

# § 20. Неприводимые многочлены над основными числовыми полями

Б.М.Верников

Уральский федеральный университет,  
Институт математики и компьютерных наук,  
кафедра алгебры и дискретной математики

- В этом параграфе рассматриваются многочлены над тремя наиболее важными числовыми полями —  $\mathbb{C}$ ,  $\mathbb{R}$  и  $\mathbb{Q}$ , а также над кольцом  $\mathbb{Z}$ . Мы интересуемся тем, как выглядят неприводимые множители у таких многочленов и что можно сказать о корнях этих многочленов.

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  $-i$  (в этом легко убедиться, вычислив  $\sqrt{-1}$  по формуле (3) из § 5). Возникает вопрос: всякий ли многочлен с комплексными коэффициентами имеет комплексный корень? При этом, разумеется, следует исключить из рассмотрения многочлены степени  $\leq 0$  (т. е. элементы поля  $\mathbb{C}$ ). Ответ на поставленный вопрос дает следующее утверждение.

## Основная теорема высшей алгебры (теорема Гаусса)

*Любой многочлен степени больше 0 над полем  $\mathbb{C}$  имеет по крайней мере один комплексный корень.* □

Доказательство этой теоремы выходит за рамки нашего курса, и потому мы не будем его приводить.

Многочлены степени 1 называются *линейными*. Пусть  $f$  — многочлен над  $\mathbb{C}$  и  $\deg f = n > 0$ . По теореме Гаусса многочлен  $f$  имеет некоторый корень  $\alpha_1$ . Но тогда, по следствию из теоремы Безу (см. § 18),  $f(x) = (x - \alpha_1)g(x)$  для некоторого многочлена  $g$ . Ясно, что  $\deg g = n - 1$ . Если  $n - 1 > 0$ , то по теореме Гаусса многочлен  $g$  имеет некоторый корень  $\alpha_2$ , и потому

$$f(x) = (x - \alpha_1)g(x) = (x - \alpha_1)(x - \alpha_2)h(x)$$

для некоторого многочлена  $h$  степени  $n - 2$ . Продолжая этот процесс, мы через  $n$  шагов представим  $f$  в виде произведения  $n$  линейных множителей и многочлена нулевой степени (т. е. элемента поля  $F$ ). Иными словами,

$$f(x) = t(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = (tx - t\alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

где  $t \in F$ . Таким образом, справедливо

**Следствие о разложении многочленов над  $\mathbb{C}$**

*Любой многочлен степени  $n > 0$  над полем  $\mathbb{C}$  разлагается в произведение  $n$  линейных многочленов над  $\mathbb{C}$ .* □

# Число комплексных корней многочлена с комплексными коэффициентами

Кроме того, из следствия о разложении многочленов над  $\mathbb{C}$  вытекает

## Следствие о числе комплексных корней уравнения

*Любое алгебраическое уравнение  $n$ -й степени с комплексными коэффициентами имеет ровно  $n$  комплексных корней, если каждый корень считать столько раз, какова его кратность.*

То же самое утверждение можно переформулировать следующим образом:

**!!** *сумма кратностей всех корней многочлена ненулевой степени над полем  $\mathbb{C}$  равна степени этого многочлена.*

Для того, чтобы доказать следствия из теоремы Гаусса, относящиеся к многочленам над полем  $\mathbb{R}$ , нам понадобится следующий факт.

## Лемма о корнях и комплексной сопряженности

Если  $f(x)$  — многочлен над полем  $\mathbb{C}$ , все коэффициенты которого являются действительными числами, а  $\gamma$  — корень этого многочлена, то и число  $\bar{\gamma}$  является корнем этого многочлена.

**Доказательство.** Пусть  $f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$ . Тогда  $\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \dots + \alpha_1 \gamma + \alpha_0 = 0$ . Используя свойства операции сопряжения комплексных чисел и тот факт, что  $\bar{\alpha} = \alpha$  для всякого  $\alpha \in \mathbb{R}$ , получаем:

$$\begin{aligned} f(\bar{\gamma}) &= \alpha_n \bar{\gamma}^n + \alpha_{n-1} \bar{\gamma}^{n-1} + \dots + \alpha_1 \bar{\gamma} + \alpha_0 = \\ &= \overline{\alpha_n} \cdot \bar{\gamma}^n + \overline{\alpha_{n-1}} \cdot \bar{\gamma}^{n-1} + \dots + \overline{\alpha_1} \cdot \bar{\gamma} + \overline{\alpha_0} = \\ &= \overline{\alpha_n} \cdot \overline{\gamma^n} + \overline{\alpha_{n-1}} \cdot \overline{\gamma^{n-1}} + \dots + \overline{\alpha_1} \cdot \bar{\gamma} + \overline{\alpha_0} = \\ &= \overline{\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \dots + \alpha_1 \gamma + \alpha_0} = \\ &= \overline{0} = 0, \end{aligned}$$

что и требовалось доказать.

Следствие о разложении многочленов над  $\mathbb{R}$ 

Любой многочлен степени  $> 0$  над полем  $\mathbb{R}$  разлагается на множители с действительными коэффициентами, каждый из которых либо линеен, либо является многочленом второй степени с отрицательным дискриминантом.

**Доказательство.** Пусть  $f(x) \in \mathbb{R}[x]$ . В силу следствия о разложении многочленов над  $\mathbb{C}$ ,  $f = \alpha(x - \gamma_1) \cdots (x - \gamma_n)$ , где  $\alpha, \gamma_1, \dots, \gamma_n \in \mathbb{C}$ . При этом  $\alpha \in \mathbb{R}$ , поскольку  $f \in \mathbb{R}[x]$ . Без ограничения общности будем считать, что  $\gamma_1, \dots, \gamma_m \in \mathbb{R}$  и  $\gamma_{m+1}, \dots, \gamma_n \notin \mathbb{R}$ . Пусть  $m + 1 \leq k \leq n$  и  $\gamma_k = \alpha + \beta i$ . Ясно, что  $\beta \neq 0$ . По лемме о корнях и комплексной сопряженности число  $\overline{\gamma_k} = \alpha - \beta i$  также является корнем многочлена  $f$ . Это означает, что  $\overline{\gamma_k} = \gamma_\ell$  для некоторого  $\ell > m$ . Следовательно, многочлен  $f$  делится на

$$\begin{aligned} (x - \gamma_k)(x - \gamma_\ell) &= (x - \gamma_k)(x - \overline{\gamma_k}) = (x - \alpha - \beta i)(x - \alpha + \beta i) = \\ &= (x - \alpha)^2 - (\beta i)^2 = x^2 - 2\alpha x + \alpha^2 + \beta^2. \end{aligned}$$

Полученный квадратный трехчлен над  $\mathbb{R}$  имеет отрицательный дискриминант:  $4\alpha^2 - 4(\alpha^2 + \beta^2) = -4\beta^2 < 0$ , поскольку  $\beta \neq 0$ . Таким образом, множители  $(x - \gamma_{k+1}), \dots, (x - \gamma_n)$  можно сгруппировать попарно таким образом, что каждая из пар после перемножения дает квадратный трехчлен над  $\mathbb{R}$  с отрицательным дискриминантом.

Простого и удобного для применения критерия неприводимости многочленов над полем  $\mathbb{Q}$  не существует. Есть только весьма сильное достаточное условие. Чтобы доказать его, нам понадобятся некоторые вспомогательные понятия и результаты. При этом нам часто надо будет рассматривать НОД конечного набора целых чисел. Как и в кольце многочленов над полем, НОД элементов в кольце  $\mathbb{Z}$  определен не однозначно, а с точностью до умножения на обратимый множитель<sup>1</sup>.

## Определение

Пусть  $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_0$  — многочлен над кольцом  $\mathbb{Z}$ . НОД чисел  $\alpha_n, \alpha_{n-1}, \dots, \alpha_0$  называется *содержанием* многочлена  $f$  и обозначается через  $d(f)$ . Если  $d(f) \in \{1, -1\}$ , то многочлен  $f$  называется *примитивным*.

Если в многочлене  $f \in \mathbb{Z}[x]$  вынести за скобки НОД всех его коэффициентов, то в скобках будет стоять примитивный многочлен над  $\mathbb{Z}$ . Таким образом,

**!!** произвольный многочлен  $f \in \mathbb{Z}[x]$  представим в виде  $f = d(f) \cdot f_0$ , где  $f_0$  — примитивный многочлен над  $\mathbb{Z}$ . □

---

<sup>1</sup> Фактически, с точностью до знака, поскольку обратимыми по умножению элементами кольца  $\mathbb{Z}$  являются только числа 1 и  $-1$ .

## Лемма Гаусса

Произведение двух примитивных многочленов над  $\mathbb{Z}$  примитивно.

**Доказательство.** Пусть  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  и  $g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$  — многочлены над  $\mathbb{Z}$ . Предположим, что многочлены  $f$  и  $g$  примитивны, а их произведение не примитивно. Следовательно, существует простое число  $p$ , делящее  $d(fg)$ . В силу примитивности многочленов  $f$  и  $g$ , существуют индексы  $s$  и  $t$  такие, что  $p$  не делит  $a_s$  и  $b_t$ . Пусть  $s$  и  $t$  — минимальные индексы с такими свойствами. Коэффициент при  $x^{s+t}$  в многочлене  $fg$  будет равен

$$c_{s+t} = a_s b_t + a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \dots + a_{s-1} b_{t+1} + a_{s-2} b_{t+2} + \dots \quad (1)$$

В силу выбора индексов  $s$  и  $t$ , коэффициенты  $a_{s-i}$  и  $b_{t-i}$  при  $i > 0$  делятся на  $p$ , а из того, что  $p$  делит  $d(fg)$ , вытекает, что  $p$  делит  $c_{s+t}$ . Отсюда и из равенства (1) вытекает, что  $p$  делит  $a_s b_t$ . Но тогда, будучи простым, число  $p$  делит либо  $a_s$ , либо  $b_t$ , что противоречит выбору  $p$ .  $\square$



Следствие о неприводимости над  $\mathbb{Z}$  и над  $\mathbb{Q}$ 

Многочлен  $f \in \mathbb{Z}[x]$  неприводим над  $\mathbb{Z}$  тогда и только тогда, когда он неприводим над  $\mathbb{Q}$ .

*Доказательство.* *Достаточность* очевидна. Докажем *необходимость*.

Предположим, что  $f$  неприводим над  $\mathbb{Z}$ , но приводим над  $\mathbb{Q}$ . Пусть  $f = gh$ , где  $g, h \in \mathbb{Q}[x]$  и  $\deg g, \deg h > 0$ . Обозначим через  $a$  наименьшее общее кратное знаменателей всех коэффициентов многочлена  $g$ , а через  $b$  — наименьшее общее кратное знаменателей всех коэффициентов многочлена  $h$ . Тогда  $gh = \frac{1}{ab} \cdot g_1 h_1$ , где  $g_1$  и  $h_1$  — многочлены над  $\mathbb{Z}$ . Теперь положим  $c = d(g_1)$  и  $d = d(h_1)$ . Тогда  $g_1 = cg_2$  и  $h_1 = dh_2$ , где  $g_2$  и  $h_2$  — примитивные многочлены над  $\mathbb{Z}$ . Объединяя сказанное, имеем

$$f = gh = \frac{1}{ab} \cdot g_1 h_1 = \frac{cd}{ab} \cdot g_2 h_2.$$

Все коэффициенты многочлена  $f$  являются целыми числами.

Следовательно,  $ab$  делит все коэффициенты многочлена  $cdg_2h_2$ , т. е.  $ab$  делит  $cd \cdot d(g_2h_2)$ . В силу леммы Гаусса многочлен  $g_2h_2$  примитивен. Это означает, что  $d(g_2h_2) = 1$ , и потому  $ab$  делит  $cd$ . Положим  $\frac{cd}{ab} = k$ . В силу сказанного выше,  $k$  — целое число и  $f = (kg_2)h_2$ . Это означает, что многочлен  $f$  приводим над  $\mathbb{Z}$  вопреки его выбору.

Если  $f \in \mathbb{Q}[x]$ , то умножив многочлен  $f$  на наименьшее общее кратное знаменателей всех его коэффициентов, мы получим многочлен  $g$  с целыми коэффициентами. Поскольку  $g = af$ , где  $a \in \mathbb{Z}$ , многочлен  $g$  неприводим над  $\mathbb{Q}$  тогда и только тогда, когда  $f$  неприводим над  $\mathbb{Q}$ . Таким образом,

- при изучении многочленов, неприводимых над  $\mathbb{Q}$ , можно ограничиться рассмотрением многочленов над  $\mathbb{Q}$  с целыми коэффициентами.

Следующее утверждение дает упомянутое выше достаточное условие неприводимости многочлена над  $\mathbb{Q}$ . По традиции оно называется критерием Эйзенштейна, хотя это и противоречит общепринятому в математике пониманию слова «критерий» как синонима слов «необходимое и достаточное условие».

### Критерий Эйзенштейна

Пусть  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  — многочлен степени  $> 0$  над  $\mathbb{Q}$  с целыми коэффициентами и существует простое число  $p$  такое, что  $a_n$  не делится на  $p$ ,  $a_{n-1}, \dots, a_0$  делятся на  $p$  и  $a_0$  не делится на  $p^2$ . Тогда  $f$  неприводим над  $\mathbb{Q}$ .

*Доказательство.* Предположим, что  $f$  приводим над  $\mathbb{Q}$ . Тогда, в силу следствия о неприводимости над  $\mathbb{Z}$  и над  $\mathbb{Q}$ ,  $f$  приводим над  $\mathbb{Z}$ .

Следовательно,  $f$  представим в виде  $f = gh$ , где

$g(x) = b_k x^k + b_{k-1} x^{k-1} + \dots + b_0$  и  $h(x) = c_m x^m + c_{m-1} x^{m-1} + \dots + c_0$  —

многочлены ненулевой степени над  $\mathbb{Z}$ . Ясно, что  $a_0 = b_0 c_0$ . Поскольку  $a_0$  делится на  $p$ , но не делится на  $p^2$ , из простоты числа  $p$  вытекает, что  $p$  делит одно из чисел  $b_0$  и  $c_0$ , но не оба одновременно. Предположим, что  $p$  делит  $b_0$ , но не делит  $c_0$ . Если  $p$  делит все коэффициенты многочлена  $g$ , то оно делит и все коэффициенты многочлена  $f$ , включая  $a_n$ .

Следовательно, существует индекс  $i$  такой, что  $p$  не делит  $b_i$ . Пусть  $i$  — минимальный индекс с таким свойством. Ясно, что  $\deg g < \deg f$ , и потому  $i \leq k < n$ . В частности,  $p$  делит  $a_i$ . По определению произведения многочленов имеем

$$a_i = b_i c_0 + b_{i-1} c_1 + \dots \quad (2)$$

Поскольку  $p$  делит  $a_i$  и  $b_j$  для всех  $j < i$ , из (2) вытекает, что  $p$  делит  $b_i c_0$ . Но это невозможно, так как  $p$  не делит ни  $b_i$ , ни  $c_0$ .  $\square$

Критерий Эйзенштейна показывает, что с точки зрения строения неприводимых многочленов поле  $\mathbb{Q}$  разительно отличается от полей  $\mathbb{R}$  и  $\mathbb{C}$ . В самом деле, как мы видели выше, всякий неприводимый над  $\mathbb{C}$  многочлен линеен, а всякий неприводимый над  $\mathbb{R}$  многочлен имеет степень  $\leq 2$ . В то же время, в силу критерия Эйзенштейна степень неприводимого над  $\mathbb{Q}$  многочлена может быть любой. Например, неприводимым над  $\mathbb{Q}$  является многочлен  $x^n - 2$ , где  $n$  — произвольное натуральное число (он удовлетворяет посылке критерия Эйзенштейна при  $p = 2$ ).

Следующее утверждение позволяет отыскивать рациональные корни многочленов с целыми коэффициентами (если они существуют, конечно).

## Предложение о рациональных корнях многочленов

Пусть  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  — многочлен над  $\mathbb{Q}$  с целыми коэффициентами, а  $\frac{p}{q}$  — рациональное число и несократимая дробь. Если  $\frac{p}{q}$  — корень многочлена  $f(x)$ , то  $p$  является делителем  $a_0$ , а  $q$  — делителем  $a_n$ . В частности, если  $a_n \in \{1, -1\}$ , то все рациональные корни многочлена  $f(x)$  являются целыми числами и делят свободный член  $a_0$ .

**Доказательство.** Поскольку  $\frac{p}{q}$  — корень многочлена  $f(x)$ , имеем:

$a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_1 \cdot \frac{p}{q} + a_0 = 0$ . Умножив обе части этого

равенства на  $q^n$ , получим:  $a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$ .

Отсюда получаем:  $a_0 q^n = p(-a_n p^{n-1} - a_{n-1} p^{n-2} q - \dots - a_1 q^{n-1})$ . Поэтому  $p$  делит  $a_0 q^n$ . Так как числа  $p$  и  $q$  взаимно просты,  $p$  делит  $a_0$ .

Аналогично, из равенства  $a_n p^n = q(-a_{n-1} p^{n-1} - \dots - a_1 p q^{n-2} - a_0 q^{n-1})$  вытекает, что  $q$  делит  $a_n$ . □