
МАТЕМАТИЧЕСКАЯ ЛОГИКА, АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

MATHEMATICAL LOGIC, ALGEBRA AND NUMBER THEORY

УДК 512.552

СУЩЕСТВОВАНИЕ МНОГОЧЛЕНОВ С ЗАДАНЫМИ КОРНЯМИ НАД НЕКОММУТАТИВНЫМИ КОЛЬЦАМИ

А. Г. ГУТОР¹⁾

¹⁾Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь

Аннотация. Рассмотрен вопрос существования многочленов с заданными корнями над ассоциативными некоммутативными кольцами. Показано, что для произвольных n элементов ассоциативного кольца с делением найдется многочлен степени n , корнями которого они являются. Определены достаточные условия существования такого многочлена для элементов произвольного (не обязательно с делением) ассоциативного кольца с единицей. Для многочленов, определенных над кольцом квадратных матриц над полем, получен критерий существования многочлена второй степени с заданными корнями, а также приведены примеры построения многочленов с заданными корнями.

Ключевые слова: кольцо; кольцо с делением; многочлен; кольцо квадратных матриц.

Благодарность. Автор выражает признательность кандидату физико-математических наук, доценту С. В. Тихонову за интересные идеи и полезные замечания.

Образец цитирования:

Гутор АГ. Существование многочленов с заданными корнями над некоммутативными кольцами. *Журнал Белорусского государственного университета. Математика. Информатика*. 2025;1:6–13.
EDN: DDWGOW

For citation:

Goutor AG. The existence of polynomials with given roots over non-commutative rings. *Journal of the Belarusian State University. Mathematics and Informatics*. 2025;1:6–13. Russian.
EDN: DDWGOW

Автор:

Алина Геннадьевна Гутор – старший преподаватель кафедры интеллектуальных методов моделирования механико-математического факультета.

Author:

Alina G. Goutor, senior lecturer at the department of intelligent modelling methods, faculty of mechanics and mathematics.
goutor7@gmail.com
<https://orcid.org/0009-0001-4586-0480>

THE EXISTENCE OF POLYNOMIALS WITH GIVEN ROOTS OVER NON-COMMUTATIVE RINGS

A. G. GOUTOR^a

^aBelarusian State University, 4 Niezaliezhnasci Avenue, Minsk 220030, Belarus

Abstract. This paper studies the problem of the existence of polynomials with given roots over associative non-commutative rings. It is shown that for arbitrary n elements of an associative division ring there exists a polynomial of degree n whose roots are these elements. The sufficient conditions for the existence of such a polynomial for elements of an arbitrary (not necessarily division) associative ring with unity are determined. For polynomials defined over a ring of square matrices over a field, a criterion for the existence of a second-degree polynomial with given roots is obtained, and examples of constructing polynomials with given roots are given.

Keywords: ring; division ring; polynomial; ring of square matrices.

Acknowledgements. The author express gratitude to PhD (physics and mathematics), docent S. V. Tikhonov for interesting ideas and useful comments.

Введение

В работе исследуется вопрос существования многочленов с заданными корнями в кольцах многочленов над ассоциативными кольцами с единицей.

Пусть R – ассоциативное кольцо с единицей. Будем рассматривать многочлены вида

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \quad a_k \in R, \quad (1)$$

где переменная x коммутирует с коэффициентами a_k . Кольцо таких многочленов будем обозначать через $R[x]$. Сложение многочленов из $R[x]$ определяется привычным образом, а умножение выполняется по правилу

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

где $c_k = \sum_{i+j=k} a_i b_j$. Степень многочлена вида (1) также определяется привычным образом, она равна n , если $a_n \neq 0$.

Для $a \in R$ определим

$$P(a) = a_n a^n + a_{n-1} a^{n-1} + \dots + a_1 a + a_0.$$

Назовем $a \in R$ (правым) корнем $P(x)$, если $P(a) = 0$. Известно, что $a \in R$ будет корнем ненулевого многочлена $P(x)$ тогда и только тогда, когда $x - a$ является правым делителем $P(x)$ в $R[x]$ [1, propos. 16.2], т. е. $P(x) = F(x)(x - a)$ для некоторого многочлена $F(x)$ из $R[x]$.

Вопрос нахождения корней многочленов над кольцами с делением исследуется в теории колец и прикладной математике.

Наиболее изученным является случай многочленов с коэффициентами в алгебре $\mathbb{H}$ гамильтоновых кватернионов (см., например, [2–6] и др.). Известно, что любой многочлен из $\mathbb{H}[x]$ разлагается в произведение линейных множителей. В работе [7] получены формулы для нахождения корней таких многочленов в специальных случаях. В статье [2] представлена формула для нахождения корней квадратного многочлена в $\mathbb{H}[x]$. Эта формула была обобщена на случай произвольной алгебры кватернионов в публикациях [3; 4]. В работе [5] показано, что корни любого многочлена из $\mathbb{H}[x]$ являются корнями так называемого многочлена-компаньона с действительными коэффициентами. В статье [8] приведен алгоритм нахождения всех корней многочлена из $\mathbb{H}[x]$ с использованием многочленов-компаньонов. Некоторые из этих результатов были обобщены на случай произвольной алгебры с делением в публикации [6]. В работе [9] получены формулы для нахождения корней многочленов с коэффициентами над кольцами с делением в специальных случаях, а также показано, что нахождение корней многочленов над кольцом с делением размерности над центром более 4 усложняется по сравнению с их нахождением в алгебре кватернионов.

Однако важной является и обратная задача – нахождение многочленов с заданными корнями. В статье [10] рассмотрен вопрос существования многочленов с заданными корнями в кольцах многочленов над кольцами матриц. В частности, показано, что для двух матриц не всегда существует квадратный многочлен, имеющий в качестве своих корней эти матрицы. Отметим, что для любых элементов $x_1, \dots, x_n$ коммутативного кольца всегда существует многочлен $(x - x_1) \dots (x - x_n)$ степени n , корнями которого являются данные элементы. Однако для некоммутативных колец ситуация принципиально иная. Задача существования многочленов с заданными корнями над кольцами с делением рассматривалась также в работах [11; 12]. Ниже построен пример, когда не существует многочленов с заданными корнями.

Случай произвольного ассоциативного кольца с единицей

Сформулируем лемму о корнях многочленов над ассоциативными кольцами с единицей. Аналогичное утверждение имеется для ассоциативного кольца с делением (см., например, [1, propos. 16.3]). Его доказательство легко обобщается на случай ассоциативных колец с единицей. Для удобства читателя приведем данное доказательство.

Лемма 1. Пусть R – ассоциативное кольцо с единицей и $P(x) = L(x)Q(x) \in R[x]$, $a, d \in R$ такое, что элемент $h := Q(d)$ обратим. Тогда

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

В частности, если hdh^{-1} – корень многочлена $L(x)$, то d – корень многочлена $P(x)$.

Доказательство. Пусть $L(x) = \sum a_i x^i$, тогда $P(x) = \sum a_i x^i Q(x) = \sum a_i Q(x) x^i$. Имеем

$$P(d) = \sum a_i Q(d) d^i = \sum a_i h d^i h^{-1} h = \sum a_i (hdh^{-1})^i h = L(hdh^{-1})Q(d).$$

Из леммы 1 следует, что элемент d будет корнем произведения, если он является корнем правого множителя либо если корнем левого множителя является элемент hdh^{-1} (с нужным h). Однако, поскольку в произвольном кольце могут присутствовать делители нуля, у произведения могут быть и другие корни.

Пусть заданы различные элементы $x_1, \dots, x_n \in R$. Положим, что $Q_1(x) = x - x_1$. Далее для $i \in \{1, \dots, n-1\}$ в случае, когда $Q_i(x_{i+1})$ – обратимый элемент в R , рекурсивно определим

$$Q_{i+1}(x) = \left(x - Q_i(x_{i+1})x_{i+1} \left(Q_i(x_{i+1}) \right)^{-1} \right) Q_i(x).$$

Получаем следующую теорему.

Теорема 1. Если для любого $i \in \{1, \dots, n-1\}$ элемент $Q_i(x_{i+1})$ обратим в R , то $Q_n(x_i) = 0$ для любого $i = 1, \dots, n$.

Доказательство. Используя индукцию, докажем, что $x_1, \dots, x_i$ являются корнями $Q_i(x)$, $i = 1, \dots, n$. Действительно, при $i = 1$ элемент x_1 будет корнем многочлена $Q_1(x) = x - x_1$. Пусть утверждение верно для i , иными словами, предположим, что $x_1, \dots, x_i$ являются корнями $Q_i(x)$. Докажем утверждение для $i + 1$, т. е. покажем, что $x_1, \dots, x_{i+1}$ – корни многочлена $Q_{i+1}(x)$. Имеем

$$Q_{i+1}(x) = \left(x - Q_i(x_{i+1})x_{i+1} \left(Q_i(x_{i+1}) \right)^{-1} \right) Q_i(x).$$

По предположению индукции $x_1, \dots, x_i$ – корни правого множителя $Q_i(x)$, а следовательно, и всего произведения, т. е. многочлена $Q_{i+1}(x)$. Осталось показать, что элемент x_{i+1} также является корнем многочлена $Q_{i+1}(x)$. Это следует из леммы 1.

Иными словами, в случае обратимости элементов $Q_i(x_{i+1})$ в R для любых различных элементов $x_1, \dots, x_n \in R$ найдется такой многочлен из $R[x]$ степени n , что $x_1, \dots, x_n$ будут его корнями.

Замечание 1. Если в условиях теоремы 1 верно равенство $Q_i(x_{i+1}) = 0$ для некоторого i , то можно взять $Q_{i+1}(x) = Q_i(x)$. Если нужен многочлен степени $i + 1$, то можно взять, например, $Q_{i+1}(x) = xQ_i(x)$. Таким образом, и в этом случае также найдется многочлен из $R[x]$ степени, меньшей либо равной n , корнями которого будут различные элементы $x_1, \dots, x_n \in R$.

Теорема 2. Пусть D – ассоциативное кольцо с делением. Тогда для любых различных элементов $x_1, \dots, x_n \in D$ существует такой многочлен $F(x)$ степени n , что $F(x_i) = 0$ для любого $i = 1, \dots, n$.

Доказательство. Доказательство данной теоремы следует из теоремы 1 и замечания 1.

Итак, построение многочлена из теоремы 2 происходит по следующему алгоритму нахождения многочлена степени n , корнями которого являются различные фиксированные элементы $x_1, \dots, x_n$. Сначала рассматривается многочлен $F_1(x) = x - x_1$, корнем которого является x_1 . Затем по нему строится многочлен $F_2(x) = (x - x_2)(x - x_1)$ так, чтобы его корнями были x_1 и x_2 . Для этого x_2 берется равным $(x_2 - x_1)x_2(x_2 - x_1)^{-1}$. Для построения многочлена $F_3(x)$, корнями которого являются x_1, x_2 и x_3 , необходимо проверить, будет ли x_3 корнем многочлена $F_2(x)$. Если будет, то $F_3(x) = xF_2(x)$, в противном случае $F_3(x) = (x - x_3)F_2(x)$, где x_3 берется из леммы 1 так, чтобы x_3 был корнем $F_3(x)$, а именно $x_3 = F_2(x_3)x_3(F_2(x_3))^{-1}$. Таким образом,

$$F_3(x) = \left(x - \left((x_3 - (x_2 - x_1)x_2(x_2 - x_1)^{-1})(x_3 - x_1) \right) x_3 \left((x_3 - (x_2 - x_1)x_2(x_2 - x_1)^{-1})(x_3 - x_1) \right)^{-1} \right) \times \\ \times \left(x - (x_2 - x_1)x_2(x_2 - x_1)^{-1} \right) (x - x_1).$$

Далее построение продолжается аналогично до тех пор, пока не будет получен многочлен $F(x) = F_n(x)$, корнями которого являются $x_1, \dots, x_n$.

Отдельно рассмотрим случай многочленов второй степени с двумя заданными различными корнями x_1 и x_2 .

Перейдем к вопросу: «Когда для конкретных элементов x_1 и x_2 ассоциативного кольца с единицей R существует многочлен вида $F(x) = x^2 + a_1x + a_0$, корнями которого являются x_1 и x_2 ?»

Рассмотрим уравнение

$$x^2 + a_1x + a_0 = 0 \quad (2)$$

и предположим, что x_1 и x_2 — его решения.

Подставляя в уравнение (2) сначала x_1 , затем x_2 , а потом отнимая от одного равенства другое, получаем [10, р. 2]

$$x_1^2 + a_1x_1 + a_0 = 0, \quad x_2^2 + a_1x_2 + a_0 = 0, \\ x_1^2 - x_2^2 + a_1(x_1 - x_2) = 0. \quad (3)$$

Последнее равенство перепишем следующим образом:

$$a_1(x_1 - x_2) = x_2^2 - x_1^2. \quad (4)$$

Лемма 2. Для элементов x_1 и x_2 найдется уравнение вида (2), имеющее решения x_1 и x_2 , тогда и только тогда, когда существует элемент a_1 , удовлетворяющий равенству (4).

Доказательство. Очевидно, что если для x_1 и x_2 существует уравнение вида (2), то a_1 удовлетворяет равенству (4). Докажем лемму 2 в обратную сторону. Пусть для данных x_1 и x_2 существует элемент a_1 , удовлетворяющий равенству (4). Это равносильно тому, что $x_1^2 + a_1x_1 = x_2^2 + a_1x_2$. Если теперь a_0 взять равным $-x_1^2 - a_1x_1 = -x_2^2 - a_1x_2$, то x_1 и x_2 будут решениями уравнения (2).

Заметим, что если существует $(x_1 - x_2)^{-1}$, то найдется уравнение вида (2) такое, что x_1 и x_2 будут его решениями (это следует и из теоремы 1). В данном случае a_1 однозначно выражается из равенства (4), а a_0 также однозначно находится из одного из равенств (3).

Если для некоторых элементов x_1 и x_2 существует уравнение вида (2), решениями которого они являются, то для них существует и уравнение степени $n > 2$, решениями которого они являются. Данное уравнение можно получить путем умножения уравнения (2), например, на x^{n-2} .

Теорема 3. Для элементов $x_1 \neq x_2$ ассоциативного кольца с единицей R достаточным условием существования уравнения степени n вида

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0, \quad (5)$$

решениями которого они являются, будет невырожденность одного из следующих элементов: $x_1 - x_2$, $x_1^2 - x_2^2, \dots, x_1^{n-1} - x_2^{n-1}$.

Доказательство. Пусть, например, элемент $x_1 - x_2$ обратим и $a_i, i = 2, \dots, n-1$, — произвольные элементы кольца R . Положим, что

$$a_1 = (x_2^n - x_1^n)(x_1 - x_2)^{-1} - a_{n-1}(x_1^{n-1} - x_2^{n-1})(x_1 - x_2)^{-1} - \dots - a_2(x_1^2 - x_2^2)(x_1 - x_2)^{-1}.$$

Тогда

$$a_1(x_1 - x_2) = x_2^n - x_1^n - a_{n-1}(x_1^{n-1} - x_2^{n-1}) - \dots - a_2(x_1^2 - x_2^2).$$

Положим также, что

$$a_0 = -a_1x_1 - a_2x_1^2 - \dots - a_{n-1}x_1^{n-1} - x_1^n = -a_1x_2 - a_2x_2^2 - \dots - a_{n-1}x_2^{n-1} - x_2^n.$$

Тогда x_1 и x_2 – решения уравнения $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$. Таким образом, искомое уравнение найдено.

Аналогичные рассуждения справедливы и в случае обратимости одного из следующих элементов: $x_1^2 - x_2^2, \dots, x_1^{n-1} - x_2^{n-1}$.

Как проверить, существует ли уравнение вида (2), решениями которого являются элементы x_1 и x_2 , если элемент $x_1 - x_2$ необратим? Ответ на этот вопрос в случае, когда R – кольцо квадратных матриц над полем, рассмотрен в следующем разделе.

Случай кольца квадратных матриц над полем

Пусть R – кольцо квадратных матриц над полем. Как показывает пример из публикации [10, р. 3], существуют такие матрицы x_1 и x_2 , что не найдется уравнения второй степени из $R[x]$, решениями которого являлись бы эти матрицы. Еще один пример подобного типа приводится ниже (см. пример 3). Для кольца квадратных матриц над полем получены следующие критерии существования уравнения второй степени с заданными решениями.

Теорема 4. Пусть R – кольцо квадратных матриц порядка k над полем. Для x_1 и x_2 из R найдется уравнение вида (2), решениями которого они являются, тогда и только тогда, когда ранг матрицы $(x_1 - x_2)^T$ равен рангу матрицы $\left((x_1 - x_2)^T \left| \begin{pmatrix} x_2^T \\ x_1^T \end{pmatrix}^2 - \begin{pmatrix} x_1^T \\ x_2^T \end{pmatrix}^2 \right) \right.$, полученной дописыванием строк матрицы $\begin{pmatrix} x_2^T \\ x_1^T \end{pmatrix}^2 - \begin{pmatrix} x_1^T \\ x_2^T \end{pmatrix}^2$ справа к строкам матрицы $(x_1 - x_2)^T$.

Доказательство. Напомним, что ввиду леммы 2 для матриц x_1 и x_2 найдется уравнение вида (2), решениями которого они являются, тогда и только тогда, когда существует матрица a_1 , удовлетворяющая равенству (4). Транспонируем равенство (4):

$$(x_1 - x_2)^T a_1^T = \begin{pmatrix} x_2^T \\ x_1^T \end{pmatrix}^2 - \begin{pmatrix} x_1^T \\ x_2^T \end{pmatrix}^2. \quad (6)$$

С учетом предыдущего равенства заметим, что j -й элемент i -го столбца матрицы $\begin{pmatrix} x_2^T \\ x_1^T \end{pmatrix}^2 - \begin{pmatrix} x_1^T \\ x_2^T \end{pmatrix}^2$ получается путем умножения j -й строки матрицы $(x_1 - x_2)^T$ на i -й столбец матрицы a_1^T . Введем обозначения $a_1^T = (q_1, \dots, q_k)$, где q_i – i -й столбец матрицы a_1^T , и $\begin{pmatrix} x_2^T \\ x_1^T \end{pmatrix}^2 - \begin{pmatrix} x_1^T \\ x_2^T \end{pmatrix}^2 = (b_1, \dots, b_k)$, где b_i – i -й столбец матрицы $\begin{pmatrix} x_2^T \\ x_1^T \end{pmatrix}^2 - \begin{pmatrix} x_1^T \\ x_2^T \end{pmatrix}^2$. Из равенства (6) получаем следующие уравнения для нахождения столбцов матрицы a_1^T :

$$(x_1 - x_2)^T q_i = b_i, \quad i = 1, \dots, k.$$

Теорема Кронекера – Капелли говорит о том, что все эти системы совместны (относительно q_i) тогда и только тогда, когда ранг матрицы $(x_1 - x_2)^T$ равен рангам матриц $\left((x_1 - x_2)^T | b_i \right)$ для любого i . Следовательно, матричное уравнение (6) имеет решение (существует a_1^T) тогда и только тогда, когда ранг матрицы $(x_1 - x_2)^T$ равен рангу матрицы $\left((x_1 - x_2)^T \left| \begin{pmatrix} x_2^T \\ x_1^T \end{pmatrix}^2 - \begin{pmatrix} x_1^T \\ x_2^T \end{pmatrix}^2 \right) \right.$. Если найдется матрица a_1^T , то по ней с помощью транспонирования также найдется матрица a_1 . Далее можно найти матрицу a_0 из одного из равенств (3), а значит, в этом случае найдется уравнение вида (2) такое, что x_1 и x_2 будут его решениями.

Данное утверждение можно сформулировать и в терминах исходных матриц.

Следствие 1. Для квадратных матриц x_1 и x_2 порядка k найдется уравнение вида (2), решениями которого они являются, тогда и только тогда, когда ранг матрицы $x_1 - x_2$ равен рангу матрицы $\left(\begin{pmatrix} x_1 - x_2 \\ x_2^2 - x_1^2 \end{pmatrix} \right)$, полученной дописыванием строк матрицы $x_2^2 - x_1^2$ снизу к строкам матрицы $x_1 - x_2$.

Доказательство. Транспонируя матрицы из теоремы 4, получаем матрицы из следствия 1. Поскольку ранг матриц при транспонировании сохраняется, имеем требуемое.

Пример 1. Приведем пример таких комплексных матриц порядка 2, что не существует обратной матрицы к матрице $x_1 - x_2$, но при этом существует уравнение вида (2), решениями которого являются x_1 и x_2 . Подходящими матрицами будут, например, $x_1 = \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix}$, $x_2 = \begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix}$, где α и β – ненулевые комплексные числа, при этом $\alpha \neq \beta$. Поскольку $x_1^2 = x_2^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $x_1^2 - x_2^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, то ранг матрицы $x_1 - x_2$ совпадает с рангом матрицы $\begin{pmatrix} x_1 - x_2 \\ x_2^2 - x_1^2 \end{pmatrix}$. Из равенства (4) находим, что $a_1 = \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix}$, где c – любое ненулевое комплексное число. Из одного из равенств (3) получаем, что a_0 – нулевая матрица. Итак, данным матрицам x_1 и x_2 соответствует континуум уравнений вида (2), решениями которых они являются.

В приведенном примере матрицы x_1 и x_2 были вырожденными. Построим пример с невырожденными матрицами x_1 и x_2 .

Пример 2. Рассмотрим матрицы $x_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $x_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Матрица $x_1 - x_2 = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ имеет ранг 1. Далее получаем $x_1^2 = x_2^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, значит, $x_1^2 - x_2^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Следовательно, ранг матрицы $x_1 - x_2$ совпадает с рангом матрицы $\begin{pmatrix} x_1 - x_2 \\ x_2^2 - x_1^2 \end{pmatrix}$. Таким образом, существует уравнение вида (2), решениями которого являются x_1 и x_2 . Из равенства (4) найдем a_1 :

$$a_1 \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Введем обозначение $a_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Подставляя его в предыдущее равенство, находим

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} a-b & -a+b \\ c-d & -c+d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Итак, получаем, что a_1 – любая матрица порядка 2, у которой $a = b$ и $c = d$. Пусть $a_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, тогда из равенств (3) имеем $a_0 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Заметим, что для матриц x_1 и x_2 также найдется бесконечное число уравнений вида (2), решениями которых они являются.

Предложение 1. Если для двух квадратных матриц x_1 и x_2 уравнение (4) имеет решение a_1 при условии, что не существует $(x_1 - x_2)^{-1}$, то таких решений уравнения (4) бесконечно много (а значит, бесконечно много и уравнений вида (2) с корнями x_1 и x_2).

Доказательство. Посмотрим на равенство (4) как на матричное уравнение относительно a_1 , тогда оно имеет вид $XA = B$, где $X = a_1$, а A и B – известные матрицы. Введем обозначения $a_1 = \begin{pmatrix} q_1 \\ \dots \\ q_k \end{pmatrix}$, где

q_i – строки матрицы a_1 , и $x_2^2 - x_1^2 = \begin{pmatrix} b_1 \\ \dots \\ b_k \end{pmatrix}$, где b_i – строки матрицы $x_2^2 - x_1^2$. Тогда матричное уравнение (4) равносильно системе уравнений

$$q_i (x_1 - x_2) = b_i, \quad i = 1, \dots, k. \quad (7)$$

Известно, что матричное уравнение (4) имеет решение, значит, и уравнения системы (7) имеют решения. Также известно, что матрица $x_1 - x_2$ каждого уравнения системы (7) является вырожденной, следовательно, у системы уравнений (7), а значит, и у матричного уравнения (4) бесконечно много решений.

Приведем пример, показывающий, что достаточные условия из теоремы 3 не являются необходимыми условиями для существования уравнения третьей степени, решениями которого были бы данные

две квадратные матрицы, а также то, что квадратные матрицы, не удовлетворяющие достаточным условиям из теоремы 3, существуют.

Пример 3. Рассмотрим матрицы $x_1 = \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix}$, $x_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Заметим, что матрицы $x_1 - x_2 = \begin{pmatrix} 0 & 0 \\ 1 & -2 \end{pmatrix}$ и $x_1^2 - x_2^2 = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$ являются вырожденными. Значит, не выполнены достаточные условия существования уравнения третьей степени, решениями которого были бы x_1 и x_2 . Также не существует уравнения второй степени для данных матриц, поскольку ранг матрицы $\begin{pmatrix} x_1 - x_2 \\ x_2^2 - x_1^2 \end{pmatrix}$ равен 2, т. е. не совпадает с рангом матрицы $x_1 - x_2$. Покажем, что, несмотря на это, для x_1 и x_2 существует уравнение вида (5) при $n = 3$. Подставив в уравнение (5) при $n = 3$ сначала x_1 , затем x_2 , а потом отняв от одного равенства другое, получим

$$a_2 \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} + a_1 \begin{pmatrix} 0 & 0 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -1 & 2 \end{pmatrix}.$$

Пусть a_2 – нулевая матрица. Матрицу a_1 будем искать в виде $a_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Тогда

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -1 & 2 \end{pmatrix}.$$

Отсюда получаем, что $b = 0$, $d = -1$, a и c – любые комплексные числа. Положим, что $a_1 = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$.

Подставляя a_1 , a_2 и x_2 в уравнение (5) при $n = 3$, находим a_0 . Полученное уравнение третьей степени, решениями которого являются x_1 и x_2 , имеет вид

$$x^3 + \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} x = 0.$$

Пример 4. Приведем пример, показывающий, что не для всех матриц x_1 и x_2 существует уравнение третьей степени, решениями которого они являются. В частности, такое уравнение не существует, если первый столбец у матриц $x_1 - x_2$ и $x_1^2 - x_2^2$ нулевой, а первый столбец у матрицы $x_1^3 - x_2^3$ уже не нулевой.

Подходящими матрицами будут, например, $x_1 = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $x_2 = \begin{pmatrix} 1 & 1 & 2 \\ -1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

Если в уравнение (5) при $n = 3$ подставить сначала x_1 , затем x_2 , а потом отнять от одного равенства другое, получим

$$a_2 \begin{pmatrix} 0 & -4 & -2 \\ 0 & 2 & 2 \\ 0 & -2 & -2 \end{pmatrix} + a_1 \begin{pmatrix} 0 & -2 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -2 & 8 & 4 \\ 0 & -6 & -4 \\ 0 & 4 & 2 \end{pmatrix}.$$

Какими бы ни были элементы на месте $(1, 1)$ в матрицах a_1 и a_2 , в левой части предыдущего матричного равенства на месте $(1, 1)$ находится 0, тогда как в правой его части на этом месте стоит -2 . Значит, не существует уравнения вида (5) при $n = 3$, решениями которого являлись бы данные матрицы x_1 и x_2 .

Заключение

Таким образом, показано, что для произвольных n элементов ассоциативного кольца с делением существует многочлен степени n , корнями которого они являются. Определены достаточные условия существования такого многочлена для элементов произвольного (не обязательно с делением) ассоциативного кольца с единицей. Отдельно рассмотрен случай многочленов, определенных над кольцом квадратных матриц над полем. Для этого случая получен критерий существования многочлена второй степени с заданными корнями, а также приведены примеры построения многочленов с заданными корнями.

Библиографические ссылки

1. Lam TY. *A first course in noncommutative rings*. 2nd edition. New York: Springer-Verlag; 2001. XIX, 388 p. (Axler S, Gehring FW, Ribet KA, editors. Graduate texts in mathematics; volume 131). DOI: 10.1007/978-1-4419-8616-0.
2. Huang L, So W. Quadratic formulas for quaternions. *Applied Mathematics Letters*. 2002;15(5):533–540. DOI: 10.1016/S0893-9659(02)80003-9.
3. Abrate M. Quadratic formulas for generalized quaternions. *Journal of Algebra and Its Applications*. 2009;8(3):289–306. DOI: 10.1142/S0219498809003308.
4. Chapman A. Quaternion quadratic equations in characteristic 2. *Journal of Algebra and Its Applications*. 2015;14(3):1550033. DOI: 10.1142/S0219498815500334.
5. Serôdio R, Pereira E, Vitória J. Computing the zeros of quaternion polynomials. *Computers and Mathematics with Applications*. 2001;42(8–9):1229–1237. DOI: 10.1016/S0898-1221(01)00235-8.
6. Chapman A, Machen C. Standard polynomial equations over division algebras. *Advances in Applied Clifford Algebras*. 2017;27(2):1065–1072. DOI: 10.1007/s00006-016-0740-4.
7. Falcão MI, Miranda F, Severino R, Soares MJ. Mathematica tools for quaternionic polynomials. In: Gervasi O, Murgante B, Misra S, Borruso G, Torre CM, Rocha AMAC, et al., editors. *Computational science and its applications – ICCSA 2017. Proceedings of the 17th International conference; 2017 July 3–6; Trieste, Italy. Part 2*. Cham: Springer; 2017. p. 394–408 (Lecture notes in computer science; volume 10405). DOI: 10.1007/978-3-319-62395-5_27.
8. Janovská D, Opfer G. A note on the computation of all zeros of simple quaternionic polynomials. *SIAM Journal on Numerical Analysis*. 2010;48(1):244–256. DOI: 10.1137/090748871.
9. Goutor AG, Tikhonov SV. Roots of polynomials over division rings. *Doklady of the National Academy of Sciences of Belarus*. 2024;68(5):359–364. DOI: 10.29235/1561-8323-2024-68-5-359-364.
10. Wilson RL. *Polynomial equations over matrices* [Internet]. Piscataway: Rutgers University; [cited 2024 November 12]. 20 p. Available from: https://sites.math.rutgers.edu/~rwilson/polynomial_equations.pdf.
11. Bray U, Whaples G. Polynomials with coefficients from a division ring. *Canadian Journal Mathematics*. 1983;35(3):509–515. DOI: 10.4153/CJM-1983-028-1.
12. Beck B. Sur les équations polynomiales dans les quaternions. *L'Enseignement mathématique. 2^e Série*. 1979;25(3–4):193–201. DOI: 10.5169/seals-50378.

Получена 28.11.2024 / исправлена 20.02.2025 / принята 20.02.2025.
Received 28.11.2024 / revised 20.02.2025 / accepted 20.02.2025.