically closed valued field.

Lemma 1. *Let*

$$h(X) = \prod_{\tau=1}^{t} (X - \gamma_\tau) = \sum_{i=0}^{t} a_i X^i \in C[X].$$

Assume ord $\gamma_1 \geqslant$ ord $\gamma_2 \cdots \geqslant$ ord γ_t. *Then for* $0 \leqslant i < t$,

$$\text{ord } a_i \geqslant \text{ord}(\gamma_{i+1} \cdots \gamma_t). \qquad (*)$$

If ord $\gamma_i >$ ord γ_{i+1}, *then equality holds and, in fact,*

$$\text{ord}(1 - (-1)^{t-i} a_i/\gamma_{i+1} \cdots \gamma_t) > 0.$$

Proof. We have

$$a_i = (-1)^{t-i} \sum_{\tau_1 < \cdots < \tau_{t-1}} \gamma_{\tau_1} \cdots \gamma_{\tau_{t-i}} \qquad (**)$$

[1] For further historical references to this result which is sometimes credited to Lucas and for some simple proofs, see Polya and Szegö, "Aufgaben und Lehrsätze aus der Analysis," Vol. 1, Solution to Problem 31 of III.

and this yields (*) since $\operatorname{ord} \gamma_{\tau_1 \cdots \tau_{t-i}} \geqslant \operatorname{ord} \gamma_{i+1} \cdots \gamma_t$ and if $\operatorname{ord} \gamma_i > \operatorname{ord} \gamma_{i+1}$, then equality holds only if $\tau_j = i + j$ for $1 \leqslant j \leqslant t - i$ so that $\gamma_{i+1} \cdots \gamma_t$ is the unique summand in (**) of smallest ord value.

DEFINITION. If $f = \sum_{i=0}^{1} a_i X^i \in C[X]$, then $f^{[j]} = \sum_{i=0}^{1} \binom{i}{j} a_i X^{i-j}$.

We note:

(a) $f^{[j]}$ has coefficients in any subring of C containing the coefficients of f;

(b) $j! f^{[j]} = f^{(j)}$, the j-th derivative of f;

(c) the (linear) operator $f \to f^{[j]}$ commutes with translations, i.e., if $a \in C$ and $g(X) = f(X + a)$, then $g^{[j]}(X) = f^{[j]}(X + a)$;

(d) if $a \in C$, then $f(X) = \sum_{j=0}^{d} f^{[j]}(a)(X - a)^j$.

DEFINITION. A subset D of C will be called a *disk* if there exists $c \in C$ and λ in the value group such that

$$D = \{x \in C \mid \operatorname{ord}(x - c) \geqslant \lambda\}.$$

The *diameter* of D is λ.

LEMMA 2. *Let $f \in C[X]$ be of exact degree $d = p^\delta d_1 = q d_1$, where $p = \operatorname{char} \bar{C}$ if $\operatorname{char} \bar{C} > 0$ and $p = 1$ if $\operatorname{char} \bar{C} = 0$, and where $(p, d_1) = 1$. Assume $q < d$ and that D is a* disk *containing all the roots of f. Then $f^{[q]}$ has a zero in D.*

Proof. We can assume f is monic and by (c), above, that $0 \in D$. Let

$$f(X) = \prod_{i=1}^{d} (X - \alpha_i) = \sum_{i=0}^{d} a_i X^i, \operatorname{ord} \gamma_1 \geqslant \cdots \geqslant \operatorname{ord} \gamma_d = r.$$

Then by Lemma 1,

$$\operatorname{ord} a_i \geqslant (d - i) r \qquad \text{for} \quad 0 \leqslant i < d.$$

Set

$$f^{[q]} = \sum_{i=q}^{d} \binom{i}{q} a_i X^{i-q} = \sum_{j=0}^{d-q} b_j X^j.$$

Then

$$b_j = \binom{j+q}{q} a_{j+q} \qquad \text{for} \quad 0 \leqslant j \leqslant d - q.$$

In particular,

$$\operatorname{ord} b_{d-q} = \operatorname{ord} \binom{d}{q} + \operatorname{ord} a_d = \operatorname{ord} \binom{d}{q} = 0$$

and

$$\operatorname{ord} b_0 = \operatorname{ord} q_q \geqslant (d-q)\,r.$$

Set

$$f^{[q]} = \binom{d}{q} \prod_{j=1}^{d-q} (X - \beta_j).$$

Then

$$\binom{d}{q} \prod_{j=1}^{d-q} (-\beta_j) = b_0$$

which yields

$$\sum_{j=1}^{d-q} \operatorname{ord} \beta_j \geqslant (d-q)r.$$

Hence, there exists j_0 such that $1 \leqslant j_0 \leqslant d-q$ and $\operatorname{ord} \beta_{j_0} \geqslant r$; this is the desired conclusion.

LEMMA 3. *Let* char $C = 0$ *and let* $f \in C[X]$ *be of exact degree* $d = p^\delta > 1$ *where* $p =$ char $\bar{C} > 0$. *Let* $q = p^{\delta-1}$ *and assume* f *has all its zeros in a* disk D. *Then* $f^{[q]}$ *has a zero in the disk* D' *with center in* D *and diameter equal to the diameter of* D *enlarged by* $(\operatorname{ord} p)/(d-q)$.

Proof. We can assume f is monic and $0 \in D$.
Set

$$f = \sum_{i=0}^{d} a_i X^i = \prod_{j=1}^{d} (X - \alpha_j),$$

$$f^{[q]} = \sum_{i=q}^{d} \binom{i}{q} a_i X^{i-q} = \binom{d}{q} \sum_{j=0}^{d-q} b_j X^j = \binom{d}{q} \prod_{j=1}^{d-q} (X - \beta_j).$$

Now

$$\operatorname{ord} \binom{d}{q} = \operatorname{ord} \binom{p^\delta}{p^{\delta-1}} = \operatorname{ord} p \neq \infty.$$

Also,

$$\sum_{j=1}^{d-q} \operatorname{ord} \beta_j = \operatorname{ord} b_0 = \operatorname{ord} \left(a_q \Big/ \binom{d}{q} \right)$$

$$= \operatorname{ord} a_q - \operatorname{ord} p \geqslant (d-q) \min_j \operatorname{ord} \alpha_j - \operatorname{ord} p.$$

Hence, there exists j_0 such that $1 \leqslant j_0 \leqslant d - q$ and

$$\operatorname{ord} \beta_{j_0} \geqslant \min_j \operatorname{ord} \alpha_j - (\operatorname{ord} p)/(d - q).$$

2. The Diameter of the Conjugates

Let k be a local field with algebraic closure $\bar{k} = C$. Then the valuation of k extends uniquely to C since this property characterizes henselian fields.

Definition. If $\alpha \in C$, we set

$$\Delta_k(\alpha) = \Delta(\alpha) = \min\{\operatorname{ord}(\alpha' - \alpha) \mid \alpha' \in C, k \text{ conjugate to } \alpha\}.$$

If $\alpha \in \sqrt{k}$, then we set $\Delta(\alpha) = \infty$.

We are interested in comparing the diameter, $\Delta(\alpha)$, of the conjugates of α with the distance from α to k or, since this may not exist, the set of $\operatorname{ord}(\alpha - a)$ with $a \in k$. We have for all $a \in k$ and all k-conjugates α' of α

$$\begin{aligned}\operatorname{ord}(\alpha' - \alpha) &= \operatorname{ord}(\alpha' - a - (\alpha - a)) \\ &\geqslant \min(\operatorname{ord}(\alpha' - a), \operatorname{ord}(\alpha - a)) = \operatorname{ord}(\alpha - a).\end{aligned}$$

Hence, for all $a \in k$, $\Delta(\alpha) \geqslant \operatorname{ord}(\alpha - a)$. Our main result depends on showing that there exists $a \in k$ such that $\operatorname{ord}(\alpha - a)$ is *almost* equal to $\Delta(\alpha)$.

Lemma 4. *Assume* $\operatorname{char} k = 0$ *and* $\operatorname{char} \bar{k} = p > 0$. *Let* $\alpha \in C$. *Set* $n = [k(\alpha) : k]$. *Then there exists* $a \in k$ *such that*

$$\operatorname{ord}(\alpha - a) \geqslant \Delta(\alpha) - \sum_{i=1}^{\lambda(n)} (p^i - p^{i-1})^{-1} \operatorname{ord} p,$$

where $\lambda(n) = \max\{e \mid p^e \leqslant n\}$.

Proof. Let f be the monic irreducible polynomial for α over k. We establish our result by induction on n, the case $n = 1$ being trivial. If $n = p^\delta d_1 = q d_1$ with $(p, d_1) = 1$ and $d_1 > 1$, then by Lemma 2 applied to D, the disk centered at α of radius $\Delta(\alpha)$, we see that there exists a root β of $f^{[q]}$ such that $\operatorname{ord}(\alpha - \beta) \geqslant \Delta(\alpha)$. Let β' be any k conjugate of β and let σ be a k automorphism of C such that $\sigma\beta = \beta'$. Then

$$\begin{aligned}\operatorname{ord}(\beta' - \beta) &= \operatorname{ord}(\sigma\beta - \beta) = \operatorname{ord}(\sigma\beta - \sigma\alpha + \sigma\alpha - \alpha + \alpha - \beta) \\ &\geqslant \min(\operatorname{ord} \sigma(\beta - \alpha), \operatorname{ord}(\sigma\alpha - \alpha), \operatorname{ord}(\alpha - \beta)).\end{aligned}$$

We have $\operatorname{ord} \sigma(\beta - \alpha) = \operatorname{ord}(\beta - \alpha)$ and $\operatorname{ord}(\beta - \alpha)$, $\operatorname{ord}(\sigma\alpha - \alpha) \geqslant \Delta(\alpha)$.

Thus, $\operatorname{ord}(\beta' - \beta) \geqslant \Delta(\alpha)$, i.e., $\Delta(\beta) \geqslant \Delta(\alpha)$. Now, $[k(\beta) : k] = m \leqslant n - q < n$ and so by inductive hypothesis there exists $a \in k$ such that

$$\operatorname{ord}(\beta - a) \geqslant \Delta(\beta) - \sum_{i=1}^{\lambda(m)} (p^i - p^{i-1})^{-1} \operatorname{ord} p$$

$$\geqslant \Delta(\alpha) - \sum_{i=1}^{\lambda(n)} (p^i - p^{i-1})^{-1} \operatorname{ord} p.$$

Hence,

$$\operatorname{ord}(\alpha - a) \geqslant \min(\operatorname{ord}(\alpha - \beta), \operatorname{ord}(\beta - a))$$

$$\geqslant \Delta(\alpha) - \sum_{i=1}^{\lambda(n)} (p^i - p^{i-1})^{-1} \operatorname{ord} p.$$

In the remaining case, we have $n = p^\delta > 1$. We apply Lemma 3 to obtain a root β of $f^{[q]}$, $q = p^{\delta-1}$, such that $\operatorname{ord}(\beta - \alpha) \geqslant \Delta(\alpha) - (\operatorname{ord} p)/(n - q)$. As before, $\Delta(\beta) \geqslant \Delta(\alpha) - (\operatorname{ord} p/n - q)$. Thus, by inductive hypothesis, there exists $a \in k$ such that

$$\operatorname{ord}(\beta - a) \geqslant \Delta(\beta) - \sum_{i=1}^{\lambda(n-q)} (p^i - p^{i-1})^{-1} \operatorname{ord} p$$

$$\geqslant \Delta(\alpha) - 1/(n - q) - \sum_{i=1}^{\delta-1} (p^i - p^{i-1})^{-1} \operatorname{ord} p$$

$$= \Delta(\alpha) - \sum_{i=1}^{\lambda(n)} (p^i - p^{i-1})^{-1} \operatorname{ord} p.$$

Since

$$\operatorname{ord}(\beta - \alpha) \geqslant \Delta(\alpha) - \sum_{i=1}^{\lambda(n)} (p^i - p^{i-1})^{-1} \operatorname{ord} p,$$

we conclude

$$\operatorname{ord}(\alpha - a) \geqslant \Delta(\alpha) - \sum_{i=1}^{\lambda(n)} (p^i - p^{i-1})^{-1} \operatorname{ord} p.$$

This completes the proof.

PROPOSITION 1. *Let k be a local field with* char $k = 0$, char $\bar{k} = p > 0$. *Then for all $\alpha \in \tilde{k}$, there exists $a \in k$ such that*

$$\operatorname{ord}(\alpha - a) \geqslant \Delta(\alpha) - (p/(p-1)^2) \operatorname{ord} p.$$

Proof. This follows from Lemma 4, and the summation

$$\sum_{i=1}^{\infty} (p^i - p^{i-1})^{-1} = p/(p-1)^2.$$

LEMMA 5. *Let k be a local field with* $\operatorname{char} k = p > 0$. *If $\alpha \in \tilde{k}$ and $p = [k(\alpha) : k]$, then there exists $\beta \in k^{1/p}$ such that*

$$\operatorname{ord}(\alpha - \beta) \geqslant ((p-1)/p) \operatorname{ord} \alpha + \Delta(\alpha)/p.$$

Proof. We may assume α is separable over k. Let $\alpha = \alpha^{(1)}, \alpha^{(2)},..., \alpha^{(p)}$ denote the k conjugates of α. Set $\eta^{(i)} = \alpha^{(i)} - \alpha$ and

$$\nu = N_{k(\alpha)/k}(\alpha) = \prod_{i=1}^{p} \alpha^{(i)} = \prod_{i=1}^{p} (\alpha + \eta^{(i)}) = \alpha^p + b_1\alpha^{p-1} + \cdots + b_p\,,$$

where b_i is the i-th symmetric function of the $\eta^{(i)}$. Since $\operatorname{ord} \eta^{(i)} \geqslant \Delta(\alpha)$, we have

$$\operatorname{ord} b_i \geqslant i\Delta(\alpha).$$

Thus,

$$\begin{aligned}\operatorname{ord}(\nu - \alpha^p) &\geqslant \min_{1 \leqslant i \leqslant p} \operatorname{ord} b_i \alpha^{p-i} \\ &\geqslant \min_{1 \leqslant i \leqslant p} (i\Delta(\alpha) + (p-i) \operatorname{ord} \alpha) = \Delta(\alpha) + (p-1) \operatorname{ord} \alpha\end{aligned}$$

since

$$\Delta(\alpha) \geqslant \operatorname{ord} \alpha.$$

Thus,

$$\nu^{1/p} \in k^{1/p}$$

and

$$\operatorname{ord}(\nu^{1/p} - \alpha) \geqslant 1/p[\Delta(\alpha) + (p-1) \operatorname{ord} \alpha]$$

as desired.

LEMMA 6. *Let $\alpha \in \tilde{k}$ be of degree p over k. Then for all positive integers j there exists $\beta_j \in \sqrt{k}$ such that*

$$\operatorname{ord}(\alpha - \beta_j) \geqslant ((p-1)/p)^j \operatorname{ord} \alpha + (1/p + (p-1)/p^2 + \cdots + (p-1)^{j-1}/p^j)\Delta(\alpha).$$

Proof. We prove this by induction on j, the case $j = 1$ being covered by

Lemma 5. Applying this lemma to $\alpha - \beta_j \in \sqrt{k}$, we obtain $\beta_{j+1} \in \sqrt{k^{1/p}} = \sqrt{k}$ with the property that

$$\begin{aligned}\operatorname{ord}(\alpha - \beta_{j+1}) \geqslant (p-1)/p[((p-1)/p)^j \operatorname{ord}\alpha + (1/p + (p-1)/p^2 \\ + \cdots + (p-1)^{j-1}/p^j)\, \Delta(\alpha)] + \Delta(\alpha)/p \\ = ((p-1)/p)^{j+1} \operatorname{ord}\alpha + (1/p + \cdots + (p-1)^j/p^{j+1})\, \Delta(\alpha),\end{aligned}$$

as desired.

COROLLARY 1. *Assuming* $\operatorname{ord}\alpha \geqslant 0$, *we have that for all integers* $l > 1$ *there exists* $\beta \in \sqrt{k}$ *such that*

$$\operatorname{ord}(\alpha - \beta) \geqslant (1 - 1/l)\, \Delta(\alpha).$$

COROLLARY 2. *If the value group is archimedean we have, without the assumption that* $\operatorname{ord}\alpha \geqslant 0$, *that there exists* $\beta \in \sqrt{k}$ *such that order* $(\alpha - \beta) \geqslant \Delta(\alpha)$.

PROPOSITION 2. *Let* k *be a local field with* char $k = p > 0$. *Then for all* $\alpha \in \tilde{k}$ *with* $\operatorname{ord}\alpha \geqslant 0$ *and for all integers* $l > 1$ *there exists* $\beta \in \sqrt{k}$ *such that*

$$\operatorname{ord}(\alpha - \beta) \geqslant (1 - 1/l)\, \Delta(\alpha).$$

Proof. First, assume that every finite extension of k has degree a power of p and k is perfect. Then there exists a tower of fields $k = k_0 \subset k_1 \cdots \subset k_n$ with $[k_{i+1} : k_i] = p$ for $i = 0,\ldots, n-1$ and $\alpha \in k_n$. By Corollary 1 to Lemma 6, there exists $\gamma \in \sqrt{k_{n-1}} = k_{n-1}$ such that

$$\operatorname{ord}(\alpha - \gamma) \geqslant (1 - 1/2l)\, \Delta_{k_{n-1}}(\alpha) \geqslant (1 - 1/2l)\, \Delta_k(\alpha).$$

If γ' is a k conjugate of γ, then for a suitable k conjugate α' of α we have (cf. proof of Lemma 4)

$$\operatorname{ord}(\gamma' - \gamma) = \operatorname{ord}(\gamma' - \alpha' + \alpha' - \alpha + \alpha - \gamma) \geqslant (1 - 1/2l)\, \Delta_k(\alpha).$$

Thus, $\Delta_k(\gamma) \geqslant (1 - 1/2l)\, \Delta_k(\alpha)$. By induction on n we can find $\beta \in \sqrt{k} = k$ for which

$$\operatorname{ord}(\gamma - \beta) \geqslant (1 - 1/2l)\, \Delta_k(\gamma) \geqslant (1 - 1/2l)(1 - 1/2l)\, \Delta_k(\alpha).$$

This implies $\operatorname{ord}(\alpha - \beta) \geqslant (1 - 1/l)\, \Delta_k(\alpha)$ completing the proof under our first assumption.

Secondly, let us consider the case where k is merely assumed to be perfect. Let K be a maximal extension of k composed of finite extensions of degree prime to p, i.e., K is the fixed field of a pro-p-Sylow subgroup of G_k so that every finite extension of K has order a power of p. Hence, by our previous considerations there exists $\gamma \in \sqrt{K} = K$ such that

$$\operatorname{ord}(\alpha - \gamma) \geqslant (1 - 1/l)\, \Delta_K(\alpha).$$

Denote $K(\gamma)$ by J and the set of K monomorphisms $J \to \tilde{K} = \tilde{k}$ by A. We have

$$\begin{aligned}
&\operatorname{ord}([J : K]^{-1} \operatorname{trace}_{J/K}(\gamma) - \gamma) \\
&\quad = \operatorname{ord}([J : K]^{-1}(\operatorname{trace}_{J/K}(\gamma) - [J : K]\gamma)) \\
&\quad = \operatorname{ord} \sum_{\sigma \in A} (\sigma\gamma - \gamma) - \operatorname{ord}[J : K] \\
&\quad = \operatorname{ord} \sum_{\sigma \in A} (\sigma\gamma - \gamma) \geqslant \Delta_K(\gamma) \geqslant (1 - 1/l)\, \Delta_K(\alpha)
\end{aligned}$$

since $(p, [J : K]) = 1$. This proves the result in the second case.

In the general case where k is arbitrary, it follows from what we have already shown that there exists $\gamma \in \sqrt{k}$ such that

$$\operatorname{ord}(\alpha - \gamma) \geqslant (1 - 1/l)\, \Delta_{\sqrt{k}}(\alpha) \geqslant (1 - 1/l) \Delta_k(\alpha)$$

completing the proof of Proposition 2.

PROPOSITION 2′. *Let k be a local field such that either* (a) char $\bar{k} = 0$ *or* (b) char $k = p > 0$ *and* ord k^* *is an archimedean ordered group. Then for all* $\alpha \in k$ *there exists* $\beta \in \sqrt{k}$ *such that order* $(\alpha - \beta) \geqslant \Delta(\alpha)$.

Proof. The proof in case (b) is similar to that of Proposition 2, the reference to Corollary 1 of Lemma 6 being replaced by a corresponding reference to Corollary 2 of Lemma 6. Case (a) is even simpler: Only the argument employed in the second case of Proposition 2 need be used; it applies since for all finite extensions $J/K/k$ we have $\operatorname{ord}[J : K] = 0$.

3. PROOF OF THE THEOREM

Let $c \in k^t$ be fixed under G_k. We may assume ord $c \geqslant 0$. Then for all $\lambda \in \operatorname{ord} \tilde{k}^*$ and for all integers $l > 1$, there exists $\alpha \in \tilde{k}$ such that

$$\operatorname{ord}(\alpha - c) \geqslant w(k, \lambda, l)$$

where:

$$\begin{aligned}
w(k, \lambda, l) &= \lambda \text{ if char } \bar{k} = 0; \\
&= \lambda + (p/(p-1)^2) \operatorname{ord} p \text{ if char } k = 0 \text{ and char } \bar{k} = p > 0; \\
&= (1 - 1/l)^{-1} \lambda \text{ if char } k = p > 0.
\end{aligned}$$

If $\sigma \in G_k$,

$$\begin{aligned}\operatorname{ord}(\sigma\alpha - \alpha) &= \operatorname{ord}(\sigma\alpha - \sigma c + \sigma c - c + c - \alpha)\\ &= \operatorname{ord}(\sigma\alpha - \sigma c + c - \alpha) \geqslant \min \operatorname{ord}(\sigma(\alpha - c), c - \alpha)\\ &= \operatorname{ord}(c - \alpha) \geqslant w(k, \alpha, l).\end{aligned}$$

By Propositions 1, 2, and 2′, there exists $\alpha \in \sqrt{k}$ such that $\operatorname{ord}(\alpha - a) \geqslant \lambda$. Thus, $\operatorname{ord}(c - a) \geqslant \lambda$. Since λ was arbitrary, we must have $c \in \sqrt{\hat{k}}$. This proves our main result, the first assertion of the Theorem.

We now show that $\tilde{k}^s$ is dense in $\tilde{k}$. We may assume $\tilde{k}^s = k$ so that $\tilde{k} = \sqrt{k}$. Let $\alpha \in \tilde{k} = \sqrt{k}$. Then there exists a power q of $p = \operatorname{char} k$ (assuming as we may that $p > 0$) such that $\alpha^q = a \in k$. If $b \in k^*$ and if θ is a root of

$$X^q - bX - a = 0, \tag{*}$$

then $\theta \in \tilde{k}^s = k$, by differentiating the left side of (*). Also, $(\theta - \alpha)^q = b\theta$ so

$$\operatorname{ord}(\theta - \alpha) = 1/q(\operatorname{ord} b + \operatorname{ord} \theta). \tag{**}$$

Let $\lambda \in \operatorname{ord} \tilde{k}^*$ be arbitrary. Choose $b \in k^*$ so that[†]

(i) $\operatorname{ord} b > ((q - 1)/q) \operatorname{ord} a$ and

(ii) $\operatorname{ord} b > q\lambda - (\operatorname{ord} a)/q$.

By (i) and (*), $\operatorname{ord} \theta = (\operatorname{ord} a)/q$ (e.g., by Lemma 1). By this and (**) we obtain

$$\operatorname{ord}(\theta - \alpha) = 1/q(\operatorname{ord} b + (\operatorname{ord} a)/q).$$

Therefore, we may apply (ii) to obtain

$$\operatorname{ord}(\theta - \alpha) > \lambda.$$

Hence, $\tilde{k}^s$ is dense in $\tilde{k}$. This complete proof of the Theorem.

4. Further Results

Let k be a local field with $\operatorname{char} \bar{k} = 0$. By Proposition 2′, for all $\alpha \in \tilde{k}$ there exists $a \in k$ such that $\operatorname{ord}(\alpha - a) \geqslant \Delta(\alpha)$. If we remove the assumption on the characteristic of $\bar{k}$, then we have demonstrated modified versions of this inequality. Indeed, let p be a prime. Let F_p denote the set of $f \in \mathbf{Q}$ such that for all local fields k with $\operatorname{char} k = 0$ and $\operatorname{char} \bar{k} = p$ and for all $\alpha \in \tilde{k}$ there exists $a \in k$ with

$$\operatorname{ord}(\alpha - a) \geqslant \Delta(\alpha) - f \operatorname{ord} p. \tag{*}$$

Proposition 1 asserts that $p/(p - 1)^2 \in F_p$. By the opening remarks of Section 2, it is clear that F_p consists of nonnegative rational numbers. We now

[†] Here we use that ord is non-trivial.

show by means of examples that $0 \notin F_p$, i.e., the last term of (*) is not superfluous.

Let k be discrete valued with ord p of minimal positive value, e.g., $k = \mathbf{Q}_p$, the p-adic numbers. Set $f(X) = X^p + pX + p$ and let α be a zero of f. We claim $\Delta(\alpha) = 1/(p-1)$. Indeed, $f(X) = \sum_{j=0}^{p} f^{[j]}(\alpha)(X-\alpha)^j$ so that it suffices to prove that for every nonzero root β of $g(Z) = \sum_{j=0}^{p} f^{[j]}(\alpha)\, Z^j$, $\operatorname{ord}\beta = 1/(p-1)$.

$$f^{[0]}(\alpha) = f(\alpha) = 0,$$

$$f^{[1]}(\alpha) = f^{(1)}(\alpha) = pX^{p-1} + p,$$

$$f^{[j]}(\alpha) = \binom{p}{j} \alpha^{p-j} \qquad \text{for} \quad 2 \leqslant j \leqslant p.$$

Thus, $g(Z) = Z \sum_{i=0}^{p-1} c_i Z^i$ with $c_{p-1} = 1$, $\operatorname{ord} c_0 = \operatorname{ord} p$ and $\operatorname{ord} c_i > \operatorname{ord} p$ for $0 < i < p-1$. By a Newton polygon argument, we have $\operatorname{ord}\beta = 1/(p-1)$ for every root of $\sum_{i=0}^{p-1} c_i Z^i$ which establishes our claim. Since $\operatorname{ord}\alpha = \operatorname{ord} p/p$, $\operatorname{ord}(\alpha - a) \leqslant 0$ for every $a \in k$, equality being achieved if, and only if, $\operatorname{ord} a > 0$, i.e., $\operatorname{ord} a \geqslant \operatorname{ord} p$, e.g., $a = 0$. This shows that for $f \in \mathbf{Q}$ there exists $a \in \mathbf{Q}$ such that

$$\operatorname{ord}(\alpha - a) \geqslant \Delta(\alpha) - f \operatorname{ord} p$$

if, and only if, $f \geqslant (\operatorname{ord} p)/(p-1)$.

We have just shown that $f \in F_p$ implies $f \geqslant 1/p - 1$.

DEFINITION. $\Phi_p = \inf F_p \in \mathbf{R}$.

We have $1/p^i - \Phi_p \leqslant p/(p-1)^2$. It is of some interest to determine Φ_p in view of its absolute character; our last result is to show that the uppper bound we have obtained is not sharp.

LEMMA. *Let* $F = X^q + a_{q-1}X^{q-1} + \cdots + a_0 \in \tilde{k}[X]$. *Assume* $\operatorname{ord}\alpha \geqslant r$ *for all roots* α *of* f. *Set*

$$\begin{aligned} g &= f^{[q-1]} f^{[q-2]} - (3q/q-2) f^{[q-3]} \\ &= [(q-1)\, a_{q-1}^2 - 2q a_{q-2}]\, X + a_{q-1}a_{q-2} - (3q/q-2)\, a_{q-3}\,. \end{aligned}$$

Then there exists a root β *of* g *or* $f^{[q-1]}$ *for which* $\operatorname{ord}\beta \geqslant r - \operatorname{ord} p$, *provided* $\operatorname{ord} q \leqslant 2 \operatorname{ord} p$.

Proof. Normaliing ord so that $\operatorname{ord} p = 1$, we may assume $\operatorname{ord}(q-1) = 0$, $\operatorname{ord}(q-2) = 1$. Since a_{q-i} is the i-th elementary symmetric polynomial in the roots of f, $\operatorname{ord} a_{q-i} \geqslant ir$. $f^{[q-1]} = qX + a_{q-1}$; if the root $-a_{q-1}/q$ does not satisfy our conclusion, we have

$$\operatorname{ord} a_{q-1} < r - 1 + \operatorname{ord} q.$$

Hence,

$$\operatorname{ord}(q-1)\, a_{q-1}^2 - 2 \operatorname{ord} a_{q-1} < 2r - 2 + 2 \operatorname{ord} q$$

while

$$\operatorname{ord} 2qa_{q-2} \geqslant \operatorname{ord} 2 + \operatorname{ord} q + 2r,$$

so

$$\operatorname{ord} 2qa_{q-2} > \operatorname{ord}(q-1)\, a_{q-1}^2 .$$

It follows that for the root β of g,

$$\begin{aligned} \operatorname{ord} \beta &= \operatorname{ord}[a_{q-1}a_{q-2} - (3q/(q-2))\, a_{q-3}] - 2 \operatorname{ord} a_{q-1} \\ &\geqslant \min\{\operatorname{ord} a_{q-2} - \operatorname{ord} a_{q-1}, \operatorname{ord}(q/(q-2)) + \operatorname{ord} a_{q-3} - 2 \operatorname{ord} a_{q-1}\} \\ &\geqslant \min\{r + 1 - \operatorname{ord} q, \operatorname{ord} q - \operatorname{ord}(q-2) + r + 2 - 2 \operatorname{ord} q\} \\ &\geqslant \min\{r - 1, r - \operatorname{ord}(q-2)\} \geqslant r - 1, \end{aligned}$$

as desired.

COROLLARY. *Let $c \in \tilde{k}$ and $f = X^q + a_{q-1}X^{q-1} + \cdots + a_0 \in k[X]$. Assume* $\operatorname{ord}(\alpha - c) \geqslant r$ *for all roots α of f. Then there exists a root $\beta \in k$ of $f^{[q-1]}$ or g (as above) for which* $\operatorname{ord}(\beta - c) \geqslant r - 1$.

Proof. We have only to use that the linear operator $f \to f^{[q-1]}$ and the nonlinear (!) operator $f \to (q-2) f^{[q-1]} f^{[q-2]} - 3q f^{[q-3]}$ commute with translations.

PROPOSITION 3.

$$1 \leqslant \Phi_2 \leqslant 3/2 = \sum_{\substack{i=1 \\ i \neq 2}}^{\infty} (2^{-i} - 2^{i-1})^{-1}.$$

Proof. $p = 2$. It suffices to show that $\alpha \in \tilde{k}$ of degree $q = p^2$ over k implies that there exists $a \in k$ with $\operatorname{ord}(\alpha - a) \geqslant \Delta(\alpha) - 1/(p-1) = 1$ (instead of just $\operatorname{ord}(\alpha - a) \geqslant \Delta(\alpha) - (1/(p-1) + 1/(p^2 - p))$ as we had before in proving Lemma 4.) Let f be the monic irreducible polynomial for c over k. Let $f^{[q-1]}$ and g be as in the lemma and its corollary. Let $c = \alpha$. Then $\operatorname{ord}(\alpha' - c) \geqslant \Delta(\alpha)$ for all roots α' of f. Hence, there exists $a \in k$ (a root of $f^{[q-1]}$ or g) for which $\operatorname{ord}(\alpha - a) \geqslant \Delta(\alpha) - 1$, which establishes the proposition.

REFERENCES

1. J. TATE, p-divisible groups, Proceedings of a Conference on Local Fields, NUFFIC Summer School held at Driebergen, 1966, Springer–Verlag, New York, 1967.
2. C. F. GAUSS, *Werke*, Vol. 3, p. 112. Göttingen, Ges. d. Wiss. 1886.