ACTA ARITHMETICA
XXV (1974)

Some applications of a non-Archimedean analogue of Descartes' rule of signs*

by

M. SCHACHER and E. G. STRAUS (Los Angeles, Calif.)

1. Introduction. Given a field k with an extension field K, the statement that K is algebraic over k can be expressed as follows: For every $\theta \in K$, the powers $1, \theta, \theta^2, \ldots, \theta^n, \ldots$ are linearly dependent over k. If $[K:k] = d < \infty$ then, in fact, every $d+1$ terms $\theta^{n_0}, \theta^{n_1}, \ldots, \theta^{n_d}$ are inearly dependent over k. It is conceivable, however, that such linear dependences exist among fewer powers of θ for all $\theta \in k$, even when $[K:k] = \infty$. This motivates us to make the:

DEFINITION 1.1. The *multinomial degree* d' of K over k is the smallest positive integer so that for every $\theta \in K$ there exist integers $0 = n_0 < n_1 < n_2 < \ldots < n_l$; $l \leqslant d'$, with $\theta^{n_0}, \theta^{n_1}, \ldots, \theta^{n_l}$ linearly dependent over k. If no such d' exist we will say the multinomial degree of K/k is infinite.

To say that K/k has finite multinomial degree d' is equivalent to saying that K/k is algebraic with every element of K satisfying a polynomial over k (of unknown degree) involving at most $d'+1$ non-0 coefficients and that d' is the smallest number with this property. We are grateful to Professor I. N. Herstein for suggesting a version of Theorem 1.2.

As mentioned above, if K/k is finite-dimensional we have $d' \leqslant d = [K:k]$. If k is finite and K algebraic over k we have $d' = 1$ since every $\theta \in K$ is a root of unity. Similarly, if $\operatorname{char} k > 0$ and K is purely inseparable over k then $d' = 1$ since every $\theta \in K$ has a power in k.

It is the purpose of this note to prove that the examples cited are typical of those cases for which $d' < [K:k]$.

THEOREM 1.2. *Suppose K/k has multinomial degree $d' < \infty$. We have:*

(1) *If* $\operatorname{char} k = 0$ *then* $[K:k] = d < \infty$ *and* $d' = d$.

(2) *If* $\operatorname{char} k > 0$ *and K is algebraic over the prime field Z_p, then* $d' = 1$.

(3) *If* $\operatorname{char} k > 0$ *and K/k is purely inseparable, then* $d' = 1$.

(4) *If* $\operatorname{char} k > 0$, *$k$ contains a transcendental element over the prime*

* Research on this paper was supported in part by NSF Grant No. GP-28696.

field Z_p, then $d' = d_1$ where $d_1 = [K_1: k]$ with K_1 the maximal separable extension of k in K.

Remark. The theorem shows that d' as well as d is a multiplicative functional on the lattice of field extensions of a given field. We note that (1)–(4) can be restated as follows: If $d' < d$ then either k is algebraic over a finite field or K is a purely inseparable extension of a finite extension of k.

In case k is formally real and there exists $\theta \in K$ with more than l positive conjugates, it is clear from Descartes rule of signs that θ cannot be a root of a polynomial in $k[x]$ involving only $l+1$ non-0 coefficients. Hence in this case $d' > l$. In § 2 we extend Descartes' rule to non-Archimedean valuations to obtain a proof of Theorem 1.2.

In § 3 we apply Theorem 1.2 to division rings and in § 4 we discuss some open questions.

2. Descartes' rule of signs

Lemma 2.1. *Let k be a field with a non-Archimedean valuation v and let $f(x) = a_0 + a_1 x^{n_1} + \ldots + a_l x^{n_l} \in k[x]$. Then the set $\{|\theta|_v \mid f(\theta) = 0\}$ contains no more than l values.*

Proof. If we plot $y = \log|f(t)|_v$ as a function of $x = \log|t|_v$ where $|f(t)|_v = \max_i |a_i t^{n_i}|_v$ then the graph is polygonal, since the graph for each monomial is a straight line of slope n_i. This polygon is convex with no more than l vertices. If $f(\theta) = 0$, then $\log|\theta|_v$ must be the abscissa of one of the vertices, since at an interior point of an edge one monomial dominates all others.

Note that this lemma is usually proved in terms of the Newton polygon (see [4], 3.1.1). The use of the dual absolute value graph, given here, seems more intuitive.

Lemma 2.2. *Let $\theta_0, \theta_1, \ldots, \theta_l$ be $l+1$ distinct elements of k_v, the completion of k under the non-Archimedean valuation v. Then there exists a polynomial $P(x) \in k[x]$ so that $|P(\theta_i)|_v \neq |P(\theta_j)|_v$ for $i \neq j$.*

Proof. Let $\pi \in k_v$ satisfy $0 < |\pi| < 1$. There exists a polynomial

$$\overline{P}(x) = \sum_{j=0}^{l} \overline{a}_j x^j \in k_v[x]$$

such that $\overline{P}(\theta_i) = \pi^i$ for $i = 0, \ldots, l$. Since k is dense in k_v, there is a polynomial $P(x) = \sum_{j=0}^{l} a_j x^j \in k[x]$ with $|a_j - \overline{a}_j| < \varepsilon$ for $i = 0, 1, \ldots, l$. We conclude that

$$|P(\theta_i) - \overline{P}(\theta_i)| \leqslant \max_j |a_j - \overline{a}_j| \, |\theta_i|^j < \varepsilon \cdot c, \qquad c = \max_{i,j} |\theta_i|^j.$$

Then for sufficiently small ε we have $|P(\theta_i)| = |\overline{P}(\theta_i)| = |\pi|^i$, so the values $|P(\theta_i)|$ are distinct.

Note that if $K \subset k_v$, $[K: k] = d$ then the above argument gives us an indication about the distribution of elements in K whose conjugates over k have distinct v-values and which therefore have multinomial degree d.

Proof of Theorem 1.2. (1) Let K contain an element θ of degree d over k. If θ is algebraic over the rational field Q then there exist primes p so that the defining equation of θ over Q factors (mod p) into distinct linear factors ([3], th. 12, p. 289). Hence all of the conjugates of θ are distinct elements of the p-adic field Q_p. We extend the p-adic valuation to a non-Archimedean valuation v of k. Let $\theta = \theta_1, \theta_2, \ldots, \theta_d$ be the d distinct conjugates of θ which are in k_v. We can construct the polynomial $P(x)$ of Lemma 2.2 for $\theta_1, \ldots, \theta_d$. Then, by Lemma 2.1, $P(\theta) \in K(\theta)$ cannot satisfy a polynomial over k involving fewer than $d+1$ non-0 coefficients. Thus the multinomial degree of $k(\theta)$ over k satisfies $d' = d = [k(\theta): k]$.

If θ is transcendental over Q, then we first consider a minimal purely transcendental extension $Q(t_1, \ldots, t_s)$ of Q contained in k over which θ is algebraic. We pick a value $u_1 \in Q(t_2, \ldots, t_s)$ for t_1 so that the different conjugates of θ can be expressed as distinct formal power series in $t_1 - u_1$ with coefficients algebraic over $Q(t_2, \ldots, t_s)$. Using the valuation on these power series we again construct a non-Archimedean valuation v of k so that the defining equation for θ/k splits completely in k_v. As before we conclude $d' = d = [k(\theta): k]$.

We have already noted the proof of statements (2) and (3) of Theorem 1.2. To prove (4) we can assume that k contains transcendental elements over the prime field Z_p. Suppose θ is separable over k of degree d. We can find a minimal set of indeterminates $t_1, \ldots, t_s$ so that θ is algebraic over $Z_p(t_1, \ldots, t_s)$. If $s = 1$, we choose t with θ separable over $Z_p(t)$. By [3], th. 12, p. 289, there are infinitely many primes of $Z_p(t)$ over which the defining equation for θ splits completely. If $s > 1$, we pick a value u_1 of $t_1 \in Z_p(t_2, \ldots, t_s)$ so that the d distinct conjugates of θ can be expressed as power series in t_1 with coefficients algebraic over $Z_p(t_2, \ldots, t_s)$. Using the valuation for this power series we obtain a non-Archimedean valuation v of $Z_p(t_1, \ldots, t_s)$. Extending this valuation to a valuation v of k, we obtain a non-Archimedean prime so that the defining equation for θ over k has d distinct separable conjugates $\theta = \theta_1, \ldots, \theta_d$ in k_v. Using Lemmas 2.1 and 2.2, we again see $d' = d = [k(\theta): k]$ for the extension $k(\theta)/k$. This is enough to establish (4), and the proof of Theorem 1.2 is complete.

3. Division rings.

Unlike the case for fields, a division ring with finite multinomial degree over its center field k must be finite-dimensional over k. In fact we have:

THEOREM 3.1. *Let D be a division ring with center k having multinomial degree $d < \infty$ over k. Then $[D: k] = d^2$.*

Proof. By Theorem 1.2 the separable subfields of D have dimension at most d over k. Let M be a maximal separable subfield of D. Let D_0 be the centralizer of M in D. By [1], 4.3.2, D_0 is a division ring with center M. As D_0 is purely inseparable over M, we have $D_0 = M$ by [2], Corollary, p. 165. This says that M is a maximal subfield of D. Then [2], Prop. 2, p. 180, assures $[D: k] = [M: k]^2$. By Theorem 1.2 we have $[M: k] = d$, so $[D: k] = d^2$.

4. Some open questions. Theorem 1.2 suggests questions concerning the nature of those elements of a finite extension K of the field k whose multinomial degree is less than $d = [K: k]$. It is, of course, easy to see that the elements with multinomial degree $d' = 1$ are exactly those elements which have a positive power in k. For $d' > 1$ the situation is less obvious, however it might be reasonable to pose the following.

CONJECTURE 4.1. *If k is a field of characteristic 0 and θ is an element of multinomial degree d over k so that there exist $d+1$ multinomials $P_i(x) \in k[x]$; $i = 0, 1, \ldots, d$*

$$P_i(x) = a_{i0} + a_{i1}x^{m_{i1}} + \ldots + a_{id}x^{m_{id}}; \qquad a_{ij} \neq 0$$

where the different exponent vectors $\overline{m}_i = (m_{i1}, \ldots, m_{id})$ are not proportional then $[k(\theta^m): k] = d$ for some positive power m of θ.

The conjecture is false if $\operatorname{char} k > 0$. For example let θ be a solution of the equation $x^p - x - t = 0$ over $k = Z_p(t)$ where t is transcendental and $p > 2$. Then $[k(\theta^n): k] = p > 2$ for all $n = 1, 2, \ldots$, but θ satisfies infinitely many trinomials

$$x^{p^n} - x - (t + t^p + \ldots + t^{p^{n-1}}) = 0, \qquad n = 1, 2, \ldots$$

with non-proportional exponent vectors $(1, p^n)$ over k. If $\operatorname{char} k = 0$ and $[k(\theta): k] = d$ we might also ask the following:

QUESTION 4.2. What is the maximal number of terms in the sequence $\theta + n$; $n = 0, \pm 1, \pm 2, \ldots$ whose multinomial degree over k is $< d$?

If k is formally real and θ is totally real of degree d over k, then, as remarked before, it follows from Descartes' theorem that the elements $\theta + n$ for which all conjugates have the same sign must have multinomial degree d. Thus, if we order the conjugates of θ as $\theta_1 < \theta_2 < \ldots < \theta_d$, and $\theta + n$ has multinomial degree less than d, then $\theta_1 + n < 0 < \theta_d + n$ so that $-\theta_d < n < -\theta_1$, which gives us an upper bound $[\theta_d - \theta_1] + 1$ for the answer to Question 4.2 in this case. We know of no similar argument if the only valuations v for which all the conjugates of θ are in k_v are non-Archimedean.

References

[1] I. N. Herstein, *Noncommutative Rings*, Carus Monograph, 1968.
[2] N. Jacobson, *Structure of Rings*, Amer. Math. Soc., 1956.
[3] André Weil, *Basic Number Theory*, 1967.
[4] E. Weiss, *Algebraic Number Theory*, New York 1963.

UNIVERSITY OF CALIFORNIA
Los Angeles, California

Received on 12. 3. 1973 (387)