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.

	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 $\dfrac{1}{2}, -\dfrac{2}{3}, \dfrac{3}{4}$.

Определение

Многочлен $f \in \mathbb{Z}[x]$ называется *примитивным*, если $f \neq 0$ и наибольший общий делитель всех коэффициентов многочлена f равен 1.

Очевидно, что для любого $g \in \mathbb{Z}[x]$, $g \neq 0$, существует единственный примитивный многочлен f такой что $g = mf$, где m – наибольший общий делитель всех коэффициентов многочлена g.

Лемма Гаусса

Произведение двух примитивных многочленов является примитивным многочленом.

$\Downarrow$Пусть $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k$ и $g = \beta_0 + \beta_1 x + \ldots + \beta_n x^n$ – примитивные многочлены. Пусть p – простое число. Поскольку f – примитивный многочлен, существует наименьший индекс ℓ такой что p не делит α_ℓ (возможно $\ell = 0$). Аналогично, существует наименьший индекс m такой что p не делит β_m (возможно $m = 0$). Тогда p не делит $\alpha_\ell \beta_m$. Коэффициент γ при $x^{\ell+m}$ в $h = fg$ 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, γ не делится на p. Таким образом, h – примитивный многочлен.$\Uparrow$

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 $g, h \in \mathbb{Q}[x]$. Тогда легко понять, что $g = \frac{m}{n} g_1$, $h = \frac{\ell}{k} h_1$, где $m, n, \ell, k \in \mathbb{N}$, $g_1, h_1 \in \mathbb{Z}[x]$ – примитивные многочлены. По лемме Гаусса (сл.7) произведение $g_1 h_1$ – примитивный многочлен. Так как $f = gh = \frac{m}{n} \frac{\ell}{k} g_1 h_1$, по этой причине в произведении дробей $\frac{m}{n} \cdot \frac{\ell}{k}$ знаменатели сокращаются с числителями, и указанное произведение – натуральное число. Обозначим его через q. 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 $\mathbb{Q}$. Теорема доказана.$\Uparrow$

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 α_k и p^2 не делит α_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 α_0, заключаем, что лишь одно из чисел β_0, γ_0 делится на p. Для определенности пусть β_0 делится на p, а γ_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 β_1 делится на p. Индукцией по j покажем, что β_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, β_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.

Глава IV. Многочлены

§ 6. Разложение рациональных дробей на простейшие

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 K – область целостности. Положим $P = K \times (K \setminus \{0\})$. Определим отношение ρ на множестве P:

$$(a, x)\rho(b, y) \Leftrightarrow a \cdot y = x \cdot b$$

Предложение

Отношение ρ является отношением эквивалентности на множестве P.

$\Downarrow$Отношение ρ рефлексивно, так как $a \cdot x = x \cdot a \Rightarrow (a, x)\rho(a, x)$. Оно симметрично: $(a, x)\rho(b, y) \Rightarrow a \cdot y = x \cdot b \Rightarrow b \cdot x = y \cdot a \Rightarrow (b, y)\rho(a, x)$. Проверим, что отношение ρ транзитивно. Пусть $(a, x)\rho(b, y)\rho(c, z)$. Тогда $a \cdot y = x \cdot b$ и $b \cdot z = y \cdot c$. Умножим обе части равенства $a \cdot y = x \cdot b$ на z: $a \cdot y \cdot z = x \cdot b \cdot z$ и используем равенство $b \cdot z = y \cdot c$: $a \cdot y \cdot z = x \cdot y \cdot c$, откуда $(a \cdot z - x \cdot c) \cdot y = 0$. Так как $y \neq 0$ и K – кольцо без делителей нуля, $a \cdot z - x \cdot c = 0$ и $a \cdot z = x \cdot c$, т.е. $(a, x)\rho(c, z)$.$\Uparrow$

Положим $F = P/\rho$ и обозначим класс $(a, x)^\rho$ через a/x. Определим на F операции сложения $a/x + b/y = (a \cdot y + b \cdot x)/(x \cdot y)$ и умножения $(a/x) \cdot (b/y) = (a \cdot b)/(x \cdot y)$.

Теорема и определение

Указанные операции определены корректно и относительно них $F = P/\rho$ является полем. Отображение $\varphi : K \longrightarrow F$, определенное правилом $\varphi(a) = a/1$, является изоморфизмом кольца K на подкольцо $\{a/1 | a \in K\}$ поля F.
Поле F называется *полем частных* области целостности K.

$\Downarrow$Проверим корректность определения сложения. Это означает, что если $a/x = a'/x'$, т.е. $(a, x)\rho(a', x')$, и $b/y = b'/y'$, то $a/x + b/y = a'/x' + b'/y'$.
Пусть $ax' = xa'$ и $by' = yb'$. Покажем, что $(ay + bx, xy)\rho(a'y' + b'x', x'y')$.
Имеем $(ay + bx)(x'y') = ayx'y' + bxx'y' = (ax')yy' + (by')xx' = xa'yy' + yb'xx' = (xy)(a'y' + b'x')$, т.е. $(ay + bx)(x'y') = (xy)(a'y' + b'x')$.
Аналогично проверяется корректность определения умножения.
Проверим, что $(F, +)$ – абелева группа. Так как $b/y + a/x = (bx + ay)/(yx)$, сложение коммутативно. Проверим его ассоциативность: $(a/x + b/y) + c/z = (ay + bx)/(xy) + c/z = ((ay + bx)z + xyc)/(xyz) = (ayz + bxz + xyc)/(xyz)$;
$a/x + (b/y + c/z) = a/x + (bz + cy)/(yz) = (ayz + (bz + cy)x)/(xyz) = (ayz + bzx + cyx)/(xyz)$.

Легко видеть, что элемент $0/1$ является нулем:
$a/x + 0/1 = (a \cdot 1 + 0 \cdot x)/(x \cdot 1) = a/x$ для любого элемента $a/x \in F$.
Наконец, элемент $(-a)/x$ будет противоположным к элементу $a/x \in F$:
$a/x + (-a)/x = (ax - ax)/(x^2) = 0/x^2 = 0/1$, так как $0/1 = 0/z$ для любого $z \in K \setminus \{0\}$.
Так как кольцо K коммутативное и ассоциативное, ясно, что операция умножения на F также является коммутативной и ассоциативной.
Для любого $z \in K \setminus \{0\}$ и любого $a/x \in F$ справедливо равенство $(az)/(xz) = a/x$.
Проверим, что F является кольцом: $(a/x + b/y)(c/z) =((ay + bx)/(xy))(c/z) =((ay + bx)c)/(xyz) =(ayc + bxc)/(xyz)$;
$(a/x)(c/z) + (b/y)(c/z) =(ac)/(xz) + (bc)/(yz) =(acyz + bcxz)/(xyz^2) =(acy + bcx)z/(xyz)z =(acy + bcx)/(xyz)$. Так как умножение в F коммутативно, этого достаточно.
Ясно, что $1/1$ является единицей кольца F. Для любого $a/x \neq 0/1$ справедливо $a \neq 0$ и поэтому элемент x/a является обратным к a/x:
$(a/x)(x/a) = (ax)/(xa) = 1/1$ Таким образом, F является полем.

Окончание доказательства

Так как $a/1 = b/1 \Longrightarrow a = b$, отображение $\varphi : a \mapsto a/1$ является инъективным. Очевидно, оно является сюръективным отображением на множество $K' = \{a/1 | a \in K\}$, т.е. биекцией.
Поскольку $a/1 + b/1 = (a+b)/1$ и $(a/1)(b/1) = (ab)/1$, множество K' замкнуто относительно операций сложения и умножения в поле F.
Проверим, что оно является кольцом относительно этих операций, т.е. подкольцом поля F.
(Одной замкнутости относительно операций сложения и умножения в поле недостаточно. Приведите пример подмножества поля $\mathbb{Q}$, замкнутого относительно сложения и умножения, но не являющегося подкольцом.)
Нуль $0/1$ содержится в K' и для любого $a/1 \in K'$ справедливо $(-a)/1 \in K'$. Остальные аксиомы, определяющие кольцо, используют только кванторы всеобщности, поэтому из их истинности в поле F следует истинность в его подмножестве K'.
Ясно, что отображение φ является изоморфизмом кольца K на кольцо $\{a/1 | a \in K\}$.$\Uparrow$
Обычно кольцо K отождествляется с подкольцом K' поля частных F, т.е. считается, что $K \subseteq F$.

Например, поле рациональных чисел $\mathbb{Q}$ изоморфно полю частных кольца целых чисел $\mathbb{Z}$.

Пусть теперь F – произвольное поле. Кольцо многочленов $F[x]$ является областью целостности (см. сл.4 §1). С помощью построения поля частных из кольца многочленов $F[x]$ строится поле рациональных дробей, которое обозначается через $F(x)$.

Определения

Рациональной дробью над полем F называется элемент поля частных $F(x)$, т.е. дробь $f(x)/g(x)$, где $f(x), g(x) \in F[x]$ и $g(x) \neq 0$.
Рациональная дробь $f(x)/g(x)$ называется *правильной*, если $\deg(f) < \deg(g)$.
Рациональная дробь $f(x)/g(x)$ называется *простейшей*, если $f \neq 0$, $g = p^n$ – некоторая степень неприводимого над полем F многочлена p и $\deg(f) < \deg(p)$.

Теорема

Любая правильная дробь может быть представлена в виде суммы простейших дробей. Это представление единственно с точностью до перестановки слагаемых.