

ФОРМУЛЫ ДЛЯ НАХОЖДЕНИЯ КОРНЕЙ НЕКОТОРЫХ МНОГОЧЛЕНОВ НАД КОЛЬЦАМИ С ДЕЛЕНИЕМ

А. Г. Гутор

Белорусский государственный университет, пр. Независимости, 4,
220030, г. Минск, Беларусь, goutor@bsu.by
Научный руководитель — С. В. Тихонов, кандидат физико-математических наук,
доцент

В работе приводится доказательство формул, позволяющих найти корни специальных многочленов с коэффициентами в кольце с делением. Данные формулы получены как обобщение известных формул для корней многочленов с коэффициентами в алгебре гамильтоновых кватернионов.

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

Под *кольцом с делением* A над F будем понимать ассоциативное кольцо A , для каждого ненулевого элемента которого существует обратный по умножению элемент, и которое также является векторным пространством над полем F . В качестве F чаще всего рассматривают центр A , т.е. множество элементов из A , которые перестановочны с любым элементом из A . Рассмотрим многочлены вида

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

Вопрос нахождения корней многочленов над кольцами с делением изучается в теории колец и прикладной математике. Наиболее изученным является случай многочленов с коэффициентами в алгебре гамильтоновых кватернионов.

Для элементов из A введём понятие *класса сопряжённости*. Элемент q' называется элементом из того же класса сопряжённости, что и q ($q : q'$), если существует $h \neq 0$, что $q' = hqh^{-1}$. A разбивается на множество непересекающихся классов сопряжённости элементов. Класс сопряжённости элемента q будем обозначать $[q] = \{q' \in A : q : q'\}$.

Заметим, что многочлен степени n с коэффициентами из поля имеет не более n корней в этом поле. Однако для многочлена степени n с коэффициентами из кольца с делением это уже не так. Но известно, что корни такого многочлена лежат не более чем в n классах сопряжённости [2, Th. 16.4].

Вначале в качестве A будем рассматривать алгебру гамильтоновых кватернионов $\mathbb{H}$. Напомним, что $\mathbb{H}$ является кольцом с делением над $\mathbb{R}$ размерности 4, т. е. состоит из элементов вида $q = q_0 + iq_1 + jq_2 + kq_3$, где $q_i \in \mathbb{R}$, $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$ [1, с. 27]. Для элементов из $\mathbb{H}$ можно ввести понятия: *сопряжённый элемент* к q , $\bar{q} := q_0 - iq_1 - jq_2 - kq_3$; *норма* q , $|q| = \sqrt{q\bar{q}} = \sqrt{\bar{q}q} = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}$, *обратный* к любому ненулевому элементу $q^{-1} = \frac{\bar{q}}{|q|^2}$.

Многочлен, сопряжённый введённому многочлену $P(x)$, если $A = \mathbb{H}$:

$$\bar{P}(x) := \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} + \dots + \bar{a}_1 x + \bar{a}_0.$$

Любой унитарный ($a_n = 1$) многочлен $P(x)$ из $\mathbb{H}[x]$ разлагается на линейные множители, т. е. существуют $x_1, \dots, x_n \in \mathbb{H}$ такие, что

$$P(x) = (x - x_n)(x - x_{n-1}) \dots (x - x_1),$$

где упорядоченную последовательность $(x_1, \dots, x_n)$ будем называть цепочкой многочлена $P(x)$ [2]. Из данного разложения следует, что x_1 является корнем многочлена $P(x)$ [2, с. 262]. Напомним, что корни многочлена $P(x)$ лежат не более чем в n классах сопряжённости, а также то, что любой корень лежит в одном классе сопряжённости с некоторым элементом x_i [2, с. 263]. Либо единственный элемент из данного класса сопряжённости является корнем многочлена, тогда корень называется *изолированным*, либо все элементы класса являются корнями, корень в этом случае называется *сферическим* [3, с. 96].

Известна следующая формула для корней многочлена $P(x) = (x - x_n)(x - x_{n-1}) \dots (x - x_1)$, если элементы цепочки x_k из различных классов сопряжённости [3 с. 97]:

$$\zeta_k = \bar{P}_k(x_k) x_k (\bar{P}_k(x_k))^{-1}; \quad k = 1, \dots, n,$$

$$\text{где } P_k(x) := \begin{cases} 1, & k = 1 \\ (x - x_{k-1}) \dots (x - x_1), & \text{иначе.} \end{cases}$$

В работе [4] нами получено обобщение данной формулы для случая произвольного кольца с делением.

Теорема. Пусть A является кольцом с делением над центром F . Пусть также

$$P(x) = (x - x_n) \dots (x - x_1),$$

где $x_1, \dots, x_n \in A$. Пусть также $x_1, \dots, x_{n-1}$ алгебраические над F . Обозначим $f_i(x)$ минимальные многочлены элементов x_i , $i = 1, \dots, n-1$. Если классы сопряжённости $[x_k]$ различны, тогда многочлен $P(x)$ имеет ровно n корней ζ_k , которые связаны с x_k следующим образом:

$$\zeta_k = P_k(x_k) x_k (P_k(x_k))^{-1}; \quad k = 1, \dots, n,$$

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

где $S_i(x) \in A[x]$ такие что $f_i(x) = S_i(x)(x - x_i)$, $i = 1, \dots, n-1$.

Доказательство. Заметим, что $S_i(x) \in F(x_i)[x]$ (следует из того, что $f_i(x)$ делятся на $(x - x_i)$ для соответствующего x_i в кольце $F(x_i)[x]$), значит

$$f_i(x) = S_i(x)(x - x_i) = (x - x_i)S_i(x) \text{ для } i = 1, \dots, n-1.$$

Заметим, что x_1 является корнем $P(x)$, что удовлетворяет формулам при $k = 1$. Далее умножим выражение $P(x) = (x - x_n) \dots (x - x_1)$ на $S_1(x)$ справа:

$$\begin{aligned} P(x)S_1(x) &= (x - x_n) \dots (x - x_1)S_1(x) = (x - x_n) \dots (x - x_2)f_1(x) = \\ &= f_1(x)(x - x_n) \dots (x - x_2). \end{aligned}$$

Из этого следует, что x_2 – корень последнего выражения, а значит, и $P(x)S_1(x)$. Но x_2 не является корнем $S_1(x)$, т.к. все корни $S_1(x)$ лежат в классе $[x_1]$. Далее для доказательства понадобится следующее утверждение.

Утверждение 1. ([2, Pr. 16.3]). Пусть A является кольцом с делением и пусть $P(x) = L(x)R(x) \in A[x]$. Пусть $d \in A$ такое что $h := R(d) \neq 0$. Тогда

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

В частности, если d – корень $P(x)$, но не корень $R(x)$, тогда hdh^{-1} – корень $L(x)$.

Согласно утверждению выше $\zeta_2 = S_1(x_2)x_2(S_1(x_2))^{-1}$ – корень $P(x)$. Далее равенство $P(x)S_1(x) = f_1(x)(x - x_n) \dots (x - x_2)$ умножаем справа на $S_2(x)$

$$P(x)P_3(x)=P(x)S_1(x) S_2(x)=f_1(x) (x-x_n) \dots (x-x_2) S_2(x) = \\ =f_1(x) (x-x_n) \dots (x-x_3) f_2(x) =f_1(x) f_2(x) (x-x_n) \dots (x-x_3).$$

Для дальнейшего доказательства понадобится утверждение.

Утверждение 2 [4]. Если a является корнем произведения $S_1(x) \dots S_n(x)$, то a сопряжено корню $S_i(x)$ для некоторого $i = 1, \dots, n$.

Доказательство утверждения 2. Докажем по индукции. Для $n = 2$ утверждение 2 верно (утв. 1). Предположим, что верно для $n - 1$. Докажем для n . Пусть a является корнем $S_1(x) \dots S_n(x)$, тогда либо a – корень $S_n(x)$, либо a сопряжено корню $S_1(x) \dots S_{n-1}(x)$ (утв. 1). Но предполагали, что корень произведения сопряжён корню $S_i(x)$ для некоторого $i = 1, \dots, n - 1$. Следовательно, a сопряжено корню $S_i(x)$ для некоторого $i = 1, \dots, n$. $\square$

Вернёмся к доказательству теоремы. Из равенства

$$P(x) S_1(x) S_2(x) = f_1(x) f_2(x) (x - x_n) \dots (x - x_3)$$

следует, что x_3 – корень правой части, а значит, и левой. По утверждению 2, если бы x_3 был корнем $S_1(x) S_2(x)$, то был бы сопряжён корню $S_1(x)$ либо корню $S_2(x)$, но это не так. Значит, по утверждению 1, $\zeta_3 = P_3(x_3)x_3(P_3(x_3))^{-1}$ – корень $P(x)$. Продолжая процесс, получим оставшиеся корни $P(x)$. $\square$

Заметим, что иногда нахождение корней с коэффициентами в некоммутативной алгебре может быть сведено к коммутативному случаю [5], что упрощает вычисления.

Библиографические ссылки

1. Пирс Р. Ассоциативные алгебры. – М.: Мир, 1986.
2. Lam T. Y. A first course in noncommutative rings. Graduate Texts in Mathematics. – New York: Springer-Verlag, 1991.
3. Falcao M. I. [et al.] Mathematica Tools for Quaternionic Polynomials. // Lecture Notes in Computer Science. 2017. Vol. 10405. P. 394-408.
4. Goutor A., Tikhonov S. Roots of polynomials over division rings, Preprint. <https://arxiv.org/abs/2403.10999>
5. Гутор А., Тихонов С. О корнях многочленов с коэффициентами в алгебре гамильтоновых кватернионов // Математическое и компьютерное моделирование: сборник материалов XI Международной научной конференции, посвященной памяти В.А. Романькова (Омск, 15 марта, 2024 г.) [отв. за вып. И.П. Бесценный]. Омск: Изд-во Ом. гос. ун-та, 2024. С. 20-23.