

Глава IV. Многочлены

§ 4. Корни многочленов. Неприводимые многочлены над полями \mathbb{C} , \mathbb{R}

А. Я. Овсянников

Уральский федеральный университет
Институт естественных наук и математики
Департамент математики, механики и компьютерных наук
Основы алгебры для направлений
Механика и математическое моделирование и
Прикладная математика
(1 семестр)

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$ – многочлен над полем F . Этот многочлен можно рассматривать как функцию из F в F , сопоставляющую каждому элементу $\beta \in F$ элемент из F , который называется **значением** многочлена $f(x)$ на элементе β :

$$f(\beta) = \alpha_n \beta^n + \alpha_{n-1} \beta^{n-1} + \dots + \alpha_1 \beta + \alpha_0.$$

Определение

Элемент $\beta \in F$ называется **корнем** многочлена $f(x)$, если $f(\beta) = 0$.

Теорема Безу

Пусть $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$ – многочлен над полем F и $\alpha \in F$. Тогда $f(x) = q(x)(x - \alpha) + f(\alpha)$, где $q(x) = b_0 x^{n-1} + b_1 x^{n-2} + \dots + b_{n-1}$, и $b_0 = a_0$, $b_k = a_k + \alpha b_{k-1}$ при всех $k = 1, \dots, n-1$, $f(\alpha) = a_n + \alpha b_{n-1}$. (1)

↓ Разделим $f(x)$ на $x - \alpha$ с остатком: $f(x) = (b_0 x^{n-1} + b_1 x^{n-2} + \dots + b_{n-1})(x - \alpha) + r$, $\deg(r) \leq 0$, и $r = f(\alpha)$. Из $a_0 x^n + a_1 x^{n-1} + \dots + a_n = (b_0 x^{n-1} + b_1 x^{n-2} + \dots + b_{n-1})(x - \alpha) + f(\alpha)$ следует $a_0 x^n + a_1 x^{n-1} + \dots + a_k x^{n-k} + \dots + a_n = b_0 x^n + (b_1 - \alpha b_0)x^{n-1} + \dots + (b_k - \alpha b_{k-1})x^{n-k} + \dots + f(\alpha) - \alpha b_{n-1}$ и $a_0 = b_0$, $a_1 = b_1 - \alpha b_0, \dots, a_k = b_k - \alpha b_{k-1}, \dots, a_n = f(\alpha) - \alpha b_{n-1}$. Отсюда получаются все равенства (1). ↑

Следствие из теоремы Безу. Связь неприводимости с наличием корней у многочлена

Следствие

Скаляр β будет корнем многочлена $f(x)$ тогда и только тогда, когда $f(x) = q(x)(x - \beta)$.

Пусть F – поле. В силу следствия получаем, что если многочлен f из $F[x]$ имеет корень в поле F , то он является неприводимым над полем F тогда и только тогда, когда $\deg(f) = 1$.

Предложение

Пусть $f \in F[x]$, $\deg(f) = 2$ или $\deg(f) = 3$. Многочлен f является неприводимым над полем F тогда и только тогда, когда он не имеет корней в поле F .

↓ В силу сказанного выше неприводимый над полем F многочлен степени выше первой не может иметь корней в поле F . Если многочлен f имеет степень 2 или 3, то отсутствие корней, равносильное тому, что многочлен не имеет делителей первой степени, влечет за собой неприводимость, так как при разложении f в произведение двух многочленов gh , где $\deg(g) < \deg(f)$ и $\deg(h) < \deg(f)$, степень по крайней мере одного из сомножителей должна быть равна 1. ↑

Если степень многочлена больше трех, то многочлен, не имеющий корней в поле F , может быть приводимым над F . Например, многочлен $(x^2 + 1)^2 = x^4 + 2x^2 + 1$ не имеет действительных корней, но приводим над полем действительных (и даже рациональных) чисел.

На формулах (1) основан упрощенный алгоритм деления многочлена f на двучлен $x - \alpha$ и нахождения значения $f(\alpha)$, известный под названием *схема Горнера*. Для осуществления алгоритма составляется таблица из двух строк. В первой строке записываются коэффициенты многочлена f по убыванию степеней (без пропусков, если некоторая степень отсутствует, то на соответствующем месте записывается нуль). Вторая строка заполняется с учетом формул (1): первое число переносится из первой строки, каждое последующее получается путем умножения предыдущего (только что полученного) числа из второй строки на число α и сложения результата с числом из первой строки, стоящим над заполняемой клеткой второй строки. Последнее число во второй строке (под свободным членом f) и будет значением $f(\alpha)$, а числа с первого по предпоследнее – коэффициентами частного в порядке убывания степеней. Для удобства проведения вычислений число α выписывают слева от первого элемента второй строки.

Рассмотрим конкретный пример. Пусть требуется найти значение многочлена $f(x) = x^3 - 18x^2 + 99x - 162$ от числа 3. Вычисления оформляем в виде таблицы:

	1	-18	99	-162
3	1	-15	54	0

Здесь в первой строке выписаны коэффициенты многочлена $f(x)$, а во второй сначала записано число 3, затем перенесен старший коэффициент $f(x)$, равный 1. Каждое последующее число во второй строке получается прибавлением к соответствующему числу первой строки предыдущего числа второй, умноженного на 3: $-15 = -18 + 1 \cdot 3$, $54 = 99 + (-15) \cdot 3$, $0 = -162 + 54 \cdot 3$. Отсюда получаем $f(3) = 0$ и частное $q(x) = x^2 - 15x + 54$ от деления $f(x)$ на $x - 3$, т.е.
 $f(x) = (x^2 - 15x + 54)(x - 3)$.

Разложить многочлен $f(x) = x^5 - 4x^4 + x^3 + 2x^2 - x + 5$ по степеням $x - 2$.

Будем делить по схеме Горнера сначала многочлен $f(x)$ на $x - 2$, потом частное, и так далее.

	1	-4	1	2	-1	5
2	1	-2	-3	-4	-9	-13
2	1	0	-3	-10	-29	
2	1	2	1	-8		
2	1	4	9			
2	1	6				
	1					

$$\begin{aligned}
 \text{Имеем } f(x) &= -13 + (x - 2)(x^4 - 2x^3 - 3x^2 - 4x - 9) = \\
 &= -13 + (x - 2)(-29 + (x - 2)(x^3 - 3x - 10)) = \\
 &= -13 + (x - 2)(-29 + (x - 2)(-8 + (x - 2)(x^2 + 2x + 1))) = \\
 &= -13 + (x - 2)(-29 + (x - 2)(-8 + (x - 2)(7 + (x - 2)(x + 4)))) = \\
 &= -13 + (x - 2)(-29 + (x - 2)(-8 + (x - 2)(9 + (x - 2)(6 + (x - 2)))))) = \\
 &= -13 - 29(x - 2) - 8(x - 2)^2 + 9(x - 2)^3 + 6(x - 2)^4 + (x - 2)^5.
 \end{aligned}$$

Коэффициенты при степенях $x - 2$ определяются как остатки при последовательном делении на этот многочлен.

Определение

Натуральное число k называется **кратностью** корня α многочлена $f(x)$, если $f(x) = g(x)(x - \alpha)^k$ и $g(\alpha) \neq 0$.

Легко понять, что кратность корня α многочлена $f(x)$ равна кратности неприводимого множителя $x - \alpha$ этого многочлена. Поэтому любой многочлен степени $n \geq 1$ имеет не более n различных корней в поле F , а сумма кратностей его корней также не превосходит n .

Из предложения сл.б §3 получается

Следствие

Пусть F – поле, $\text{char}(F) = 0$ и $f \in F[x]$, $\alpha \in F$ – корень многочлена f кратности k . Если $k = 1$, то α не является корнем производной f' . Если $k > 1$, то α – корень многочлена f' кратности $k - 1$.

Одним из мотивов расширения множества действительных чисел до множества комплексных чисел является то, что существуют многочлены с действительными коэффициентами, которые не имеют действительных корней. Таков, например, многочлен $x^2 + 1$. Между тем, этот многочлен имеет два комплексных корня: i и $-i$. Возникает вопрос: всякий ли многочлен с комплексными коэффициентами имеет комплексный корень? При этом, разумеется, следует исключить из рассмотрения многочлены степени 0 (т.е. константы). Ответ на поставленный вопрос дает следующее утверждение, которое называют *теоремой Гаусса* или *основной теоремой высшей алгебры*.

Теорема

Любой многочлен степени больше 0 над полем \mathbb{C} имеет корень в \mathbb{C} .

Мы не приводим доказательства этого утверждения. Оно будет доказано в курсе теории функций комплексного переменного.

Пусть $f \in \mathbb{C}[x]$, $\deg(f) \geq 1$. По теореме Гаусса $f(x)$ имеет некоторый корень α . Следовательно, $f = (x - \alpha)g$ для некоторого многочлена $g \in \mathbb{C}[x]$. Если многочлен $f(x)$ неприводим над полем \mathbb{C} , то $\deg(f) = 1$. Таким образом, справедливо

Следствие 1

Неприводимыми над полем \mathbb{C} являются только многочлены первой степени.

Рассматривая разложение любого многочлена степени больше 1 из $\mathbb{C}[x]$ на неприводимые множители, над полем \mathbb{C} , получаем

Следствие 2

Любой многочлен с комплексными коэффициентами степени больше 1 разлагается на линейные множители с комплексными коэффициентами.

Предложение

Если многочлен f из $\mathbb{R}[x]$ имеет комплексный корень γ , то и число $\bar{\gamma}$, комплексно сопряженное к γ , является корнем f .

↓ Пусть $f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$ – многочлен из $\mathbb{R}[x]$, $\gamma \in \mathbb{C}$ и $f(\gamma) = 0$, т.е. $\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \dots + \alpha_1 \gamma + \alpha_0 = 0$. Тогда, используя свойства операции комплексного сопряжения (сл.7 §1 гл.III), получаем $\frac{f(\bar{\gamma}) = \alpha_n \bar{\gamma}^n + \alpha_{n-1} \bar{\gamma}^{n-1} + \dots + \alpha_1 \bar{\gamma} + \alpha_0 = \bar{\alpha}_n \bar{\gamma}^n + \bar{\alpha}_{n-1} \bar{\gamma}^{n-1} + \dots + \bar{\alpha}_1 \bar{\gamma} + \bar{\alpha}_0 = \overline{\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \dots + \alpha_1 \gamma + \alpha_0} = \bar{0} = 0$, что и требуется доказать. ↑

Предложение

Многочлен $f \in \mathbb{R}[x]$ неприводим над полем \mathbb{R} тогда и только тогда, когда либо $\deg(f) = 1$, либо $\deg(f) = 2$ и f имеет отрицательный дискриминант.

↓ Очевидно, что если $\deg(f) = 1$ или $\deg(f) = 2$ и f имеет отрицательный дискриминант, то f неприводим над полем \mathbb{R} . Пусть многочлен $f \in \mathbb{R}[x]$ неприводим над полем \mathbb{R} . Если он имеет действительный корень, то делится на многочлен первой степени, поэтому $\deg(f) = 1$. Пусть f имеет комплексный корень $\gamma = \alpha + \beta i$ и $\beta \neq 0$. Тогда согласно предложению сл.10 и число $\bar{\gamma} = \alpha - \beta i$ является его корнем. Поэтому f делится на $x - \gamma$ и на $x - \bar{\gamma}$. Так как $\gamma \neq \bar{\gamma}$, указанные двучлены взаимно просты. Согласно утверждению 1 предложения сл.7 §2 многочлен f делится на их произведение $(x - \gamma)(x - \bar{\gamma})$, которое равно $(x - \alpha - i\beta)(x - \alpha + i\beta) = x^2 - 2\alpha x + i\beta x - i\beta x + (\alpha + i\beta)(\alpha - i\beta) = x^2 - 2\alpha x + \alpha^2 + \beta^2$ и представляет собой квадратный трехчлен с отрицательным дискриминантом. Так как f неприводим, он ассоциирован с многочленом $x^2 - 2\alpha x + \alpha^2 + \beta^2$, что завершает доказательство. ↑

Пусть $f \in \mathbb{C}[x]$ и $\deg(f) = n$, $n > 0$. Тогда

$$f(x) = a_0(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \dots (x - \alpha_m)^{k_m},$$

где α_j – все различные комплексные корни многочлена f кратностей k_j ,

a_0 – старший коэффициент многочлена f и $\sum_{j=1}^m k_j = n$.

Пусть $f \in \mathbb{R}[x]$ и $\deg(f) = n$, $n > 0$. Тогда

$$f(x) = a_0(x - \alpha_1)^{k_1} \dots (x - \alpha_m)^{k_m} (x^2 - \beta_1x + \gamma_1)^{\ell_1} \dots (x^2 - \beta_px + \gamma_p)^{\ell_p},$$

где α_j – все различные действительные корни многочлена f кратностей k_j ($j = 1, 2, \dots, m$), различные многочлены $x^2 - \beta_jx + \gamma_j$ ($j = 1, 2, \dots, p$) не

имеют действительных корней, a_0 – старший коэффициент многочлена f

и $\sum_{j=1}^m k_j + 2 \sum_{j=1}^p \ell_j = n$.

Из наблюдения сл.13 §2 получается следующее

Наблюдение

Пусть многочлены f и g из кольца $\mathbb{F}[x]$, где $\mathbb{F} \subseteq \mathbb{C}$. Чтобы многочлен f делил многочлен g , необходимо и достаточно, чтобы каждый комплексный корень многочлена f кратности k был также корнем многочлена g не меньшей чем k кратности.

Разложить на неприводимые множители над полем \mathbb{R} многочлен $x^{2n} + x^n - 2$.

Идея решения состоит в том, чтобы найти все действительные и все комплексные, не являющиеся действительными, корни этого многочлена, последние сгруппировать попарно на комплексно сопряженные и для каждой пары таких корней $\alpha \pm i\beta$ записать неприводимый над полем \mathbb{R} многочлен $x^2 - 2\alpha x + \alpha^2 + \beta^2$, имеющий данные комплексные корни.

Пусть $y = x^n$. Тогда $y^2 + y - 2 = 0$, $y_1 = 1$, $y_2 = -2$. Комплексные корни уравнения $x^n = 1$ – все корни n -й степени из 1, $x_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$. Попарно сопряжены корни, расположенные на верхней полуокружности, с корнями на нижней: $\cos \frac{2\pi k}{n} \pm i \sin \frac{2\pi k}{n}$; при $n = 2m$ $k = 1, \dots, m-1$, а при $n = 2m+1$ $k = 1, \dots, m$. Таким образом,

$$x^n - 1 = \begin{cases} (x-1)(x+1) \prod_{k=1}^{m-1} \left(x^2 - 2x \cos \frac{2\pi k}{n} + 1 \right), & n = 2m; \\ (x-1) \prod_{k=1}^m \left(x^2 - 2x \cos \frac{2\pi k}{n} + 1 \right), & n = 2m+1. \end{cases}$$

Найдем комплексные корни уравнения $x^n = -2$. Тригонометрическая форма $-2 = 2(\cos \pi + i \sin \pi)$; корни

$x_k = 2^{\frac{1}{n}} \left(\cos \frac{\pi + 2\pi k}{n} + i \sin \frac{\pi + 2\pi k}{n} \right)$. Опять попарно сопряжены корни,

расположенные на верхней полуокружности, с корнями на нижней:

$2^{\frac{1}{n}} \left(\cos \frac{\pi + 2\pi k}{n} \pm i \sin \frac{\pi + 2\pi k}{n} \right)$; $k = 1, \dots, m$ при $n = 2m$ и при

$n = 2m + 1$.

Таким образом,

$$x^n + 2 = \begin{cases} \prod_{k=1}^m \left(x^2 - 2^{1-\frac{1}{n}} x \cos \frac{\pi + 2\pi k}{n} + 2^{\frac{1}{m}} \right), & n = 2m; \\ (x + 2^{\frac{1}{n}}) \prod_{k=1}^m \left(x^2 - 2^{1-\frac{1}{n}} x \cos \frac{\pi + 2\pi k}{n} + 2^{\frac{2}{n}} \right), & n = 2m + 1. \end{cases}$$

Окончательно при $n = 2m$ имеем $x^{2n} + x^n - 2 = (x - 1)(x + 1) \times$

$$\times \prod_{k=1}^{m-1} \left(x^2 - 2x \cos \frac{2\pi k}{n} + 1 \right) \prod_{k=1}^m \left(x^2 - 2^{1-\frac{1}{n}} x \cos \frac{\pi + 2\pi k}{n} + 2^{\frac{1}{m}} \right),$$

а при $n = 2m + 1$ — $x^{2n} + x^n - 2 = (x - 1)(x + 2^{\frac{1}{n}}) \times$

$$\times \prod_{k=1}^m \left(x^2 - 2x \cos \frac{2\pi k}{n} + 1 \right) \prod_{k=1}^{m-1} \left(x^2 - 2^{1-\frac{1}{n}} x \cos \frac{\pi + 2\pi k}{n} + 2^{\frac{2}{n}} \right).$$

Найти условия для натурального числа m , при которых многочлен $(x+1)^m - x^m - 1$ делится многочлен $x^2 + x + 1$.

Так как $(x-1)(x^2+x+1) = x^3 - 1$, корни многочлена $x^2 + x + 1$ являются корнями 3-й степени из 1, отличными от 1. Именно, $\varepsilon_1 = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$, $\varepsilon_2 = \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3}$. Найдем значения натурального числа m , при которых $\varepsilon_1, \varepsilon_2$ являются корнями многочлена

$(x+1)^m - x^m - 1$. Вспомним, что $\varepsilon_1 + 1 = 1 + \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = 2 \cos^2 \frac{\pi}{3} + 2i \cos \frac{\pi}{3} \sin \frac{\pi}{3} = 2 \cos \frac{\pi}{3} (\cos \frac{\pi}{3} + i \sin \frac{\pi}{3}) = \cos \frac{\pi}{3} + i \sin \frac{\pi}{3}$ и $\varepsilon_2 + 1 = 1 + \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} = 2 \cos^2 \frac{2\pi}{3} + 2i \cos \frac{2\pi}{3} \sin \frac{2\pi}{3} = 2 \cos \frac{2\pi}{3} (\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}) = -(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3})$. Имеем

$(\varepsilon_1 + 1)^m - \varepsilon_1^m - 1 = (\cos \frac{\pi}{3} + i \sin \frac{\pi}{3})^m - (\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}) - 1 = \cos \frac{\pi m}{3} + i \sin \frac{\pi m}{3} - \cos \frac{2\pi m}{3} - i \sin \frac{2\pi m}{3} - 1 = \cos \frac{\pi m}{3} + i \sin \frac{\pi m}{3} - 2 \cos \frac{\pi m}{3} (\cos \frac{\pi m}{3} + i \sin \frac{\pi m}{3}) = (\cos \frac{\pi m}{3} + i \sin \frac{\pi m}{3})(1 - 2 \cos \frac{\pi m}{3})$.

Аналогично $(\varepsilon_2 + 1)^m - \varepsilon_2^m - 1 = (-1)^m (\cos \frac{2\pi m}{3} + i \sin \frac{2\pi m}{3}) - 2 \cos \frac{2\pi m}{3} (\cos \frac{2\pi m}{3} + i \sin \frac{2\pi m}{3}) = (\cos \frac{2\pi m}{3} + i \sin \frac{2\pi m}{3})((-1)^m - 2 \cos \frac{2\pi m}{3})$.

Следовательно, $\varepsilon_1, \varepsilon_2$ являются корнями многочлена $(x+1)^m - x^m - 1$

тогда и только тогда, когда $\begin{cases} \cos \frac{\pi m}{3} = \frac{1}{2}, \\ \cos \frac{2\pi m}{3} = \frac{(-1)^m}{2}. \end{cases}$

Если $m = 1, 2, 3, 4, 5$, то оба равенства $\cos \frac{\pi m}{3} = \frac{1}{2}$ и $\cos \frac{2\pi m}{3} = \frac{(-1)^m}{2}$ выполняются лишь при $m = 1$ или $m = 5$. Так как наименьший положительный период у функции $\cos \frac{x}{3}$ равен 6π , а у функции $\cos \frac{2x}{3} = 3\pi$, m может принимать значения лишь $1 + 6k$ или $5 + 6k$ при любом неотрицательном целом k .

Для многочленов первой степени ответ на этот вопрос хорошо известен из школьного курса математики. Для многочленов второй степени ответ дается известной формулой корней квадратного уравнения. Как уже отмечалось в §1 гл.III (сл.13), если $az^2 + bz + c = 0$ – уравнение с комплексными коэффициентами и $a \neq 0$, то

$$z_{1,2} = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

Знак минус перед корнем из дискриминанта можно не ставить, так как здесь подразумевается комплексный корень, имеющий два значения, а не арифметическое значение действительного корня.

В высшей алгебре известны формулы для нахождения комплексных корней уравнений третьей и четвертой степени, но они громоздки и неудобны для практического применения. Доказано, что при $n \geq 5$ единой формулы, использующей только арифметические операции извлечение корня любой степени, для нахождения корней произвольного алгебраического уравнения степени n не существует. Однако решать такие уравнения приходится. Иногда у такого уравнения удается подобрать корни.