

Алгебра

6 септября 2022

Делимость в кольце многочленов

K – поле

$K[x]$ – кольцо многочленов

§1 Наибольший общий делитель

Определение. $f_1, \dots, f_m \in K[x]$

$d \in K[x]$ – НОД f_1, \dots, f_m , если выполняется 2 условия:

1. $d|f_1, \dots, d|f_m$
2. Если $\tilde{d}|f_1, \dots, \tilde{d}|f_m$, то $\tilde{d}|d$

Пример 1. $f_1 = \dots = f_m$

Тогда $d = 0$

Замечание (Обозначение).

$$\begin{aligned}d &= \text{НОД}(f_1, \dots, f_m) \\&= \gcd(f_1, \dots, f_m) \\&= (f_1, \dots, f_m)\end{aligned}$$

Замечание (Вопрос единственности).

Пусть d, \bar{d} – два НОД(f_1, \dots, f_m)

Тогда $\bar{d}|d$, но и $d|\bar{d}$

$$\Rightarrow \deg d = \deg \bar{d}$$

$$\Rightarrow d = c \cdot \bar{d}, \quad c \in K^*$$

Тогда будем говорить, что h и g ассоциированы, если $h = cg$, $c \in K^*$

Теорема. $f_1, \dots, f_m \in K[x]$

Тогда $\exists d = \text{НОД}(f_1, \dots, f_m)$ и более того $\exists h_1, \dots, h_m \in K[x]$:

$$d = h_1 f_1 + \dots + h_m f_m$$

Доказательство.

1. $f_1 = \dots = f_m = 0$

Очевидно $0 = 1 \cdot 0 + \dots + 1 \cdot 0$

2. Среди f_1, \dots, f_m есть хотя бы 1 ненулевой

Рассмотрим $I = \{h_1 f_1 + \dots + h_m f_m \mid h_i \in K[x]\}$

Очевидно, что $f_1, \dots, f_m \in I$

I содержит ненулевой многочлен наименьшей степени множества I

Пусть d – это ненулевой многочлен (из предположения)

Утверждается, что это и есть НОД(f_1, \dots, f_m)

$$f_i = q_i d + r_i, \deg r_i < \deg d$$

$$r_i = f_i - q_i d$$

$$d = h_1 f_1 + \dots + h_m f_m, \quad d \in I$$

$$r_i = -(h_1 q_i f_1) + \dots + (1 - h_i q_i) f_i + \dots + (-h_m q_m) f_m, \quad r_i \in I$$

Так как d – ненулевой многочлен наименьшей степени в I

$$\text{то } r_i = 0, \quad f_i = q_i d, \quad d | f_i$$

$$d = h_1 f_1 + \dots + h_m f_m \quad (\text{т. к. } d \in I)$$

$$\tilde{d} | f_1, \dots, \tilde{d} | f_m$$

$$f_i = \tilde{d}_i \tilde{q}_i$$

$$d = \tilde{d}(h_1 \tilde{q}_1 + \dots + h_m \tilde{q}_m)$$

$$\tilde{d} | d \Rightarrow d = \text{НОД}(f_1, \dots, f_m)$$

По выбору $d \in I \Rightarrow d$ допускает лин. представление

□

§2 Алгоритм Евклида

Лемма 12. $f, g, q \in K[x]$

$$\text{НОД}(f, g) = \text{НОД}(f - qg, g)$$

Доказательство. Пусть $d = \text{НОД}(f, g)$

$$\tilde{d} = \text{НОД}(f - qg, g)$$

$$d | f, d | g \Rightarrow d | (f - qg)$$

$$\Rightarrow d | \tilde{d} \quad (\text{т. к. } \tilde{d} = \text{НОД}(f - qg, g))$$

$$\tilde{d} | f - qg, \quad \tilde{d} | f$$

$$f = (f - qg) + qg$$

$$\tilde{d} | f$$

$$\tilde{d} - \text{общий делитель } f \text{ и } g$$

$$\Rightarrow \tilde{d} | d$$

$$\tilde{d} = cd, \quad c \in K^*$$

□

Рассмотрим алгоритм:

$$\begin{aligned}
 r_0 &= f, \quad r_1 = g \\
 \boxed{=} \quad r_0 &= q_1 r_1 + r_2, \quad \deg r_2 < \deg r_1 \\
 &\dots \\
 r_{i-1} &= q_i r_i + r_{i+1}, \quad \deg r_{i+1} < \deg r_i \\
 r_{n-2} &= q_{n-1} r_{n-1} + r_n, \quad \deg r_n < \deg r_{n-1} \\
 r_{n-1} &= q_n r_n \\
 r_n &- \text{последний ненулевой остаток}
 \end{aligned}$$

Из $\boxed{=}$: $r_{i+1} = r_{i-1} - q_i r_i$. По лемме: $\text{НОД}(r_{i-1}, r_i) = \text{НОД}(r_{i+1}, r_i) = \text{НОД}(r_i, r_{i+1})$

$$\begin{aligned}
 \text{НОД}(r_0, r_1) &= \\
 \text{НОД}(r_1, r_2) &= \\
 &\dots \\
 \text{НОД}(r_{n-1}, r_n) &= r_n
 \end{aligned}$$

§3 Взаимно простые

Определение. $f_1, \dots, f_m \in K[x]$ *взаимно простые*, если

$$\text{НОД}(f_1, \dots, f_m) = 1$$

(То есть общими делителями являются только ненулевые константы)

Замечание. Следует различать простоту и попарную простоту:

f_1, \dots, f_m – попарно просты, если $\forall i, j, i \neq j \quad f_j$ и f_i – взаимно простые

Теорема 1 (Критерий взаимной простоты).

$$\begin{aligned}
 f_1, \dots, f_m \in K[x] \text{ взаимно просты} &\Leftrightarrow \\
 \exists h_1, \dots, h_m \in K[x] & \\
 \text{т. ч. } h_1 f_1 + \dots + h_m f_m &= 1
 \end{aligned}$$

Доказательство.

\Rightarrow 1 – НОД. По т. §1 допускает линейное представление

$\Leftarrow 1 | f_1, \dots, 1 | f_m$

Пусть \tilde{d} – какой-то общий делитель

$$\tilde{d} | f_1, \dots, \tilde{d} | f_m$$

$$\Rightarrow \tilde{d} | 1$$

□

Теорема 2. $f, g_1, \dots, g_m \in K[x]$

f, g_i взаимно простые $\forall i = 1, \dots, m$

Тогда f взаимно прост с $g_1 \cdot \dots \cdot g_m$

Доказательство. f, g_1 взаимно просты, тогда

$$1 = fu_i + g_iv_i, \quad u_i, v_i \in K[x]$$

$$1 - fu_i = g_iv_i, \quad i = 1, \dots, m$$

$$\prod_{i=1}^m (1 - fu_i) = g_1 \cdot \dots \cdot g_m \cdot v_1 \cdot \dots \cdot v_m =$$

$$= 1 + f \cdot A$$

$$1 = f(-A) + g_1 \cdot \dots \cdot g_m \cdot v_1 \cdot \dots \cdot v_m$$

\Rightarrow по т. 1: f и $g_1 \cdot \dots \cdot g_m$ – взаимно просты

□

Теорема 3.

$$f, g, h \in K[x]$$

$f | gh$ и f и g взаимно просты

Тогда $f | h$

Доказательство. $\exists u, v \in K[x]$

$$f \cdot u + g \cdot v = 1$$

$$fhu + ghv = 1$$

...

$$f \quad f \Rightarrow f | h$$

□

§4 Неприводимые многочлены ОТА для $K[x]$

Определение. $f \in K[x] \setminus K$

f – составной, если

$$\exists h, g \notin K^*$$

$$f = hg$$

Если таких h и g не существует, то f называется неприводимым (над K)

f неприводим:

$$f = hg \Rightarrow h \in K^* \text{ или } g \in K^*$$

векторный сомножитель ассоциированы с f

f неприводим, если его делители – это в точности константы и ассоциированные с f (полный аналог простых)

Теорема 4 (ОТА).

$$0 \neq f \in K[x]$$

Тогда $\exists c \in K^*$ и неприводимые h_1, \dots, h_m со старшим коэффициентом 1 таким, что

$$f = c \cdot h_1 \cdot \dots \cdot h_m \quad (m \geq 0)$$

c совпадает со старшим коэффициентом f и тогда разложение единственно с точностью до порядка сомножителя

Доказательство.

1. Существование:

а) $f \in K^*$ – очевидно $c = f, m = 0$

б) $\deg f > 0$

Если f неприводим, то остановимся

Если f составной, то разложим $f = u \cdot v, \deg u < \deg v < \deg f$

Дальше так же поступим с каждым из сомножителей

Процесс оборвется за конечное число шагов

$$f = \tilde{h}_1 \cdot \dots \cdot \tilde{h}_m, \tilde{h}_i - \text{неприводимый}$$

$$\tilde{h}_i = c_i h_i, h_i - \text{неприводимый, старший коэффициент 1}$$

$$f = \underbrace{(c_1 \cdot \dots \cdot c_m)}_{=c} \cdot h_1 \cdot \dots \cdot h_m$$

2. Единственность:

$$f = ch_1 \cdot \dots \cdot h_m = e \cdot g_1 \cdot \dots \cdot g_n, \quad h_i, g_i - \text{неприв.}, \text{ ст. коэфф. } 1$$

$$\Rightarrow c = e, m = n \text{ и (после перенумерации) } g_i = h_i, c = 1, \dots, m$$

$$\text{НУО: } m \leq n$$

Индукция по m :

$$\text{База } m = 0 \quad f = c = eg_1 \dots g_m \quad \deg f = 0 \Rightarrow n = 0 \Rightarrow c = e$$

$$\text{Индукционный переход: } m \geq 1 \quad h_m | eg_1 \dots g_m \quad \boxed{*}$$

Неприводимые либо ассоциированы, либо взаимно простые.

Если h_m не ассоциирован ни с одним из g_1, \dots, g_m , то h_m взаимно прост с g_1, \dots, g_m , а значит h_m взаимно прост с $eg_1 \cdot \dots \cdot g_m$ (Т. 2)

\rightarrow но многочлен не может делить и быть взаимно простым \rightarrow что противоречит $\boxed{*}$

(т. к. из $\boxed{*}$ следует, что $K^* \nmid h_m = \text{НОД}(h_m, eg_1 \cdot \dots \cdot g_m)$)

$\Rightarrow \exists i : h_m$ ассоциируется с g_i . НУО $i = n$

т. к. h_m, g_n со старшем коэффициентом 1, из ассоциированности следует, что $h_m = g_n$

$$ch_1 \cdot \dots \cdot h_m = eg_1 \cdot \dots \cdot g_n$$

$$ch_1 \cdot \dots \cdot h_{m-1} = eg_1 \cdot \dots \cdot g_{n-1}$$

По индукционному предположению: $m - 1 = n - 1$, $c = e$ и после перенумерации:

$$g_1 = h_1, \dots, g_{m-1} = h_{m-1} \Rightarrow m = n \text{ и } g_m = h_m$$

□