

Неприводимые многочлены над \mathbb{Q}

Классификация многочленов над \mathbb{Q} - сложная задача.

Факт: $x^n + 2$ - неприводим над \mathbb{Q} , $\forall n \geq 2$. Это следует из критерия Эйзенштейна и будет рассмотрен в 3-м семестре.

Теорема 1. Пусть $f(x) \in \mathbb{Z}[x]$, то есть:

$$f(x) = a_n x^n + \dots + a_1 x + a_0, \quad a_i \in \mathbb{Z}$$

Тогда $x = \frac{u}{v}$, $u, v \in \mathbb{Z}$, $(u, v) = 1$ является корнем $f(x) \Rightarrow a_n : v, a_0 : v$.

□

$$\begin{aligned} 0 &= a_n \cdot \frac{u^n}{v^n} + \dots + a_1 \cdot \frac{u}{v} + a_0 \Rightarrow 0 = \underbrace{a_n u^n + \dots + a_1 u v^{n-1}}_{\text{делится на } u} + a_0 v^n \Rightarrow \\ &\Rightarrow -a_0 v^n = a_n u^n + \dots + a_1 u v^{n-1} : u \Rightarrow -a_0 v^n : u, (u, v) = 1 \Rightarrow (u, v^n) = 1 \end{aligned}$$

По аналогии:

$$0 = a_n u^n + \underbrace{a_{n-1} u^{n-1} v + \dots + a_1 v u^{n-1} + a_0 v^n}_{\text{делится на } v} \Rightarrow a_n u^n : v \Rightarrow a_n : v$$

■

Следствие 1. (Алгоритм нахождения всех корней $f(x) \in \mathbb{Q}[x]$)

- 1) $f(x) \in \mathbb{Q}[x] \Rightarrow g(x) \in \mathbb{Z}[x]$ - перейти от многочлена $\in \mathbb{Q}[x]$ к многочлену $\in \mathbb{Z}[x]$, домножив на НОК знаменателей рациональных коэффициентов. Понятно, что корни от этого не изменятся;
- 2) Перебрать все пары $(u, v): a_0 : u, a_n : v$. Можно считать, что $a_0 \neq 0, a_n \neq 0$. $a_n \neq 0$ как старший член. Если $a_0 = 0$, то 0 является корнем. Разделив уравнение на x в подходящей степени, получим уравнение с ненулевым свободным членом, либо корнями уравнения будут только нули. Множество делителей a_n и a_0 конечно \Rightarrow количество пар (u, v) конечно;
- 3) Подставляем все $\frac{u}{v}$ в $g(x)$ и находим корни;
- 4) (Схема Горнера) Находим кратности полученных корней;

Rm: 1. Заметим, что если мы нашли корни многочлена, это ещё не значит, что он распался на линейные множители. Возможно в разложении будет присутствовать множитель, который корней над данным полем не имеет.

Факт: Существует алгоритм Дедекинда разложения многочлена $f(x) \in \mathbb{Q}[x]$ на неприводимые множители над \mathbb{Q} .

Теорема выше - часть этого алгоритма, позволяющего найти линейные множители разложения. Оставшуюся часть также нужно разложить на неприводимые множители более высоких степеней и алгоритм Дедекинда описывает этот процесс.

Нахождение корней многочленов над полем \mathbb{R}

Мы видели, что разложение многочлена на неприводимые множители над \mathbb{R} или \mathbb{C} сводится к нахождению его комплексных корней. Отметим, что явных формул для выражения корней многочленов, которые выражают корни этих многочленов через их коэффициенты с помощью каких-то операций сложения, умножения, деления, извлечения корней не существует для многочленов степени выше 4.

Теорема 2. (Руффини-Абеля) Общее уравнение степени ≥ 5 не разрешимо в радикалах.

Термин общее уравнение здесь мы будем понимать как обычный многочлен степени n .

Вопрос о нахождении корней заданного многочлена, часто сводится к тому, что важны не точные значения корней, а приближенные. То есть нужно уметь находить корни многочлена приближенно со сколь угодно заданной точностью. Для этого достаточно уметь находить количество корней заданного многочлена в заданном интервале (для \mathbb{R})/заданной области комплексной плоскости (для \mathbb{C}).

Приближенное нахождение корней многочлена на заданном интервале

Пусть у нас есть некий многочлен $f \in \mathbb{R}[x]$ и мы умеем искать количество корней на любом интервале. У нас есть интервал и некоторое количество корней многочлена f на нем. Мы хотим найти эти корни со сколь угодно заданной точностью. Предположим, что мы посчитали общее количество корней на этом интервале, нашли сколько их и поделили интервал пополам. Затем посчитали сколько корней на каждой половине. Затем поделили каждую из половин ещё на две равные части и посчитали количество корней уже на них. Продолжаем эту процедуру.

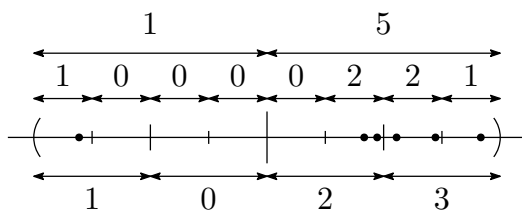


Рис. 1: Поиск корней на заданном интервале.

Рано или поздно, мы каждый из корней окружим таким маленьким интервалом, внутри которого он будет содержаться (только один корень) так, что мы найдем его со сколь угодно заданной точностью. Если мы умеем искать количество корней в любой области \mathbb{C} , то рассуждая точно также, мы можем эти корни локализовать - заключить в окрестности со сколь угодно малым радиусом.

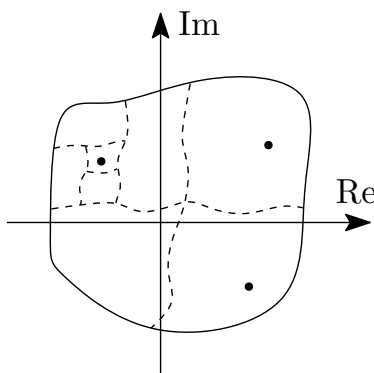


Рис. 2: Поиск корней на заданной плоскости.

Нахождение количества корней в интервале (\mathbb{R}) или области (\mathbb{C})

Есть несколько точных методов нахождения количества корней заданного многочлена на заданном интервале или на заданной области \mathbb{C} . Например, есть метод Штурма, метод подсчета изменения аргумента на \mathbb{C} . Но они обычно требуют достаточно больших вычислений. Мы разберём метод, который дает оценку сверху для $f \in \mathbb{R}[x]$ и не требует каких-либо вычислений. Пусть:

$$f \in \mathbb{R}[x], f(x) = a_0 + a_1x + \dots + a_nx^n$$

Рассмотрим последовательность коэффициентов этого многочлена: (a_0, a_1, \dots, a_n) .

Опр: 1. Скажем, что в члене a_k последовательности (a_0, a_1, \dots, a_n) имеет место перемена знака, если:

$$\exists l < k: a_k, a_l \neq 0, \operatorname{sgn}(a_k) \neq \operatorname{sgn}(a_l), a_{l+1} = a_{l+2} = \dots = a_{k-1} = 0$$

Таким образом, перемена знака происходит, когда последовательность коэффициентов имеет вид:

$$a_0, a_1, \dots, \underset{\pm}{a_l}, 0, \dots, 0, \underset{\mp}{a_k}, \dots, a_n$$

Обозначение: $L(f)$ - число перемен знака в последовательности коэффициентов (a_0, a_1, \dots, a_n) , без учета нулей.

Пример: $f(x) = 2 + 3x - 5x^3 + 4x^4 + x^6 - 6x^7$, тогда: $L(f) = 3: 3 \rightarrow -5 \rightarrow 4, 1 \rightarrow -6$.

Обозначение: $N(f)$ - число положительных корней многочлена f с учётом их кратностей.

Теорема 3. (Декарт)

- 1) $N(f) \leq L(f)$, причем равенство достигается, если f - не имеет мнимых корней;
- 2) $N(f) \equiv L(f) \pmod{2}$, то есть четность $N(f)$ такая же, как у $L(f)$;

Rm: 2. Другое название теоремы Декарта - **правило знаков**.

□

- (1) Пусть $a_n \neq 0, \deg(f) = n$. Заменяя f на $-f$ при необходимости, можно считать, что $a_n > 0$, при этом число положительных корней и число перемен знаков последовательности коэффициентов при такой замене не изменится. Поэтому доказав с этим условием, мы докажем и $\forall f \in \mathbb{R}[x]$. Тогда:

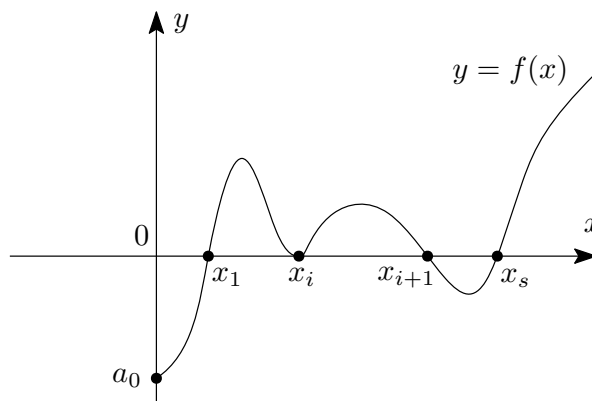
$$f(x) = a_kx^k + \dots + a_nx^n, a_k \neq 0, a_n > 0$$

где a_k - первый ненулевой коэффициент;

- (2) Поделим f на $x^k \Rightarrow$ можем считать, что $a_0 \neq 0$ и $n - k = n$. Число положительных корней не изменится, поскольку нулевые корни нас не интересуют. Число перемен знака тоже не изменится, поскольку в последовательности коэффициентов мы просто отрезаем кусок из нулей. Тогда:

$$f(x) = a_0 + \dots + a_nx^n, a_0 \neq 0, a_n > 0$$

Пусть: $x_1 < x_2 < \dots < x_s$ - все + корни f . Обозначим их кратности: k_1, k_2, \dots, k_s ;

Рис. 3: Многочлен $f(x)$ и его корни: $x_1 < x_2 < \dots < x_s$.

(3) Докажем, что $N(f) \equiv L(f) \pmod{2}$. Рассмотрим $\operatorname{sgn} f(x)$ при изменении x от 0 до $+\infty$:

- а) $x_i < x < x_{i+1} \Rightarrow \operatorname{sgn} f(x) = \operatorname{const} \Rightarrow$ надо посмотреть, что происходит при переходе через корень многочлена;
- б) Рассмотрим произвольный корень x_i кратности k_i , тогда:

$$f(x) = (x - x_i)^{k_i} \cdot g(x), \quad g(x_i) \neq 0$$

Следовательно, в окрестности точки x_i многочлен $g(x)$ имеет тот же самый знак, что и в точке $g(x_i) \neq 0$. Сдвигаясь вправо, получим:

$$x_i < x < x_i + \varepsilon \Rightarrow x - x_i > 0 \Rightarrow \operatorname{sgn} f(x) = \operatorname{sgn} g(x_i)$$

Сдвигаясь левее, получим:

$$x_i - \varepsilon < x < x_i \Rightarrow x - x_i < 0 \Rightarrow \operatorname{sgn} f(x) = (-1)^{k_i} \cdot \operatorname{sgn} g(x_i)$$

Если k_i - четное, то знак не поменяется, если нечетно, то знак поменяется;

- в) При $0 < x < \varepsilon \Rightarrow \operatorname{sgn} f(x) = \operatorname{sgn} a_0$;
- г) При $x \rightarrow +\infty$, вынесем x^n , тогда многочлен $f(x)$ приобретет вид:

$$f(x) = x^n \cdot \left(\frac{a_0}{x^n} + \frac{a_1}{x^{n-1}} + \dots + \frac{a_{n-1}}{x} + a_n \right) \Rightarrow \frac{a_0}{x^n} + \frac{a_1}{x^{n-1}} + \dots + \frac{a_{n-1}}{x} + a_n \xrightarrow{x \rightarrow +\infty} a_n$$

Поскольку $a_n > 0$, $x > 0$, тогда:

$$\exists C > 0, \forall x > C \Rightarrow \operatorname{sgn} f(x) = \operatorname{sgn} a_n > 0$$

Таким образом, при прохождении через корень кратности k , $\operatorname{sgn} f(x)$ меняется k раз \Rightarrow общее количество перемен знака = числу положительных корней, с учётом кратности. Если сумма кратных корней - чётна, то знак меняется четное число раз и не изменится при переходе от 0 к $+\infty$:

$$N(f) = k_1 + k_2 + \dots + k_s = 2m, \quad m \in \mathbb{N}, \quad a_n > 0 \Rightarrow a_0 > 0$$

Если коэффициенты $a_0 > 0$, $a_n > 0 \Rightarrow L(f)$ - чётно:

$$\left(\underset{+}{a_0}, \dots, \underset{+}{a_n} \right) \Rightarrow L(f) = 2k, \quad k \in \mathbb{N}$$

Если сумма кратных корней - нечётна, то:

$$N(f) = k_1 + k_2 + \dots + k_s = 2m + 1, m \in \mathbb{N}, a_n > 0 \Rightarrow a_0 < 0$$

аналогично, поскольку знак при переходе от 0 к $+\infty$ не меняется $\Rightarrow L(f)$ - нечётно:

$$\begin{matrix} (a_0, \dots, a_n) \\ - \quad \quad \quad + \end{matrix} \Rightarrow L(f) = 2k + 1, k \in \mathbb{N}$$

Следовательно: $N(f) \equiv L(f) \pmod{2}$ и пункт 2) - доказан;

- (4) Докажем, что $N(f') \geq N(f) - 1$. Положительные корни многочлена бывают простые и кратные. Если кратность корня x_i равна $k_i \geq 2$, то x_i является корнем f' , причем кратности $k_i - 1$. Если же кратность корня $k_i = 1$, то x_i - не корень f' (или корень кратности 0).

Вспомним из анализа **теорему Ролля**: если в двух крайних точках отрезка значения функции одинаковы, то где-то посередине существует корень из производной. В частности, между любыми двумя соседними корнями нашего многочлена есть корень производной.

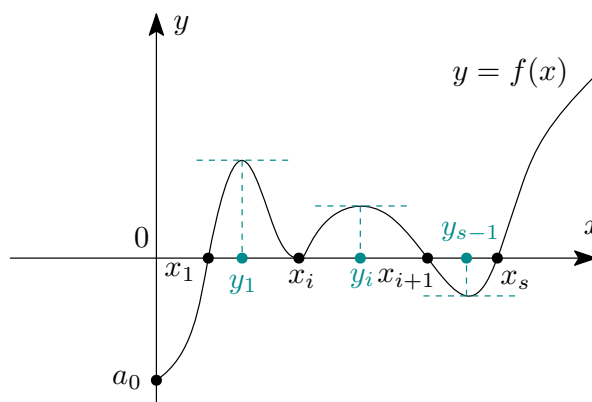


Рис. 4: Применение теоремы Ролля для нахождения корней производной многочлена f .

Таким образом, по теореме Ролля:

$$\exists y_i \in \mathbb{R}, x_i < y_i < x_{i+1}: f'(y_i) = 0$$

Следовательно, число корней производной многочлена как минимум будет не меньше суммы кратностей корней исходного многочлена, уменьшенных на единицу плюс число корней между корнями исходного многочлена:

$$N(f') \geq (k_1 - 1) + (k_2 - 1) + \dots + (k_s - 1) + s - 1 = k_1 + k_2 + \dots + k_s - s + s - 1 = N(f) - 1$$

где $s - 1$ - число корней f' между двумя соседними корня многочлена f , тогда:

- (5) Докажем, что $L(f') \leq L(f)$. Рассмотрим последовательность коэффициентов f :

$$(a_0, a_1, a_2, \dots, a_n)$$

Последовательность коэффициентов f' будет иметь вид:

$$(a_1, 2a_2, 3a_3, \dots, na_n)$$

С точностью до положительных множителей, это будут коэффициенты исходного многочлена, без учета первого члена $a_0 \Rightarrow$ число перемен знака в (a_1, \dots, a_n) равно $L(f') \Rightarrow$ может возникнуть максимум одна перемен знака $\Rightarrow L(f) \geq L(f')$;

(6) Докажем, что $N(f) \leq L(f)$. Будем доказывать индукцией по n :

База индукции: $n = 0 \Rightarrow f(x) = a_0 = \text{const} \Rightarrow N(f) = 0, L(f) = 0$.

Шаг индукции: Воспользуемся пунктом (4): $N(f) \leq N(f') + 1 \leq L(f') + 1$ - по предположению индукции. Тогда по (5):

$$N(f) \leq L(f') + 1 \leq L(f) + 1 \wedge N(f) \equiv L(f) \pmod{2} \Rightarrow N(f) \neq L(f) + 1 \Rightarrow N(f) \leq L(f)$$

(7) Пусть $\tilde{f}(x) = f(-x)$, тогда:

$$\tilde{f}(x) = a_0 - a_1x + a_2x^2 - a_3x^3 + \dots + (-1)^n \cdot a_n x^n$$

Покажем, что $L(f) + L(\tilde{f}) \leq n$. Если $a_k \neq 0, \forall k$, то на каждом k -ом месте ($k = 1, 2, \dots, n$) есть перемена знака либо в последовательности:

$$(a_0, \dots, a_{k-1}, a_k, \dots, a_n)$$

либо в последовательности:

$$(a_0, \dots, (-1)^{k-1} a_{k-1}, (-1)^k a_k, \dots, (-1)^n a_n)$$

Следовательно, суммарная перемена знака: $L(f) + L(\tilde{f}) = n$. В общем случае, если есть нулевые коэффициенты, то заменим эти $a_k = 0$ на ненулевые $\Rightarrow L(f)$ и $L(\tilde{f})$ могут только возрасти и после замены в сумме они станут равны n , а до неё они не больше n ;

(8) Число отрицательных корней f = числу положительных корней \tilde{f} :

$$f(x_k) = 0, x_k > 0 \Leftrightarrow \tilde{f}(-x_k) = f(x_k) = 0, -x_k < 0$$

(9) Если f не имеет мнимых корней $\Rightarrow N(f) + N(\tilde{f}) = n$. $x = 0$ - не является корнем, поскольку свободный член не равен 0. По (6) и (7) мы доказали:

$$\begin{aligned} N(f) \leq L(f) \wedge N(\tilde{f}) \leq L(\tilde{f}) &\Rightarrow n = N(f) + N(\tilde{f}) \leq L(f) + L(\tilde{f}) \leq n \Rightarrow \\ &\Rightarrow N(f) + N(\tilde{f}) = L(f) + L(\tilde{f}) = n \Rightarrow N(f) = L(f) \end{aligned}$$

■

Дополнение к правилу знаков:

1) Число отрицательных корней многочлена $f = N(\tilde{f}) \leq$ числа перемен знаков в последовательности:

$$(a_0, -a_1, a_2, -a_3, \dots, (-1)^n a_n)$$

то есть, с помощью правила Декарта мы можем оценить сверху количество отрицательных корней многочлена f ;

2) Разложим многочлен f по степеням $x - x_0$:

$$f(x) = c_0 + c_1(x - x_0) + \dots + c_n(x - x_0)^n$$

Число корней f , которые больше, чем $x_0 = N(f)_{>x_0} \leq L(f)_{>x_0}$ = число перемен знаков в последовательности:

$$(c_0, c_1, \dots, c_n)$$

или в последовательности:

$$(f(x_0), f'(x_0), \dots, f^{(n)}(x_0))$$

поскольку коэффициенты c_i связаны с $f^{(i)}(x_0)$ множителями, которые на знак не влияют. По этой же причине: $N(f)_{>x_0} \equiv L(f)_{>x_0} \pmod{2}$. Аналогично, с помощью 1) оценивается число корней, которые меньше x_0 ;

Упр. 1. Найти все действительные корни многочлена: $f(x) = x^4 - x^3 + x^2 - x - 1$ с точностью до знаков после запятой (с точностью до целых чисел).

Rm: 3. Правило знаков не позволяет отличать простые корни от кратных.

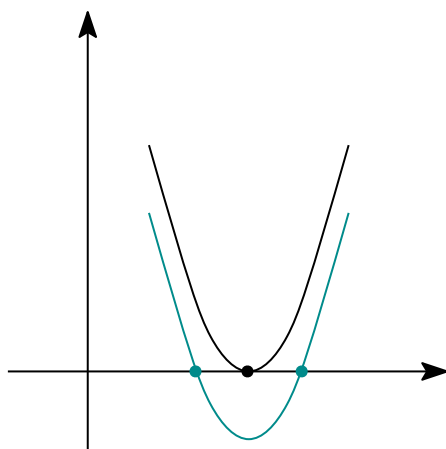


Рис. 5: Кратный корень не отличим от простого.

Два случая на картинке неотличимы друг от друга методом Декарта. Один двухкратный считается также, как два однократных, а хотелось бы различать.

Опр: 2. Приведенным многочленом f_{red} многочлена f называется многочлен: $f_{red} = \frac{f}{(f, f')}$.

Утв. 1. Пусть $\text{char } K = 0$ и $f \in K[x]$. Тогда f_{red} имеет те же корни, что и f , но все корни f_{red} - простые.

□

(\Rightarrow) $f = f_{red} \cdot (f, f')$, тогда если x_0 - корень $f_{red} \Rightarrow x_0$ - корень f .

(\Leftarrow) Пусть x_0 - корень f кратности $k \Rightarrow x_0$ - корень f' кратности $k - 1 \Rightarrow x_0$ также будет корнем (f, f') кратности $k - 1$ потому, что:

$$f : (x - x_0)^k \wedge f \not\vdash (x - x_0)^{k+1}, f' : (x - x_0)^{k-1} \wedge f' \not\vdash (x - x_0)^k \Rightarrow (f, f') : (x - x_0)^{k-1}$$

Следовательно, x_0 - корень f_{red} кратности 1, поскольку:

$$f(x) = (x - x_0)^k \cdot g(x) = f_{red} \cdot (x - x_0)^{k-1} \cdot p(x), g(x_0) \neq 0, p(x_0) \neq 0 \Rightarrow f_{red} = (x - x_0) \cdot q(x), q(x_0) \neq 0$$

■

Рм: 4. Заметим, что (f, f') находится с помощью алгоритма Евклида.

Утв. 2. Если $(f, f') = \text{const}$, то кратных корней нет.

□

$$f(x) = \alpha(x - x_1)^{k_1} \cdot \dots \cdot (x - x_s)^{k_s}, \quad k_1 + \dots + k_s = n$$
$$(f, f') = \beta(x - x_1)^{k_1-1} \cdot \dots \cdot (x - x_s)^{k_s-1} \Rightarrow (f, f') = \text{const} \Leftrightarrow k_1 = \dots = k_s = 1$$

■

Чтобы найти точное значение корня, можно попробовать найти (f, f') и отделить кратные корни. Есть вероятность, что после этого степень многочлена уменьшится до меньшей и корни можно будет найти по известным формулам.

Дроби

У кольца многочленов есть один недостаток: не любые два многочлена можно поделить один на другой без остатка. Иногда хочется уметь делить без всяких ограничений. По этой же самой причине, кольцо целых чисел расширили до поля рациональных чисел: в кольце целых чисел делить не всегда можно нацело, а в поле рациональных можно. Как произошел этот переход?

Задание рационального числа происходит следующим образом:

$$\forall r \in \mathbb{Q}, \exists m, n \in \mathbb{Z}, n \neq 0: r = \frac{m}{n}$$

Причем это задание - неоднозначно. Существует **правило пропорции**:

$$\frac{m}{n} = \frac{m'}{n'} \Leftrightarrow mn' = m'n$$

Операции над дробями:

(+):

$$\forall \frac{m}{n}, \frac{k}{l} \in \mathbb{Q}, \frac{m}{n} + \frac{k}{l} = \frac{ml + nk}{nl}$$

(·):

$$\forall \frac{m}{n}, \frac{k}{l} \in \mathbb{Q}, \frac{m}{n} \cdot \frac{k}{l} = \frac{m \cdot k}{n \cdot l}$$

Множество рациональных чисел является полем, поскольку:

$$\left(\frac{m}{n}\right)^{-1} = \frac{n}{m}$$

Вот таким образом происходит расширение кольца целых чисел до поля рациональных. Аналогичное расширение можно сделать и для кольца многочленов и для любого целостного кольца.

Расширение области целостности

Пусть A - произвольная область целостности. Рассмотрим множество $A \times (A \setminus \{0\})$ и введем на нем отношение эквивалентности.

Опр. 3. В множестве $A \times (A \setminus \{0\})$ будем говорить, что $(a, b) \sim (a', b')$, если $a \cdot b' = a' \cdot b$.

Утв. 3. Заданное отношение \sim является отношением эквивалентности.

□

1) **Рефлексивность:** $a \cdot b = a \cdot b \Rightarrow (a, b) \sim (a, b)$;

2) **Симметричность:** $a \cdot b' = a' \cdot b \Rightarrow a' \cdot b = a \cdot b' \Rightarrow (a, b) \sim (a', b') \Rightarrow (a', b') \sim (a, b)$;

3) **Транзитивность:** Пусть $(a, b) \sim (a', b') \sim (a'', b'')$, тогда:

$$\begin{aligned} a \cdot b' &= a' \cdot b \wedge a' \cdot b'' = a'' \cdot b' \Rightarrow a \cdot a' \cdot b' \cdot b'' = b \cdot a' \cdot b' \cdot a'' \Rightarrow \\ &\Rightarrow a' \neq 0 \Rightarrow a \cdot b'' = b \cdot a'' \Rightarrow (a, b) \sim (a'', b'') \end{aligned}$$

где мы сократили на $a' \cdot b'$, поскольку $b' \neq 0$ по условию и $a' \neq 0$. Если $a' = 0$, то:

$$a \cdot b' = a' \cdot b = 0, b' \neq 0 \Rightarrow a = 0, a' \cdot b'' = a'' \cdot b' = 0, b' \neq 0 \Rightarrow a'' = 0 \Rightarrow a \cdot b'' = a'' \cdot b \Rightarrow (a, b) \sim (a'', b'')$$



Опр: 4. Классы эквивалентности отношения \sim назовём дробями элементов из кольца A .

Обозначение: $\frac{a}{b}$ - класс, содержащий (a, b) .

Правило пропорции: $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow a \cdot b' = a' \cdot b$. В частности, из правила следует: $\frac{a}{b} = \frac{ac}{bc}, \forall c \neq 0$.

Операции над дробями:

$$(+): \forall \frac{a}{b}, \frac{c}{d} \in A \times (A \setminus \{0\}), \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd};$$

$$(\cdot): \forall \frac{a}{b}, \frac{c}{d} \in A \times (A \setminus \{0\}), \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d};$$

Корректность: Пусть $\frac{a}{b} = \frac{a'}{b'}$, $ab' = a'b$, тогда:

$$(+): \frac{ad + bc}{bd} = \frac{ab'd + bb'c}{bb'd} = \frac{a'bd + bb'c}{bb'd} = \frac{a'd + b'c}{b'd} \Rightarrow \text{операция сложения - корректна};$$

$$(\cdot): \frac{ac}{bd} = \frac{ab'c}{bb'd} = \frac{a'c}{b'd} \Rightarrow \text{операция умножения - корректна};$$

Опр: 5. Множество всех дробей (классов эквивалентностей) $Q(A)$ с введенными операциями сложения и умножения дробей называется полем дробей или полем частных или полем отношений кольца A :

$$Q(A) = \left\{ \frac{a}{b} \mid a, b \in A, b \neq 0 \right\}$$