# Глава IV. Многочлены

# §5. Многочлены над полем $\mathbb{Q}$

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)

# Подбор рациональных корней

Отыскивать рациональные корни многочленов с целочисленными коэффициентами помогает следующее утверждение.

**Предложение**

Пусть $f(x) = m_0x^n + m_1x^{n-1} + \ldots + m_{n-1}x + m_n$ – многочлен с целочисленными коэффициентами, $p/q$ – рациональное число и несократимая дробь. Если $p/q$ – корень многочлена $f(x)$, то $p$ является делителем $m_n$, $q$ является делителем $m_0$ и для любого целого числа $s$ число $f(s)$ делится на $p - qs$. В частности, если $m_0 = 1$ или $m_0 = -1$, то все рациональные корни многочлена $f(x)$ являются целыми числами и делят свободный член $m_n$.

⇓Запишем

$$f\left(\frac{p}{q}\right) = m_0\left(\frac{p}{q}\right)^n + m_1\left(\frac{p}{q}\right)^{n-1} + \ldots + m_{n-1}\frac{p}{q} + m_n, \qquad (1)$$

тогда $m_0(\frac{p}{q})^n + m_1(\frac{p}{q})^{n-1} + \ldots + m_{n-1}\frac{p}{q} + m_n = 0$. Умножим обе части этого равенства на $q^n$: $m_0p^n + m_1p^{n-1}q + \ldots + m_{n-1}pq^{n-1} + m_nq^n = 0$. Отсюда получаем $m_nq^n = -m_0p^n - m_1p^{n-1}q - \ldots - m_{n-1}pq^{n-1}$, поэтому число $p$ делит $m_nq^n$. Так как числа $p, q$ взаимно просты, $p$ делит $m_n$.

# Окончание доказательства

Аналогично доказывается, что $q$ делит $m_0$.
Для доказательства последнего утверждения предложения запишем $f(s) = m_0 s^n + m_1 s^{n-1} + \ldots + m_{n-1} + m_n$ и вычтем из этого равенства равенство (1) сл.2. Тогда будем иметь

$$f(s) = m_0 \left( s^n - \left(\frac{p}{q}\right)^n \right) + m_1 \left( s^{n-1} - \left(\frac{p}{q}\right)^{n-1} \right) + \ldots + m_{n-1} \left( s - \frac{p}{q} \right).$$

Умножив обе части этого равенства на $q^n$, получим
$q^n f(s) = m_0(s^n q^n - p^n) + q m_1 (s^{n-1} q^{n-1} - p^{n-1}) + \ldots + q^{n-1} m_{n-1}(sq - p)$.
Заметим, что

$$x^\ell - y^\ell = (x - y)(x^{\ell-1} + x^{\ell-2} y + \ldots + x y^{\ell-2} + y^{\ell-1})$$

для любых скаляров $x, y$ и любого целого числа $\ell > 1$.
Отсюда следует, что $sq - p$ делит $s^\ell q^\ell - p^\ell$ при любом натуральном $\ell$ и значит $sq - p$ делит $q^n f(s)$. Так как $(q^n, sq - p) = 1$ при любом целом $s$, заключаем, что $sq - p$ делит $f(s)$. Предложение доказано.⇑

# Пример 1

Найти рациональные корни многочлена $f(x) = x^4 - 2x^3 - 19x^2 - 24x - 36$.

Решение. В силу предложения, если этот многочлен имеет целочисленные корни, то они находятся среди делителей числа $-36$. Это число имеет 18 делителей: 1, $-1$, 2, $-2$, 3, $-3$, 4, $-4$, 6, $-6$, 9, $-9$, 12, $-12$, 18, $-18$, 36 и $-36$. Вычислим сначала $f(1) = -80$ и $f(-1) = -28$. Среди делителей $p$ числа $-36$ (кроме $1, -1$) выберем такие, чтобы число $p + 1$ делило $f(-1) = -28$ и $p - 1$ делило $f(1) = -80$. Делители $2, -2$ не годятся. Делители $3, -3$ и $6$ годятся, делители $4, -4, -6, 9, -9, 12, -12$ – нет. Вычисляем $f(3)$ и $f(-3)$ по схеме Горнера. Если получается нуль, то вычисляем значение частного от $6$.

| | 1 | $-2$ | $-19$ | $-24$ | $-36$ |
|---|---|---|---|---|---|
| 3 | 1 | 1 | $-16$ | $-72$ | $-252$ |
| $-3$ | 1 | $-5$ | $-4$ | $-12$ | 0 |
| 6 | 1 | 1 | 2 | 0 | |

Итак, мы нашли два корня многочлена $f(x)$: $x_1 = -3$, $x_2 = 6$. По схеме Горнера получаем, что $f(x) = (x + 3)(x - 6)(x^2 + x + 2)$. Осталось найти корни многочлена $h(x) = x^2 + x + 2$, т.е. решить уравнение $x^2 + x + 2 = 0$. Так как дискриминат квадратного трехчлена отрицательный, последнее уравнение не имеет действительных, а потому и рациональных корней.

# Пример 2

Найти рациональные корни многочлена
$f = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6.$

Решение. В силу предложения, если этот многочлен имеет рациональные корни, то они имеют вид несократимых дробей $\frac{p}{q}$, где $p|6$ (берем все делители), $q|24$ (берем только положительные делители). Подставляем в многочлен те дроби, для которых $p+q$ делит $f(-1) = -21$ и $p-q$ делит $f(1) = 15$. Числа $p$ и $q$ берем из таблицы, минус означает, что дробь подставлять не нужно. Строки, соответствующие делителям $6$, $8$, $12$, $24$ в таблице не приведены, так как не используются при нахождении корней.

| $q\backslash p$ | $1$ | $-1$ | $2$ | $-2$ | $3$ | $-3$ | $6$ | $-6$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | - | - | ? | ? | - | - | ? | - |
| $2$ | ? | - | - | - | - | ? | - | - |
| $3$ | - | - | - | ? | - | - | ? | - |
| $4$ | - | ? | - | - | ? | - | - | - |

Значения многочлена вычисляем по схеме Горнера в одной таблице на следующем слайде.

# Окончание решения примера 2

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 24 | 10 | $-1$ | $-19$ | $-5$ | 6 | |
| 2 | 24 | 58 | 115 | 211 | 417 | 840 | не корень |
| $-2$ | 24 | $-38$ | 75 | $-169$ | 333 | $-660$ | не корень |
| 6 | 24 | 154 | 923 | 5519 | 33109 | 198660 | не корень |
| $\frac{1}{2}$ | 24 | 22 | 10 | $-14$ | $-12$ | 0 | корень |
| | 12 | 11 | 5 | $-7$ | $-6$ | | сократили на 2 |
| $-\frac{3}{2}$ | 12 | $-7$ | $\frac{31}{2}$ | $-\frac{165}{4}$ | $\frac{543}{8}$ | | не корень |
| $-\frac{2}{3}$ | 12 | 3 | 3 | $-9$ | 0 | | корень |
| | 4 | 1 | 1 | $-3$ | | | сократили на 3 |
| $-\frac{1}{4}$ | 4 | 0 | $-1$ | $-\frac{11}{4}$ | | | не корень |
| $\frac{3}{4}$ | 4 | 4 | 4 | 0 | | | корень |

Имеем $f = (x - \frac{1}{2})(24x^4 + 22x^3 + 10x^2 - 14x - 12) =$
$(2x - 1)(12x^4 + 11x^3 + 5x^2 - 7x - 6) =$
$(2x - 1)(x + \frac{2}{3})(12x^3 + 3x^2 + 3x - 9) = (2x - 1)(3x + 2)(4x^3 + x^2 + x - 3) =$
$(2x - 1)(3x + 2)(x - \frac{3}{4})(4x^2 + 4x + 4) = (2x - 1)(3x + 2)(4x - 3)(x^2 + x + 1).$

Так как многочлен $x^2 + x + 1$ не имеет действительных корней, рациональные корни многочлена $f$ есть $\frac{1}{2}$, $-\frac{2}{3}$, $\frac{3}{4}$.

**Определение**

Наибольший общий делитель всех коэффициентов многочлена $f \in \mathbb{Z}[x]$ называется его *содержанием* и обозначается $c(f)$.

Многочлен $f \in \mathbb{Z}[x]$ называется *примитивным*, если $c(f) = 1$. Очевидно, что для любого $f \in \mathbb{Z}[x]$, $f \neq 0$, существует единственный примитивный многочлен $g$ такой что $f = c(f)g$.

**Лемма Гаусса**

$\forall f, g \in \mathbb{Z}[x]\ c(f \cdot g) = c(f) \cdot c(g)$. В частности, произведение двух примитивных многочленов является примитивным многочленом.

⇓Достаточно доказать последнее утверждение. Пусть $p$ – простое число и $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k$ и $g = \beta_0 + \beta_1 x + \ldots + \beta_n x^n$ – примитивные многочлены. Поскольку $c(f) = 1$, существует наименьший индекс $\ell$ такой что $p$ не делит $\alpha_\ell$ (возможно $\ell = 0$). Аналогично, существует наименьший индекс $m$ такой что $p$ не делит $\beta_m$ (возможно $m = 0$). Тогда $p$ не делит $\alpha_\ell \beta_m$. Коэффициент $\gamma$ при $x^{\ell+m}$ в произведении $h = fg$ равен $\sum_{s+t=\ell+m} \alpha_s \beta_t$. В этой сумме все ненулевые слагаемые, кроме $\alpha_\ell \beta_m$, делятся на $p$, так как при $s > \ell$ $t < m$ и при $t > m$ $s < \ell$. Следовательно, $\gamma$ не делится на $p$. Таким образом, $h$ – примитивный многочлен.⇑

# Связь неприводимости над полем $\mathbb{Q}$ и кольцом $\mathbb{Z}$

Неприводимость многочлена над кольцом $\mathbb{Z}$ определяется аналогично неприводимости над полем (сл.9 §2).

**Теорема**

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

$\Downarrow$Так как $\mathbb{Z} \subset \mathbb{Q}$, очевидно, что из неприводимости многочлена $f \in \mathbb{Z}[x]$ над полем $\mathbb{Q}$ следует его неприводимость над кольцом $\mathbb{Z}$. Пусть многочлен $f \in \mathbb{Z}[x]$ неприводим над кольцом $\mathbb{Z}$ и пусть $f = gh$, где $g, h \in \mathbb{Q}[x]$. Легко понять, что $g = \frac{m}{n} g_1$, $h = \frac{\ell}{k} h_1$, где $m, n, \ell, k \in \mathbb{N}$, $g_1, h_1 \in \mathbb{Z}[x]$ и $c(g_1) = c(h_1) = 1$. По лемме Гаусса (сл.7) $c(g_1 h_1) = 1$. Из равенства $f = \frac{m}{n} \frac{\ell}{k} g_1 h_1$ следует $nkf = m\ell g_1 h_1$ и $c(nkf) = c(m\ell g_1 h_1)$, откуда $nk \cdot c(f) = m\ell \cdot c(g_1 h_1) = m\ell$. Значит, $\frac{m}{n} \cdot \frac{\ell}{k} = c(f)$. Положим $q = c(f)$. Имеем $f = (qg_1)h_1$ – произведение двух многочленов из $\mathbb{Z}[x]$. Из неприводимости $f$ над кольцом $\mathbb{Z}$ следует, что $\deg(qg_1) = 0$ или $\deg(h_1) = 0$. В первом случае имеем $\deg(g) = 0$, а во втором – $\deg(h) = 0$. Следовательно, $f$ неприводим над полем $\mathbb{Q}$.$\Uparrow$

В силу теоремы сл.8 проблема выяснения неприводимости многочленов из $\mathbb{Q}[x]$ над полем $\mathbb{Q}$ полностью сводится к соответствующей проблеме для многочленов из $\mathbb{Z}[x]$ над кольцом $\mathbb{Z}$. Простого утверждения, дающего необходимые и достаточные условия неприводимости многочлена из $\mathbb{Z}[x]$ над кольцом $\mathbb{Z}$, не существует. Приведем одно достаточное условие.

**Теорема (признак Эйзенштейна)**

Пусть многочлен $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k \in \mathbb{Z}[x]$. Если существует простое число $p$, которое делит коэффициенты $\alpha_{k-1}, \ldots, \alpha_0$, но не делит $\alpha_k$ и $p^2$ не делит $\alpha_0$, то многочлен $f$ неприводим над полем $\mathbb{Q}$.

$\Downarrow$От противного, ввиду теоремы сл.8, предположим, что $f = gh$, где $g = \beta_0 + \beta_1 x + \ldots + \beta_m x^m$, $h = \gamma_0 + \gamma_1 x + \ldots + \gamma_n x^n$ – многочлены из $\mathbb{Z}[x]$ и $\deg(g), \deg(h) < \deg(f)$. Тогда $\alpha_s = \sum_{j+\ell=s} \beta_j \gamma_\ell$ при $s = 0, 1, \ldots, k$ и $k = m + n$. Так как $p$ делит $\alpha_0 = \beta_0 \gamma_0$, а $p^2$ не делит $\alpha_0$, заключаем, что лишь одно из чисел $\beta_0, \gamma_0$ делится на $p$. Для определенности пусть $\beta_0$ делится на $p$, а $\gamma_0$ не делится на $p$. Так как $\alpha_1 = \beta_0 \gamma_1 + \beta_1 \gamma_0$, заключаем, что $\beta_1 \gamma_0 = \alpha_1 - \beta_0 \gamma_1$ делится на $p$, и следовательно $\beta_1$ делится на $p$. Индукцией по $j$ покажем, что $\beta_j$ делится на $p$ при $j = 0, 1, \ldots, m$. Предположим, что уже доказано, что $\beta_0, \ldots, \beta_{j-1}$ делятся на $p$. Так как $\alpha_j = \sum_{q+\ell=j} \beta_q \gamma_\ell$, имеем $\beta_j \gamma_0 = \alpha_j - \sum_{q+\ell=j, q<j} \beta_q \gamma_\ell$, откуда следует требуемое. Таким образом, $\beta_m$ делится на $p$, и потому $\alpha_k = \beta_m \gamma_n$ делится на $p$. Полученное противоречие завершает доказательство теоремы.$\Uparrow$

# Пример

Фердинанд Готтхольд Макс Эйзенштейн (1823-1852).
Непосредственное применение признака Эйзенштейна не представляет трудностей. Иногда удается сделать замену переменной так, что становится возможным применить признак Эйзенштейна. При этом используется следующее очевидное

**Наблюдение**

Многочлен $f(x) \in \mathbb{Z}[x]$ неприводим над полем $\mathbb{Q}$ тогда и только тогда, когда для некоторого $r \in \mathbb{Z}$ многочлен $f(x-r)$ неприводим над полем $\mathbb{Q}$.

Покажем, что многочлен $x^4+x^3+x^2+x+1$ неприводим над полем $\mathbb{Q}$. Для этого сделаем замену $y = x-1$. Имеем

$$x^4+x^3+x^2+x+1 = \frac{x^5-1}{x-1} = \frac{(y+1)^5-1}{y} = y^4+5y^3+10y^2+10y+5.$$

Многочлен $y^4+5y^3+10y^2+10y+5$ неприводим над полем $\mathbb{Q}$ согласно признаку Эйзенштейна (сл.9) с $p=5$, поэтому многочлен $x^4+x^3+x^2+x+1$ также неприводим над полем $\mathbb{Q}$.

# Пример

Пусть $a_1, a_2, \ldots, a_n$ — различные целые числа. Доказать неприводимость над полем $\mathbb{Q}$ многочлена $(x - a_1)(x - a_2) \cdots (x - a_n) - 1$.

От противного, пусть многочлен $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) - 1$ приводим: $f(x) = g(x)h(x)$, где $g(x), h(x) \in \mathbb{Z}[x]$ и $\deg(g(x)), \deg(h(x)) < \deg(f(x))$, причем старшие коэффициенты многочленов $g(x), h(x)$ равны $1$. Так как при всех $i = 1, 2, \ldots, n$ $f(a_i) = -1$, из $g(a_i)h(a_i) = -1$ и $g(a_i), h(a_i) \in \mathbb{Z}$ следует $g(a_i) = \pm 1$, $h(a_i) = \mp 1$ и $g(a_i) + h(a_i) = 0$. Поскольку $\deg(g(x) + h(x)) < n$, $g(x) + h(x) = 0$ и $g(x) = -h(x)$. Таким образом, $f(x) = -g(x)^2$. Получаем противоречие: старший коэффициент многочлена $f(x)$ равен $1$, а старший коэффициент многочлена $-g(x)^2$ равен $-1$.

# Интерполяционный многочлен Лагранжа

Согласно теореме сл.44 §3 гл.II для любых попарно различных целых чисел $m_0, m_1, \ldots, m_n$ и произвольных целых чисел $k_0, k_1, \ldots, k_n$ существует единственный многочлен $f(x) \in \mathbb{Q}[x]$ такой, что $\deg(f) \leq n$ и $f(m_i) = k_i$ при всех $i = 0, 1, \ldots, n$. Он называется *интерполяционным многочленом*.

Одна из явных формул для интерполяционного многочлена — формула Лагранжа:

$$L_{(m_0,\ldots,m_n;k_0,\ldots,k_n)}(x) = \sum_{i=0}^{n} k_i \prod_{1\leq j\leq n, j\neq i} \frac{(x-m_j)}{(m_i-m_j)}.$$

При применении этой формулы с различными наборами целых чисел $k_0, k_1, \ldots, k_n$ и одним и тем же набором попарно различных целых чисел $m_0, m_1, \ldots, m_n$ целесообразно сначала вычислить при $i = 0, 1, \ldots n$ многочлены $p_i(x) =$

$$= \prod_{1\leq j\leq n, j\neq i} \frac{(x-m_j)}{(m_i-m_j)} = \frac{(x-m_0)\ldots(x-m_{i-1})(x-m_{i+1})\ldots(x-m_n)}{(m_i-m_0)\ldots(m_i-m_{i-1})(m_i-m_{i+1})\ldots(m_i-m_n)},$$

а затем вычислять интерполяционные многочлены Лагранжа

$$L_{(m_0,\ldots,m_n;k_0,\ldots,k_n)}(x) = \sum_{i=0}^{n} k_i p_i(x).$$

# Алгоритм Кронекера

Этот алгоритм позволяет проверить, является ли многочлен $g(x) \in \mathbb{Q}[x]$ степени $n > 1$ неприводимым над полем $\mathbb{Q}$.
Положим $\ell = [n/2]$ (целая часть числа $n/2$). Найдем многочлен $h(x) \in \mathbb{Z}[x]$, ассоциированный с $g(x)$. Очевидно, $g(x)$ приводим над полем $\mathbb{Q}$ тогда и только тогда, когда $h(x)$ приводим над кольцом $\mathbb{Z}$. Выберем попарно различные целые числа $m_0, m_1, \ldots, m_\ell$ и положим $k_i = h(m_i)$ для $i = 0, 1, \ldots, \ell$. Если $k_i = 0$ для некоторого $i \in \{0, 1, \ldots, \ell\}$, то $h(x)$ имеет корень $m_i$, поэтому $h(x)$ приводим и следовательно $g(x)$ приводим. Предположим, что $k_i \neq 0$ для всех $i = 0, 1, \ldots, \ell$. Рассмотрим всевозможные наборы $(s_0, s_1, \ldots, s_\ell)$ целых чисел таких, что $s_i$ делит $k_i$ при $i = 0, 1, \ldots, \ell$. Очевидно, что множество всех таких наборов конечно. Для каждого такого набора построим интерполяционный многочлен Лагранжа

$$L_{(m_0,\ldots,m_\ell;s_0,s_1,\ldots,s_\ell)}(x).$$

Если построенный многочлен имеет степень $0$, то отбросим его. Если один из построенных многочленов ненулевой степени делит $h(x)$, то $h(x)$ приводим и следовательно $g(x)$ приводим. Если же ни один из указанных многочленов не делит $h(x)$, то $h(x)$ неприводим и следовательно $g(x)$ неприводим.

# Обоснование алгоритма Кронекера

Ясно, что в обосновании нуждается только последний шаг алгоритма — заключение о неприводимости $h(x)$. Предположим, от противного, что многочлен $h(x)$ приводим, а ни один многочленов $L_{(m_0,\ldots,m_\ell;s_0,s_1,\ldots,s_\ell)}(x)$ ненулевой степени не делит $h(x)$.
Если многочлен $h(x)$ приводим над полем $\mathbb{Q}$, то согласно теореме сл.8 §5 гл.IV он приводим и над кольцом $\mathbb{Z}$, и потому может быть представлен в виде произведения $h_1(x) \cdot h_2(x)$, где $h_1(x), h_2(x) \in \mathbb{Z}[x]$ и $\deg(h_1(x)), \deg(h_2(x)) < \deg(h(x))$. При этом $\deg(h(x)) = \deg(h_1(x)) + \deg(h_2(x))$ и следовательно условия $\deg(h_1(x)), \deg(h_2(x)) > \ell = [n/2]$ выполняться не могут. Предположим (без ограничения общности), что $\deg(h_1(x)) \leq \ell$. Тогда набор значений $(h_1(m_0), h_1(m_1), \ldots, h_1(m_\ell))$ обладает тем свойством, что каждое целое число $h_1(m_i)$ делит целое число $h(m_i) = k_i$ при всех $i = 0, 1, \ldots, \ell$. Таким образом, этот набор совпадает с одним из наборов $(s_0, s_1, \ldots, s_\ell)$, выбранных в алгоритме Кронекера. Поэтому $h_1(x) = L_{(m_0,\ldots,m_\ell;s_0,s_1,\ldots,s_\ell)}(x)$ — противоречие с утверждением, что ни один из таких многочленов не делит $h(x)$.

# Пример применения алгоритма Кронекера

Выяснить, приводим ли над полем $\mathbb{Q}$ многочлен $f(x) = x^4 - 3x^3 + 2x^2 + 1$.
Находим $\ell = [\deg(f(x))/2] = 2$. Положим $m_0 = 0$, $m_1 = 1$, $m_2 = 2$. Имеем $f(0) = 1$, $f(1) = 1$, $f(2) = 1$. Так как среди значений $f(m_i)$ нет нуля, нужно вычислить $p_0(x) = \frac{(x-1)(x-2)}{(0-1)(0-2)} = \frac{1}{2}(x^2 - 3x + 2)$,
$p_1(x) = \frac{(x-0)(x-2)}{(1-0)(1-2)} = -x^2 + 2x$, $p_2(x) = \frac{(x-0)(x-1)}{(2-0)(2-1)} = \frac{1}{2}(x^2 - x)$.
Каждое из чисел $f(m_i)$ имеет два делителя – $1$ и $-1$, поэтому имеется 8 наборов $(s_0, s_1, s_2)$ значений для построения интерполяционных многочленов. Так как $L_{(0,1,2;-s_0,-s_1,-s_2)}(x) = -L_{(0,1,2;s_0,s_1,s_2)}(x)$, достаточно рассматривать наборы $(s_0, s_1, s_2)$, где $s_0 = 1$. Их всего 4:
$L_{(0,1,2;1,1,1)} = p_1(x) + p_2(x) + p_3(x) = 1$ – это скаляр, отбрасывается;
$L_{(0,1,2;1,-1,1)} = p_1(x) - p_2(x) + p_3(x) = 2x^2 - 4x + 1$ – не делит $f(x)$ (проверить самостоятельно);
$L_{(0,1,2;1,1,-1)} = p_1(x) + p_2(x) - p_3(x) = -x^2 + x + 1$ – не делит $f(x)$ (проверить самостоятельно);
$L_{(0,1,2;1,-1,-1)} = p_1(x) - p_2(x) - p_3(x) = x^2 - 3x + 1$ – не делит $f(x)$ (проверить самостоятельно).
В соответствии с алгоритмом Кронекера заключаем, что многочлен $f(x)$ неприводим над полем $\mathbb{Q}$.