Доказательство

1. Существование

Неполное частное $q(x)$ и остаток $r(x)$ находятся при помощи процедуры „деления углом".

Продемонстрируем это на примере. Пусть

$$f(x) = 4x^3 - 2x^2 + x - 1$$

$$g(x) = x^2 - x + 1$$

(здесь $F = \mathbb{R}$)

$$\begin{array}{r|l} -\,4x^3 - 2x^2 + x - 1 & x^2 - x + 1 \\ \underline{4x^3 - 4x^2 + 4x} & \overline{4x + 2} = q(x) \\ -\,2x^2 - 3x - 1 & \\ \underline{2x^2 - 2x + 2} & \\ x - 3 = r(x) & \end{array}$$

2. Единственность

Пусть $f(x) = g(x)\,q_1(x) + r_1(x) = g(x)\,q_2(x) + r_2(x)$ — два способа поделить $f(x)$ на $g(x)$ с остатком.

Имеем:

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

Если допустить, что $q_1(x) \neq q_2(x)$, то $r_2(x) - r_1(x) \neq 0$ и $\deg(r_2(x) - r_1(x)) < \deg g(x)$,

$$\deg(g(x)(q_1(x) - q_2(x))) \geq \deg g(x) > \deg(r_1(x) - r_2(x))$$

противоречие, след-но $q_1(x) = q_2(x)$ и $r_1(x) = r_2(x)$.

Опр. Пусть $f_1(x), \dots, f_m(x) \in F[x]$ — многочлены, среди к-рых есть отличные от 0

Наибольшим общим делителем (НОД) этих многочленов называется любой многочлен $d(x) \in F[x]$, обладающий следующими свойствами:

1. $f_1(x), \dots, f_m(x)$ делятся на $d(x)$, т.е. $d(x)$ есть общий делитель $f_1(x), \dots, f_m(x)$.
2. Если $d_1(x)$ — любой другой общий делитель многочленов $f_1(x), \dots, f_m(x)$, то $d(x)$ делится на $d_1(x)$.

Аналогично определяется наименьшее общее кратное (НОК) ненулевых многочленов $f_1(x), \ldots, f_m(x)$: слово „делитель" заменяется на „кратное".

Равенство вида

$$d(x) = \text{НОД}\,(f_1(x), \ldots, f_m(x))$$

означает, что многочлен $d(x)$ является одним из НОД многочленов $f_1(x), \ldots, f_m(x)$.

Аналогично следует понимать равенство

$$m(x) = \text{НОК}\,(f_1(x), \ldots, f_m(x))$$

Замечание

1. Из определений формально не следует, что НОД и НОК данных многочленов существуют.

   На самом деле, как будет показано ниже, они существуют.

2. Если $d(x)$ некоторый НОД многочленов $f_1(x), \ldots, f_m(x)$, то любой другой НОД этих многочленов $\tilde{d}(x)$ связан с $d(x)$ соотношением:

$$\tilde{d}(x) = c \cdot d(x)$$

   где $c \in F$, $c \neq 0$.

   Аналогичное утверждение справедливо и в отношении НОК

   Говорят, что многочлены $f(x)$ и $g(x) \in F[x]$ ассоциированы, если $f(x) = c\, g(x)$, где $0 \neq c \in F$

Пусть сначала $m = 2$.

Теорема 6 (алгоритм Евклида отыскания НОД многочленов $f(x)$ и $g(x)$)

Пусть $f(x), g(x) \in F[x]$, $g(x) \neq 0$

Если $f(x)$ делится на $g(x)$, то $g(x) = \text{НОД}(f(x), g(x))$ иначе

$$f(x) = g(x)\,q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x)$$

$$g(x) = r_1(x)\,q_2(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x)$$

Теорема 8

Пусть $f(x), g(x) \in F[x]$

Тогда

$$\text{НОК}(f(x), g(x)) = \frac{f(x)g(x)}{d(x)}$$

где $d(x) = \text{НОД}(f(x), g(x))$.

Доказательство

Обозначим

$$m(x) = \frac{f(x)g(x)}{d(x)} \in F[x]$$

и докажем, что $m(x)$ и есть $\text{НОК}(f(x), g(x))$, т.е. $m(x)$ – общее кратное этих многочленов (что очевидно) и если $M(x)$ – другое общее кратное, то $M(x)$ делится на $m(x)$.

Имеем:

$$M(x) = f(x)q_1(x) = g(x)q_2(x)$$

для нек-рых $q_1, q_2 \in F[x]$.

Разделим на $d(x)$:

$$f_1(x)q_1(x) = g_1(x)q_2(x)$$

где $f_1(x) = \frac{f(x)}{d(x)}$

$g_1(x) = \frac{g(x)}{d(x)}$

при этом $f_1(x)$ и $g_1(x)$ взаимно простые

По свойству 1 взаимно простых многочленов имеем:

$$q_2(x) = f_1(x)q_3(x)$$

подставив, получим после сокращения на $f_1(x)$.

$$q_1(x) = g_1(x)q_3(x)$$

что и так ясно.

Подставив в выражение для $M(x)$, получим

$$M(x) = g(x)f_1(x)q_3(x) = g(x)\frac{f(x)}{d(x)}q_3(x) = \\ = m(x)q_3(x)$$

т. е. $M(x)$ делится на $m(x)$.

Замечание (о НОД и НОК произвольного набора мн-в)

Д/отыскания НОД и НОК нескольких (≥ 3) многочленов используют следующие рекуррентные правила:

$$\text{НОД}(f_1(x), .., f_{m-1}(x), f_m(x)) =$$
$$= \text{НОД}(f_m(x), \text{НОД}(f_1(x), \dots, f_{m-1}(x)))$$
$$\text{НОК}(f_1(x), \dots, f_{m-1}(x), f_m(x)) =$$
$$= \text{НОК}(\text{НОК}(f_1(x), \dots, f_{m-1}(x)), f_m(x))$$

Кроме того для $\text{НОД}(f_1(x), \dots, f_m(x)) = d(x)$ справедливо утверждение о линейном представлении:

Существуют такие $u_1(x), .., u_m(x)$, что
$$d(x) = f_1(x)u_1(x) + .. + f_m(x)u_m(x)$$

п 4 Теорема о факторизации

Опр. Многочлен $P(x) \in F[x]$, $\deg P(x) > 0$ наз неприводимым (точнее, неприводимым над полем F), если $P(x)$ нельзя представить в виде
$$P(x) = P_1(x)\,P_2(x)$$
где $\deg P_i(x) > 0$ $(i = 1, 2)$
$P_1(x), P_2(x) \in F[x]$.

Примеры

1. $P(x) = ax + b \in F[x]$ неприводим над любым полем F $(a \neq 0)$.
2. $P(x) = x^2 + 1$ неприводим над $\mathbb{Q}$ и $\mathbb{R}$; над $\mathbb{C}$ этот многочлен приводим:
$$x^2 + 1 = (x + i)(x - i)$$

Замечание

Понятие неприводимости многочлена не явл. абсолютным, т. е. если $P(x) \in F[x]$ неприводим и $F \subset \tilde{F}$, то $P(x)$ может оказаться приводимым над $\tilde{F}$