ISSN 1561-8323 (Print)
ISSN 2524-2431 (Online)

МАТЕМАТИКА
MATHEMATICS

UDC 512.552
https://doi.org/10.29235/1561-8323-2024-68-5-359-364

Received 23.04.2024
Поступило в редакцию 23.04.2024

Alina G. Goutor, Sergey V. Tikhonov

Belarusian State University, Minsk, Republic of Belarus

ROOTS OF POLYNOMIALS OVER DIVISION RINGS

(Communicated by Academician Vyacheslav I. Yanchevskiĭ)

Abstract. In this article, we study the properties of polynomials over division rings. Formulas for finding roots of polynomials which are the products of linear factors are obtained. These formulas generalize the known results for quaternion algebras. As known, if a minimal polynomial of a conjugacy class A in a noncommutative division ring is quadratic, then any polynomial having two roots in A vanishes identically on A. We show that in the case of a conjugacy class with minimal polynomial of larger degree, the situation is completely different. For any conjugacy class with minimal polynomial of degree >2, we construct a quadratic polynomial with infinitely many roots in this class, but there also are infinitely many elements in this class which are not the roots of this polynomial.

Keywords: division ring, roots of polynomials, quaternion algebra, minimal polynomial

For citation. Goutor A. G., Tikhonov S. V. Roots of polynomials over division rings. *Doklady Natsional'noi akademii nauk Belarusi = Doklady of the National Academy of Sciences of Belarus*, 2024, vol. 68, no. 5, pp. 359–364. https://doi.org/10.29235/1561-8323-2024-68-5-359-364

А. Г. Гутор, С. В. Тихонов

Белорусский государственный университет, Минск, Республика Беларусь

КОРНИ МНОГОЧЛЕНОВ С КОЭФФИЦИЕНТАМИ В КОЛЬЦАХ С ДЕЛЕНИЕМ

(Представлено академиком В. И. Янчевским)

Аннотация. В работе изучены свойства многочленов с коэффициентами в кольцах с делением. Получены формулы для нахождения корней многочленов, являющихся произведением линейных множителей, обобщающие известные результаты для кватернионных алгебр. Как известно, если минимальный многочлен класса сопряженности A в некоммутативном кольце с делением является квадратичным, то любой многочлен, имеющий два корня в A, обнуляется тождественно на A. В работе показано, что в случае класса сопряженности с минимальным многочленом большей степени ситуация принципиально другая. Для любого класса сопряженности с минимальным многочленом степени >2 построен квадратичный многочлен, имеющий бесконечно много корней в этом классе, при этом в данном классе сопряженности имеется бесконечно много элементов, не являющихся корнями такого многочлена.

Ключевые слова: кольцо с делением, корни многочленов, алгебра кватернионов, минимальный многочлен

Для цитирования. Гутор, А. Г. Корни многочленов с коэффициентами в кольцах с делением / А. Г. Гутор, С. В. Тихонов // Докл. Нац. акад. наук Беларуси. – 2024. – Т. 68, № 5. – С. 359–364. https://doi.org/10.29235/1561-8323-2024-68-5-359-364

Introduction and preliminary results. In this paper, we study polynomials over division rings. Let D be an associative division ring. Let also $D[x]$ denote the polynomial ring in one variable x over D, where x commutes elementwise with D. The coefficients of such polynomials may not commute with elements of the ring. Polynomials in $D[x]$ are added in the obvious way, and multiplied according to the rule

$$(a_n x^n + \cdots + a_0)(b_m x^m + \cdots + b_0) = (c_{m+n} x^{m+n} + \cdots + c_0),$$

where $c_k = \sum_{i+j=k} a_i b_j$. For references on polynomial rings over division rings, see [1, Ch. 5, §16; 2]. The degree of $P(x) \in D[x]$ is defined in the usual way. For a polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in D[x]$$

and an element $a \in D$, we define $P(a)$ to be the element

$$a_n a^n + a_{n-1} a^{n-1} + \cdots + a_1 a + a_0.$$

An element $a \in D$ is said to be a (right) root of $P(x)$ if $P(a) = 0$. The noncommutative form of the Remainder Theorem says that an element $a \in D$ is a root of a nonzero polynomial $P(x)$ iff $x - a$ is a right divisor of $P(x)$ in $D[x]$ (see, e. g., [1, Prop. 16.2]).

For $a \in D$, the set

$$[a] := \{dad^{-1} | d \in D \setminus \{0\}\}$$

will be called the conjugacy class of a. The centralizer of a is defined as

$$Z(a) := \{b \in D | ab = ba\}.$$

Over a field, a polynomial of degree n has at most n distinct roots. Over a division ring this is no longer true, but by Gordon–Motzkin theorem [1, Th. 16.4], a polynomial of degree n in $D[x]$ has roots in at most n conjugacy classes of D, moreover, if $P(x) = (x - a_1)\ldots(x - a_n)$, where $a_1, \ldots, a_n \in D$, then any root of $P(x)$ is conjugate to some a_i. Note that from $P(x) = L(x)R(x) \in D[x]$ it does not follow that $P(a) = L(a)R(a)$ (see Proposition below). In particular, if a is a root of $L(x)$, then a is not necessarily a root of $P(x)$.

The problem of finding the roots of a polynomial over a division ring has been investigated in ring theory and applied mathematics. The most studied is the case of polynomials over Hamilton's quaternion algebra $\mathbb{H}$. In analogy to field theory, the notion of a (right) algebraically closed division ring R is defined. This is equivalent to saying that every polynomial in $R[x]$ splits completely into a product of linear factors in $R[x]$. By Niven–Jacobson theorem [1, Th. 16.14], the quaternion division algebra over a real-closed field is algebraically closed. Baer's theorem [1, Th. 16.15] says that noncommutative centrally finite (right) algebraically closed division rings are precisely the division rings of quaternions over real-closed fields. In [3], a formula was found for roots of any quadratic polynomial in $\mathbb{H}[x]$. This formula was generalized to any quaternion algebra in [4] and [5]. In [6], it was shown that the roots of any polynomial in $\mathbb{H}[x]$ are roots of the real companion polynomial. In [7], it was presented an algorithm for finding all roots of a polynomial in $\mathbb{H}[x]$ using the real companion polynomial. In [8], a few of these results were generalized to the case of any central division algebra. Recall that a central division algebra is a division algebra which is finite dimensional over its center. A complete method for finding the roots of all polynomials over an octonion division algebra was described in [9].

In [10], it was presented the following explicit formula describing roots of a product of linear factors in $\mathbb{H}[x]$.

T h e o r e m 1 [10, Th. 4]. *Let $P(x) = (x - q_n)\ldots(x - q_1)$, where $q_1, \ldots, q_n \in \mathbb{H}$. If the conjugacy classes $[q_k]$ are distinct, then the polynomial $P(x)$ has exactly n roots ζ_k which are related to the elements q_k as follows:*

$$\zeta_k = \overline{P_k}(q_k) q_k (\overline{P_k}(q_k))^{-1}; k = 1, \ldots, n,$$

$$P_k(x) := \begin{cases} 1, \mathit{if}\, k = 1, \\ (x - q_{k-1})\ldots(x - q_1), \mathit{otherwise} \end{cases}$$

and $\overline{P_k}(x)$ is the conjugate polynomial of $P_k(x)$.

In theorem 9 below, we generalize this formula for the case of any division ring. This is the first aim of this paper.

Let F be the center of a division ring D. If a is a root of a polynomial $f(x) \in F[x]$, then any element from the conjugacy class $[a]$ is a root of $f(x)$. The conjugacy class A is called algebraic over F if one (and hence all) of its elements is algebraic over F. If A is algebraic over F, then the minimal polynomial of A is, by definition, the minimal polynomial of any element from A.

In the case of a quadratic minimal polynomial, there is the following

T h e o r e m 2 [1, Lm. 16.17]. *Let D be a division ring with center F, and let A be a conjugacy class of D which has a quadratic minimal polynomial $\lambda(x)$ over F. If $P(x) \in D[x]$ has two roots in A, then $P(x) \in D[x]\lambda(x)$ and $P(x)$ vanishes identically on A.*

This means that a polynomial over a quaternion division algebra may have two different types of roots: isolated and spherical roots. A root q of $P(x)$ is called spherical if q is not central and for every $d \in [q]$ we have $P(d) = 0$. A root q is called isolated if the conjugacy class $[q]$ contains no other root of $P(x)$.

The second aim of this paper is to show that in the case of a conjugacy class with minimal polynomial of bigger degree the situation is completely different. More precisely, we proved the following

T h e o r e m 3. *Let D be a noncommutative division ring with the center F, $a \in D$ an algebraic over F element with minimal polynomial $\lambda(x)$ of degree $n > 2$. Then there exists a quadratic polynomial $P(x) \in D[x]$ such that*

1. $P(x)$ has infinitely many roots in the conjugacy class $[a]$,

2. There are infinitely many elements in $[a]$ which are not roots of $P(x)$,

3. $\lambda(x)$ does not divide $P(x)$.

In the proof of Theorem 3 we will use the following statements.

T h e o r e m 4 [1, Th. 16.6]. *Let D be a division ring with center F and A a conjugacy class of D which is algebraic over F with minimal polynomial $f(x) \in F[x]$. A polynomial $P(x) \in D[x]$ vanishes identically on A iff $P(x) \in D[x]f(x)$.*

T h e o r e m 5 [1, Th. 16.11; 2, Th. 4]. *If a polynomial $P(x) \in D[x]$ has two distinct roots in a conjugacy class of D, then it has infinitely many roots in that class.*

P r o p o s i t i o n [1, Pr. 16.3]. *Let D be a division ring and let $P(x) = L(x)R(x) \in D[x]$. Let $d \in D$ be such that $h := R(d) \neq 0$. Then*

$$P(d) = L(hdh^{-1})R(d).$$

In particular, if d is a root of $P(x)$ but not of $R(x)$, then hdh^{-1} is a root of $L(x)$.

P r o o f o f T h e o r e m 3. Let $a \in D$ be an element with minimal polynomial $\lambda(x)$ of degree $n > 2$. Let also $d \in D$ be an element such that d does not commute with a. Let $q = dad^{-1}$ and $b = (q - a)q(q - a)^{-1}$. Then $q \neq a$ and $q \in [a]$. By Proposition, q is a root of the polynomial $P(x) := (x - b)(x - a)$.

Since a is also a root of $P(x)$, then by Theorem 5, $P(x)$ has infinitely many roots in $[a]$. Moreover, since the degree of $\lambda(x)$ is bigger than 2, then $\lambda(x)$ does not divide $P(x)$. Hence by Theorem 4, $P(x)$ does not vanish identically on $[a]$.

Suppose that $tat^{-1} \in [a]$ is not a root of $P(x)$. This means that $tat^{-1} \neq a$ and

$$(tat^{-1} - a)tat^{-1}(tat^{-1} - a)^{-1} \neq b$$

by Proposition.

Note that

$$(tat^{-1} - a)tat^{-1}(tat^{-1} - a)^{-1} = (ta - at)a(ta - at)^{-1}.$$

Let $z \in Z(a)$, $t_1 = t + z$ and $q_1 = t_1at_1^{-1}$. Then

$$(q_1 - a)q_1(q_1 - a)^{-1} = (t_1at_1^{-1} - a)t_1at_1^{-1}(t_1at_1^{-1} - a)^{-1} =$$

$$= (t_1a - at_1)a(t_1a - at_1)^{-1} = ((t + z)a - a(t + z))a((t + z)a - a(t + z))^{-1} = (ta - at)a(ta - at)^{-1} \neq b.$$

Thus q_1 is not a root of $P(x)$ by Proposition.

Now let $z_1 \in Z(a)$, $z_1 \neq z$. Note that the centralizer $Z(a)$ is infinite by [2, Th. 3]. Let also $t_2 = t + z_1$ and $q_2 = t_2 a t_2^{-1}$. Then q_2 is also not a root of $P(x)$.

Assume that $q_1 = q_2$. Then

$$(t+z)a(t+z)^{-1} = (t+z_1)a(t+z_1)^{-1} \Leftrightarrow (t+z_1)^{-1}(t+z)a = a(t+z_1)^{-1}(t+z) \Leftrightarrow$$

$$\Leftrightarrow (t+z_1)^{-1}(t+z_1+(z-z_1))a = a(t+z_1)^{-1}(t+z_1+(z-z_1)) \Leftrightarrow$$

$$\Leftrightarrow a + (t+z_1)^{-1}(z-z_1)a = a + a(t+z_1)^{-1}(z-z_1) \Leftrightarrow$$

$$\Leftrightarrow (t+z_1)^{-1}(z-z_1)a = a(t+z_1)^{-1}(z-z_1) \Leftrightarrow (t+z_1)^{-1}a(z-z_1) = a(t+z_1)^{-1}(z-z_1) \Leftrightarrow$$

$$\Leftrightarrow (t+z_1)^{-1}a = a(t+z_1)^{-1} \Leftrightarrow a(t+z_1) = (t+z_1)a \Leftrightarrow at = ta.$$

This gives a contradiction since t does not commute with a. Then $q_1 \neq q_2$. Hence any $z \in Z(a)$ defines the element $(t+z)a(t+z)^{-1} \in [a]$ which is not a root of $P(x)$ and all such elements are distinct. Since the centralizer $Z(a)$ is infinite, then there are infinitely many elements in $[a]$ which are not roots of $P(x)$. □

R e m a r k 1. *In the notation of the proof of Theorem 3, let*

$$b_1 = (tat^{-1} - a)tat^{-1}(tat^{-1} - a)^{-1}.$$

The polynomials $(x-b)(x-a)$ *and* $(x-b_1)(x-a)$ *have infinitely many roots in the conjugacy class* $[a]$, *but* a *is the unique common root of these polynomials.*

Roots of polynomials. It seems to us that the following lemma may be a known result, but we have not found an exact reference. For the reader's convenience, we provide a proof here.

L e m m a. *Let D be a division ring. Let also*

$$P(x) = (x-d_n)\ldots(x-d_1),$$

where $d_1, \ldots, d_n \in D$. *If the conjugacy classes* $[d_k]$ *are distinct, then the polynomial* $P(x)$ *has exactly n roots and any root of* $P(x)$ *is conjugate to some* d_i.

P r o o f. By Gordon–Motzkin theorem [1, Th. 16.4], the roots of $P(x)$ lie in n conjugacy classes of D and any root of $P(x)$ is conjugate to some d_i. Let $d \in D$ be a root of $P(x)$, then $P(x) = L(x)(x-d)$ for some $L(x) \in D[x]$. By Proposition, all roots of $P(x)$ different from d are conjugate to roots of $L(x)$. Since the conjugacy classes $[d_k]$ are distinct and $\deg(L(x)) = n-1$, then by Gordon–Motzkin theorem, $L(x)$ has no roots in $[d]$. Thus $P(x)$ has only one root in each conjugacy class. □

T h e o r e m 6. *Let D be a division ring with center F. Let also*

$$P(x) = (x-d_n)\ldots(x-d_1),$$

where $d_1, \ldots, d_n \in D$. *Assume that* $d_1, \ldots, d_{n-1}$ *are algebraic over F. Let also* $f_i(x)$ *be the minimal polynomial of* d_i, $i = 1, \ldots, n-1$. *If the conjugacy classes* $[d_k]$ *are distinct, then the polynomial* $P(x)$ *has exactly n zeros* ζ_k *which are related to the elements* d_k *as follows:*

$$\zeta_k = P_k(d_k)d_k(P_k(d_k))^{-1};\ k = 1, \ldots, n,$$

$$P_k(x) := \begin{cases} 1, & \text{if } k = 1, \\ S_1(x)\ldots S_{k-1}(x), & \text{otherwise}, \end{cases}$$

where $S_i(x) \in D[x]$ *is such that* $f_i(x) = S_i(x)(x-d_i)$, $i = 1, \ldots, n-1$.

P r o o f. Since $S_i(x)$ has coefficients in the field $F(d_i)$, then

$$f_i(x) = S_i(x)(x-d_i) = (x-d_i)S_i(x)$$

for $i = 1, \ldots, n-1$. Note that

$$P(x)P_k(x) = (x-d_n)\ldots(x-d_1)S_1(x)\ldots S_{k-1}(x) = (x-d_n)\ldots(x-d_k)f_{k-1}(x)\ldots f_1(x).$$

Since $f_{k-1}(x)\ldots f_1(x) \in F[x]$, then d_k is a root of the polynomial $P(x)P_k(x)$. Note that for $i = 1, \ldots, k-1$, $d_k \notin [d_i]$, so d_k is not a root of $f_i(x)$ by Dickson's Theorem [1, Th. 16.8]. Hence d_k is not a root of $f_{k-1}(x)\ldots f_1(x)$. Then d_k is not a root of $P_k(x)$. Indeed,

$$(x - d_{k-1})\ldots(x - d_1)P_k(x) = (x - d_{k-1})\ldots(x - d_1)S_1(x)\ldots S_{k-1}(x) = f_{k-1}(x)\ldots f_1(x)$$

and if d_k is a root of $P_k(x)$, then d_k is a root of $f_{k-1}(x)\ldots f_1(x)$.

Hence by Proposition, $P_k(d_k)d_k(P_k(d_k))^{-1}$ is a root of $P(x)$ for $k = 1, \ldots, n$. By Lemma, $P(x)$ has no other roots. □

In the notation of Theorem 6, we have the following

C o r o l l a r y. *Let D be a division ring with center F, $d_1, d_2 \in D$ such that the conjugacy classes $[d_1]$ and $[d_2]$ are distinct. Assume that d_1 is algebraic over F. Let also $f(x)$ be the minimal polynomial of d_1 and $S(x) \in D[x]$ such that $f(x) = S(x)(x - d_1)$. Then*

$$(x - d_2)(x - d_1) = (x - d)(x - S(d_2)d_2(S(d_2))^{-1}),$$

where $d = (d_1 - S(d_2)d_2(S(d_2))^{-1})d_1(d_1 - S(d_2)d_2(S(d_2))^{-1})^{-1}$.

P r o o f. Let $P(x) := (x - d_2)(x - d_1)$. By Theorem 6, $d_3 := S(d_2)d_2(S(d_2))^{-1}$ is a root of $P(x)$. Then $x - d_3$ is a right divisor of $P(x)$ and $P(x) = (x - d)(x - d_3)$ for some $d \in D$. Since d_1 is a root of $P(x)$ and $d_1 \neq d_3$, then by Proposition,

$$d = (d_1 - d_3)d_1(d_1 - d_3)^{-1} = (d_1 - S(d_2)d_2(S(d_2))^{-1})d_1(d_1 - S(d_2)d_2(S(d_2))^{-1})^{-1}. \ \square$$

R e m a r k 2. *The formula from the previous corollary allows to change the order of factors in products of monic linear polynomials. This formula generalizes formulas for Hamilton's quaternion algebra from [11, Lm. 1] (see also [10, Th.7]).*

E x a m p l e. Let F be a field, $\mathrm{char}(F) \neq 2$. Let also Q be a quaternion division algebra over F.

Assume that $d_1, d_2 \in Q$, $[d_1] \neq [d_2]$. If $d_1 \notin F$ then the minimal polynomial of d_1 is $(x - \overline{d_1})(x - d_1)$, where $\overline{d_1}$ is the conjugate of d_1. Hence in the notation of Corollary, $S(x) = x - \overline{d_1}$. Then

$$S(d_2)d_2(S(d_2))^{-1} = (d_2 - \overline{d_1})d_2(d_2 - \overline{d_1})^{-1}.$$

Simple computations show that

$$(d_1 - S(d_2)d_2(S(d_2))^{-1})d_1(d_1 - S(d_2)d_2(S(d_2))^{-1})^{-1} = (d_2 - \overline{d_1})d_1(d_2 - \overline{d_1})^{-1}.$$

Thus

$$(x - d_2)(x - d_1) = (x - hd_1h^{-1})(x - hd_2h^{-1}),$$

where $h = d_2 - \overline{d_1}$ (compare with the formula from [11, Lm. 1]).

References

1. Lam T. Y. *A first course in noncommutative rings. Graduate Texts in Mathematics 131*. New York, Springer-Verlag, 2001. https://doi.org/10.1007/978-1-4419-8616-0

2. Gordon B., Motzkin T. S. On the zeros of polynomials over division rings. *Transactions of the American Mathematical Society*, 1965, vol. 116, pp. 218–226. https://doi.org/10.1090/S0002-9947-1965-0195853-2

3. Huang L., So W. Quadratic formulas for quaternions. *Applied Mathematics Letters*, 2002, vol. 15, no. 5, pp. 533–540. https://doi.org/10.1016/s0893-9659(02)80003-9

4. Abrate M. Quadratic formulas for generalized quaternions. *Journal of Algebra and its Applications*, 2009, vol. 8, no. 3, pp. 289–306. https://doi.org/10.1142/s0219498809003308

5. Chapman A. Quaternion quadratic equations in characteristic 2. *Journal of Algebra and its Applications*, 2015, vol. 14, no. 3, art. 1550033. https://doi.org/10.1142/s0219498815500334

6. Serodio R., Pereira E., Vitoria J. Computing the zeros of quaternion polynomials. *Computers and Mathematics with Applications*, 2001, vol. 42, no. 8–9, pp. 1229–1237. https://doi.org/10.1016/s0898-1221(01)00235-8

7. Janovska D., Opfer G. A note on the computation of all zeros of simple quaternionic polynomials. *SIAM Journal of Numerical Analysis*, 2010, vol. 48, no. 1, pp. 244–256. https://doi.org/10.1137/090748871

8. Chapman A., Machen C. Standard polynomial equations over division algebras. *Advances in Applied Clifford Algebras*, 2017, vol. 27, pp. 1065–1072. https://doi.org/10.1007/s00006-016-0740-4

9. Chapman A. Polynomial equations over octonion algebras. *Journal of Algebra and its Applications*, 2020, vol. 19, no. 6, art. 2050102. https://doi.org/10.1142/s0219498820501029

10. Falcão M. I., Miranda F., Severino R., Soares M. J. Mathematica tools for quaternionic polynomials. *Computational science and its applications. ICCSA 2017*. 2017, part II, pp. 394–408. https://doi.org/10.1007/978-3-319-62395-5_27

11. Serodio R., Siu L.-S. Zeros of quaternion polynomials. *Applied Mathematics Letters*, 2001, vol. 14, no. 2, pp. 237–239. https://doi.org/10.1016/s0893-9659(00)00142-7

Information about the authors

Goutor Alina G. – Senior Lecturer. Belarusian State University (4, Nezavisimosti Ave., 220030, Minsk, Republic of Belarus). E-mail: goutor@bsu.by.

Tikhonov Sergey V. – Ph. D. (Physics and Mathematics), Head of the Department. Belarusian State University (4, Nezavisimosti Ave., 220030, Minsk, Republic of Belarus). E-mail: tikhonovsv@bsu.by. ORCID: 0000-0002-2597-7964.

Информация об авторах

Гутор Алина Геннадьевна – ст. преподаватель. Белорусский государственный университет (пр. Независимости, 4, 220030, Минск, Республика Беларусь). E-mail: goutor@bsu.by.

Тихонов Сергей Викторович – канд. физ.-мат. наук, заведующий кафедрой. Белорусский государственный университет (пр. Независимости, 4, 220030, Минск, Республика Беларусь). E-mail: tikhonovsv@bsu.by. ORCID: 0000-0002-2597-7964.