Werk

Titel: Zeros of polynomials with coefficients in the center of a division algebra.

Autor: Pritchard, F. Leon

PURL: https://resolver.sub.uni-goettingen.de/purl?365956996_0057|log12

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

manuscripta math. 57, 169 - 180 (1987)

manuscripta mathematica
© Springer-Verlag 1987

ZEROS OF POLYNOMIALS WITH COEFFICIENTS IN THE CENTER OF A DIVISION ALGEBRA

F. Leon Pritchard

In [1] it was shown that a polynomial of degree n with coefficients in the center of an associative division algebra, which is d-dimensional over its center, has either infinitely many or at most n^d zeros. In [4] it was shown that if P(x) is a polynomial of degree n with coefficients in a d-dimensional k-algebra A, with k algebraically closed, then the number of zeros of P(x) plus the number of zeros of the dominant part of P(x), both counted with appropriate multiplicity is either equal to n^d or the cardinality of k. In this paper we investigate the multiplicities and geometry of zeros of polynomials whose coefficients are in the center of a finite dimensional division algebra.

Conjugates are of central importance to this investigation and they are studied further in their own right.

We also show that there are no finite dimensional non-associative division algebras over an algebraically closed field, thus extending a classical result for associative (unital) division algebras.

1. INTRODUCTION. This paper will use freely the definitions and results of [4]. In particular, given a (not necessarily associative, commutative or unital) algebra A and a set X $A[X]$, the polynomial algebra over A with indeterminates in X, is defined.

If A has dimension n as a k-vector space and basis $\{e_i\}_{i=1}^n$ then we have:

PROPOSITION 1.1. ([4]) There is a canonical injective, graded algebra morphism

$$\chi : A\langle\chi\rangle \longrightarrow k[\chi_1, \ldots, \chi_n] \otimes_k A .$$

LEMMA 1.2. ([4]) For $P \in A\langle x\rangle$ put

$$\chi(P) = \sum_{i=1}^{n} P_i(x_1, \ldots, x_n) \otimes e_i .$$

Then $a = \sum_{i=1}^{n} a_i e_i \in A$ is a zero of P if and only if $(a_1, \ldots, a_n)$ is a common zero of the polynomials $P_1, \ldots, P_n$.

Let $P \in A\langle x\rangle$ and $a \in A$ be such that $P(a) = 0$. We define the multiplicity of a as a zero of P to be the multiplicity of $(a_1, \ldots, a_n)$ as a common zero of $P_1, \ldots, P_n$ as defined in [5] chapter IV. In the event that $(a_1, \ldots, a_n)$ is not an isolated zero of $P_1, \ldots, P_n$ we define the multiplicity of a as a zero of P to be infinite. This notion of multiplicity is independent of the basis chosen.

If A is an associative unital algebra we denote the group of units of A by $A^{\times}$.

2. POLYNOMIALS OVER AN ASSOCIATIVE DIVISION ALBEGRA.

In this section we will assume that D is some fixed associative, unital division algebra with center $Z(D) = K$. It will also be assumed that D is finite dimensional as a K-vector space. We will study the zeros in D of $f(x) \in K[x]$. We will first examine the situa-

tion where $f(x)$ is irreducible in $K[x]$. In addition it will be assumed that there exists $a \in D - K$ such that $f(a) = 0$.

LEMMA 2.1. $\{x \in D \mid f(x) = 0\} = \{dad^{-1} \mid d \in D^{\times}\}$.

Proof: Clearly $\{dad^{-1} \mid d \in D^{\times}\} \subseteq \{x \in D \mid f(x) = 0\}$. Let $b \in D^{\times}$ be such that $f(b) = 0$. The irreducibility of $f(x)$ implies that $K(a)$ is isomorphic to $K(b)$ by an isomorphism that sends a to b and leaves K fixed. By the Noether-Skolem Theorem [2] there exists $d \in D^{\times}$ such that $b = dad^{-1}$. ■

We will examine the mapping $\sigma_a : D^{\times} \longrightarrow D^{\times}$ given by $\sigma_a : x \longmapsto xax^{-1}$. For this purpose we must first establish some notational conventions. As a K-vector space let $\dim_K D = n$. Select a K-basis $\{e_i\}_{i=1}^{n}$ for D and identify D with n-dimensional K-affine space, $\mathbb{A}_K^n$, in the obvious manner. Let $a = \sum_{i=1}^{n} a_i e_i$. We also denote by x_i the i^{th} coordinate function of x.

Let D have structure coefficients $\{a_j^{i_1,i_2}\}_{i_1,i_2,j=1}^{n}$ with $e_{i_1} e_{i_2} = \sum_{j=1}^{n} a_j^{i_1,i_2} e_j$. Let $\bar{K}$ be the algebraic closure of K. It is also convenient at this point to set $\bar{D} = D \otimes_K \bar{K}$. $\bar{D}$ has canonical basis $\{E_i\}_{i=1}^{n}$ where $E_i = e_i \otimes_K 1$ and with respect to this basis $\bar{D}$ has structure coefficients $\{a_j^{i_1,i_2}\}$. We will assume $e_1 = 1$ and will identify D with its canonical image in $\bar{D}$.

It will be convenient to have a coordinate representation for σ_a. Let M be the matrix representation for the linear transformation given by right multipli-

cation by x. Let M_j be the matrix obtained from M by replacing the $j^{\underline{th}}$ column of M with $\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$. Let $P = \det M$ and Let $P_j = \det M_j$. Observe that $P, P_1, \ldots, P_n$ are polynomials in $x_1, \ldots, x_n$ and that the mapping $x \longmapsto x^{-1}$ is a rational mapping with $j^{\underline{th}}$ coordinate function P_j/P. Thus $\sigma_a : \mathbb{A}^n_K \longrightarrow \mathbb{A}^n_K$ by $x \longmapsto xax^{-1}$ is a rational mapping with $j^{\underline{th}}$ coordinate function:

$$q_j = \sum_{i_1,\ldots,i_4=1}^{n} (x_{i_1} a_{i_2} a_{i_3} a_j P_{i_4})/P .$$

In order to facilitate a study of the zeros of $f(x)$ it will be convenient to work with $\bar{K}$ and $\bar{D}$ instead of K and D. As with D we identify $\bar{D}$ with $\mathbb{A}^n_{\bar{K}}$, affine n-dimensional $\bar{K}$ space, in the obvious manner. Let $\sigma_a : \bar{D} \longrightarrow \bar{D}$ be the obvious extension of $\sigma_a : D \longrightarrow D$. σ_a is a rational mapping on $\bar{D}$ so we let $\mathcal{O}(P)$ be the set of points in $\mathbb{A}^n_{\bar{K}}$ such that $P(x) \neq 0$. It is evident that the Zeriski open set $\mathcal{O}(P)$ in $\mathbb{A}^n_{\bar{K}}$ corresponds precisely to the invertible elements of $\bar{D}$.

$\mathcal{O}(P)$ is thus an irreducible algebraic variety and σ_a induces the canonical mapping:

$$\tilde{\sigma}_a : \mathcal{O}(P) \longrightarrow \mathbb{A}^n_{\bar{K}} .$$

With our identifications we have:

$$\{x \in D \mid f(x) = 0\} \subseteq \operatorname{Im} \tilde{\sigma}_a \subseteq \overline{\operatorname{Im} \tilde{\sigma}_a} \subseteq \{x \in \bar{D} \mid f(x) = 0\}.$$

THEOREM 2.2. Let $f \in K[x]$ be irreducible and let $a \in D - K$ be such that $f(a) = 0$. Then the multiplicity of a as a zero of $f(x)$ is infinite.

Proof: Since $a \notin K$ the image of σ_a consists of more than one point. $\overline{\mathrm{Im}\,\tilde{\sigma}_a}$ is irreducible and consists of more than one point implies that the Krull dimension of $\overline{\mathrm{Im}\,\tilde{\sigma}_a}$ is greater than zero. Thus the theorem follows from the above discussion, the definition of infinite multiplicity and Theorem (5.1) [3]. ■

It is of interest, before continuing, to examine the dimension of $\overline{\mathrm{Im}\,\tilde{\sigma}_a}$. Set $m = \sqrt{n}$. (m is often referred to as the index of D.) Let $b \in \mathrm{Im}\,\tilde{\sigma}_a$. Then $b = xax^{-1}$ for some $x \in \mathcal{O}(P) \subseteq \bar{D}$ and thus $b^{-1} = xa^{-1}x^{-1}$ ($a \in D - K \Rightarrow a \neq 0$). For notation set $\tilde{\sigma}^{-1}(b) = W_b$. An easy calculation shows that x and y are in the fiber over the same point if and only if $y^{-1}x \in W_a$. (Note that $a = \tilde{\sigma}_a(1_D)$ and therefore $a \in \mathrm{Im}\,\tilde{\sigma}_a$.) Thus we have a morphism of varieties $\Phi_y : W_b \longrightarrow W_a$ by $\Phi_y : x \longrightarrow y^{-1}x$ for $y \in W_b$. Clearly Φ_y is an isomorphism. With $C_a = \{x \in \bar{D} \mid ax = xa\}$ $W_a = \mathcal{O}(P) \cap C_a$. C_a is a $\bar{K}$-vector space whose dimension is equal to the dimension of W_a as a variety. It is also immediate that W_a is irreducible. Set $V_a = \{x \in D \mid ax = xa\} = C_a \cap D$. C_a is determined by the homogeneous system of equations:

$$\left\{ \sum_{j=1}^{n} \left[\sum_{i=1}^{n} a_i (a_k^{i,j} - a_k^{j,i}) \right] x_j = 0 \right\}_{k=1}^{n} . \qquad (\bigstar)$$

Recall that a_i and $a_k^{i,j} \in K$. Since ★ can be solved by Gaussian elimination, there exists a basis for C_a consisting of elements of D. Since ★ also defines V_a as a subspace of D it follows that $\dim_K V_a = \dim_{\bar{K}} C_a$. It is also easily seen that V_a is precisely the maximum subfield of D that contains a, thus $\dim_K V_a = m$ ([2] page

459). We conclude that $\dim_{\overline{K}} C_a = m$.

THEOREM 2.3. For all $y \in \mathrm{Im}\,\tilde{\sigma}_a$ $\tilde{\sigma}_a^{-1}(y)$ has dimension m.

Proof: The proof follows from the above discussion. ■

THEOREM 2.4. $\overline{\mathrm{Im}\,\tilde{\sigma}_a}$ is an irreducible variety of dimension $n-m$.

Proof: We know $\overline{\mathrm{Im}\,\tilde{\sigma}_a}$ is irreducible. That the dimension of $\overline{\mathrm{Im}\,\tilde{\sigma}_a} = n-m$ follows from Theorem 2.3 and [5] page 60. ■

We will now consider the case of arbitrary $f(x) \in K[x]$. We start with the following:

LEMMA 2.5. Let $f(x)$ and $g(x)$ be irreducible elements of $K[x]$. Moreover, assume that neither $f(x)$ nor $g(x)$ possesses a zero in K. In this case there are exactly two possibilities:

(i) $\{x \in D \mid f(x) = 0\} = \{x \in D \mid g(x) = 0\}$

(ii) $\{x \in D \mid f(x) = 0\} \cap \{x \in D \mid g(x) = 0\} = \emptyset$.

Proof: The proof follows at once from Lemma 2.1. ■

We consider now the situation where f has one or more roots in K. We have a factorization:

$$f(x) = \ell_1^{N_1}(x) \cdot \ldots \cdot \ell_M^{N_M}(x) \cdot r(x)$$

where $N_i \in \mathbb{Z}^+$, $\ell_i = x - a_i$ ($a_i \in K$, $i \neq j \Rightarrow a_i \neq a_j$) and $r(x) \in K[x]$ has no roots in K. We will examine the multiplicity of a_i as a zero of $f(x)$. Set $h_i(x) = f(x + a_i)$ and $\tilde{f}_i(x) = \ell_1^{N_1}(x + a_i) \cdot \ldots \cdot \widehat{\ell_i^{N_i}(x + a_i)} \cdot \ldots \cdot \ell_M^{N_M}(x + a_i) \cdot r(x + a_i)$ where $\widehat{\ }$ means to omit the

indicated term. With this notation we have:

$$h_i(x) = x^{N_i}\tilde{f}_i(x), \quad \tilde{f}_i(a_i) \neq 0$$

and 0 is a root of $h_i(x)$ with the same multiplicity as the multiplicity of a_i as a root of $f(x)$.

We have two possibilities:

1. x^{N_i} has a non-trivial homogeneous zero in $\bar{D}$. In this case it is easily seen that 0 is a zero of $h_i(x)$ of infinite multiplicity.

2. x^{N_i} has no non-trivial homogeneous zeros in $\bar{D}$. In this case 0 is a zero of $h_i(x)$ of multiplicity N_i^n. (Recall that $n = \dim_K D$.) We define $N(D) = N$ if x^N has a non-trivial zero in $\bar{D}$ and if $M < N \Rightarrow x^M$ has no non-trivial zeros in $\bar{D}$ (N and $M \in \mathbb{Z}$). If for every $N \in \mathbb{Z}$ x^N has no non-trivial zeros in $\bar{D}$ we set $N(D) = \infty$.

With notation as above we collect together the results of this section:

THEOREM 2.6. Let D be an associative unital division algebra with center $Z(D) = K$ and with dimension n over K. In addition let $f \in K[x]$ and $a \in D$ such that $f(a) = 0$. If $a \notin K$ then a is a root of $f(x)$ of infinite multiplicity. If $a \in K$ then let m be the smallest integer such that $(x - a)^m \mid f(x)$. If $m \geq N(D)$ then a is a root of $f(x)$ of infinite multiplicity. Otherwise, if $m < N(D)$ then a is a root of $f(x)$ of multiplicity m^n.

3. CONJUGATES IN AN ASSOCIATIVE UNITAL ALGEBRA.

In the previous section we examined the multiplicities of zeros of a polynomial $f(x)$ with coefficients in the center of an associative unital division algebra.

We said very little about the number of zeros of f(x). This problem was studied by Herstein [1]. The principal results are:

THEOREM 3.1. ([1]) If in an (associative, unital) division ring D an element $a \in D$ has only a finite number of conjugates in D then it has only one conjugate, that is, a is in Z, the center of D.

From Theorem 3.1 the following corollary is almost immediate:

COROLLARY 3.2. ([1]) Let D be an (associative,unital) division ring with center Z and suppose that $p(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ where the α_i are in Z, has one root in D that is outside of Z. Then p(x) has an infinite number of roots in D.

We will now give an alternative proof of 3.1. As does Herstein's proof, our proof will make use of Wedderburn's Theorem. We feel, however, that our proof is considerably simpler than the proof given in [1].

Proof of 3.1: Fix $a \in D$. Assume $\{ dad^{-1} \mid d \in D^{\times} \}$ is finite $\Rightarrow$ there exist $b_1, \ldots, b_m$ such that $\{ dad^{-1} \mid d \in D^{\times} \} = \{ b_1, \ldots, b_m \}$. Assume $m > 1$. Set $B_i = \{ d \in D \mid da = b_i d \}$ for $i = 1, \ldots, m$. Clearly each B_i is a vector space over the center of D and $i \neq j \Rightarrow B_i \cap B_j = 0$. By assumption $D = \bigcup_{i=1}^{m} B_i$. Since D is a vector space over its center it is an elementary exercise in linear algebra to show that D must be finite as a set. Thus by Wedderburn's Theorem [2] page 462, D must be a field and we arrive at a contradiction. ■

We will now look at conjugates in a slightly different setting.

Let A be an associative, unital algebra with center $Z(A) = K$. We assume K to be algebraically closed. As a K-vector space, set $\dim_K A = n$. Let A have a K-vector space basis $\{e_i\}_{i=1}^n$ and structure coefficients $\{a_k^{i,j}\}_{i,j,k=1}^n$. As before, identify A with $\mathbb{A}_K^n$.

LEMMA 3.3. *$A^\times$ is a Zariski open subset of $\mathbb{A}_K^n$.*

Proof: To every $x \in A$ there is associated $R_x : A \longrightarrow A$ a K-vector space homomorphism given by right multiplication by x. Clearly $x \in A^\times \Rightarrow R_x$ is an isomorphism. Similarly if R_x is an isomorphism then $x \in A^\times$ since x^{-1} is given by $R_x^{-1}(1)$. The openness of $A^\times$ now follows since R_x being an isomorphism is equivalent to the matrix representation of R_x having nonzero Jacobian determinant. ■

We are now ready to prove:

THEOREM 3.4. *If a is an element of A and if a has only a finite number of conjugates in A then a has only one conjugate in A.*

Proof: First note that $A^\times \neq \emptyset$. Now suppose that $\{xax^{-1} \mid x \in A^\times\}$ is a finite set. Set $\{xax^{-1} \mid x \in A^\times\} = \{b_1, \ldots, b_m\}$. Set $B_i = \{x \in A \mid xa = b_i x\}$. Clearly each B_i is a K-vector space and $\dim_K A > \dim_K B_i$ for each i. Thus $C_i = B_i \cap A$ is a proper subvariety of $A^\times$. Now $x \in A^\times \Rightarrow xax^{-1} = b_i$ for some i, therefore $xa = b_i x$ $\Rightarrow x \in C_i$. Thus we have $A^\times = \bigcup_{i=1}^m C_i$. $A^\times$ is a Zariski

open subset of $\mathbb{A}^n_K$ and thus irreducible, but each C_i is a proper subvariety and so we have arrived at a contradiction, and the lemma is established. ■

4. NONASSOCIATIVE DIVISION ALGEBRAS.

We will conclude with some results on nonassociative algebras.

From this point on A will be called a K-algebra (or simply algebra) of arity m if A is a K-vector space and A is equipped with a K-vector space homomorphism $\mu : \bigotimes_K^m A \longrightarrow A$ defining the m-ary multiplication on A. If $\mu = 0$ then A is said to be a null algebra. We shall assume $m \geq 2$. For a more complete discussion see [4].

For $j = 1, \ldots, m$ and any $a_1, \ldots, a_{m-1} \in A$, call the K-vector space morphism $A \longrightarrow A$ given by $x \longmapsto \mu(a_1 \otimes \ldots \otimes a_{j-1} \otimes x \otimes a_j \otimes \ldots \otimes a_{m-1})$ a j^{th} place multiplication. The multiplication algebra $\mathcal{M}(A)$ of A is defined to be the associative, unital (binary) subalgebra of $\mathrm{End}_K A$ which is generated by id_A and all j^{th} place multiplications for various j.

DEFINITION 4.1. A K-algebra A is called a division algebra if the nonzero elements of $\mathcal{M}(A)$ form a group (under multiplication in $\mathcal{M}(A)$).

THEOREM 4.2. Let A be a finite dimensional algebra over an algebraically closed field K. If the nonzero elements of the multiplication algebra are K-vector space automorphisms of A, then A has dimension one as a K-vector space or else A is a null algebra.

Proof: We assume that A is not a null algebra and that A has dimension n as a K-vector space with $n > 1$. We

assume that A has a K-vector space basis $\{e_j\}_{j=1}^n$ and corresponding structure coefficients $\left\{ a_i^{j_1,\ldots,j_m} \right\}_{i,j_1,\ldots,j_m=1}^n$.

Let $a_1, \ldots, a_{m-1}$ be generic elements of A with $a_i = \sum_{j=1}^n a_j^{(i)} e_j$. We define a K-vector space endomorphism M on A by $M(x) = \mu(a_1 \otimes \ldots \otimes a_{\ell-1} \otimes x \otimes a_\ell \otimes \ldots \otimes a_{m-1})$, for suitable choice of ℓ so that for some $a_1, \ldots, a_{m-1}$ M is not identically zero. Such a choice is always possible since A is not a null algebra. Fix i, $1 \leqslant i \leqslant m-1$ and select $a_1, \ldots, a_{m-1}$ so that M is not the zero endomorphism on A. Fix $a_1, \ldots, a_{i-1}$, $a_{i+1}, \ldots, a_{m-1}$ as above and consider a_i as an indeterminate. Each choice of $a_i = a$ determines a K-vector space endomorphism on A that we shall denote by M_a. M_a has matrix representation with i, j^{th} component:

$$\sum_{j_1,\ldots,j_{m-1}=1}^n a_{j_1}^{(1)} \cdot \ldots \cdot a_{j_{m-1}}^{(m-1)} a_i^{j_1,\ldots,j_{\ell-1},j,j_\ell,\ldots,j_{m-1}}.$$

The determinate $\det(M_a)$ is either identically zero or else it is a homogeneous polynomial of degree n in $a_1^{(i)}, \ldots, a_n^{(i)}$. In either case $\det(M_a) = 0$ has a nontrivial solution since K is algebraically closed. Let $\bar{a} = \sum_{j=1}^n \bar{a}_j^{(i)} e_j$ be a nonzero solution to $\det(M_a) = 0$. Since the nonzero elements of $\mathcal{M}(A)$ are K-vector space automorphisms on A we must have that $M_{\bar{a}}$ is the zero endomorphism on A. Select $b \in A$ so that M_b is a K-vector space automorphism on A and select $c \in A$, $c \neq 0$. Define a K-

vector space endomorphism N on A by $N(x) = M_x(c)$. $N(b) = M_b(c) \neq 0$ so N must not be identically zero. But $N(\bar{a}) = M_{\bar{a}}(c) = 0$, so N is not a K-vector space automorphism and thus we have a contradiction to our assumption that all nonzero elements of $\mathcal{M}(A)$ are K-vector space automorphisms. Therefore A must either be the null algebra or A must have dimension one as a K-vector space. ■

COROLLARY 4.3. If A is a finite dimensional algebra over an algebraically closed field K and if A is a division algebra then either A has dimension one as a K-vector space or A is a null algebra.

ACKNOWLEDGMENT. I would like to thank Helmut Röhrl for suggesting many of the problems discussed in this paper. I would also like to thank him for his many helpful discussions and comments.

REFERENCES.

[1] HERSTEIN, I.N., Conjugates in division rings, Proc. AMS 7, 1021-1023 (1956)

[2] HUNGERFORD, T.W., Algebra, Holt, Rinehart and Winston, 1974

[3] PRITCHARD, F.L., On the multiplicity of zeros of polynomials over arbitrary finite dimensional k-algebras, Manuscripta Mathematica 49, 267-292 (1985)

[4] RÖHRL, H., On the zeros of polynomials over arbitrary finite dimensional algebras, Manuscripta Mathematica 25, 359-390 (1978)

[5] SHAFAREVICH, I.R., Basic Algebraic Geometry, Springer Verlag, 1977

F. Leon Pritchard
Department of Mathematics
Western Illinois University
Macomb, Illinois 61455, U.S.A.

(Received September 17, 1986)