многочлены 3.0 без п5-6

prerequisite knowledge: глава кольцо многочленов (a.k.a. многочлены база.pdf).

---

1. Наибольший общий делитель

Далее K - поле.

Есть какой-то набор многочленов: $f_1, \ldots, f_m \in K[x]$.
Многочлен $d \in K[x]$ - их **наибольший общий делитель**, если:

> 1. d делит все многочлены: $d | f_1, \ \ldots, \ d | f_m$
> 2. Любой другой общий делитель делит d.

ⓘ **Обозначение:**

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

> ***Пример***:
> $f_1 = \ldots = f_m = 0$
> Тогда $d = 0$

Пусть d, e - два наибольших делителя $f_1, \ldots, f_m$.
$d | e$, и наоборот, $e | d \implies \deg e = \deg g$.

$d = c \cdot e,\ c \in K^*$ - поле обратимых элементов K.

Два многочлена h, g **ассоциированы**, если $h = c \cdot g,\ c \in K^*$.

> *Упражнение: докажите, что ассоциированность - отношение эквивалентности.*

В классе ассоциированных многочленов есть ровно один со старшим коэффициентом единицей.

Теорема. $f_1, \ldots, f_m \in K[x]$.
Тогда существует их наибольший делитель, и более того, существуют $h_1, \ldots, h_m \in K[x]$ такие, что

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

Это **линейное представление НОД**.

Доказательство:

1. Тривиальный случай: $f_1 = \ldots = f_m = 0$.
   $h_i = 1\ \forall i \in \{1, \ldots, m\}$

2. Среди $f_1, \ldots, f_m$ есть ненулевой. Рассмотрим вспомогательное множество
   $I = \{h_1 f_1 + \ldots + h_m f_m \mid h_i \in K[x]\}$.
   $f_1, \ldots, f_m \in I$.
   I содержит ненулевой многочлен. Выберем из ненулевых многочлен наименьший степени - d.
   Проверим, что он НОД$(f_1, \ldots, f_m)$.
   Каждый $f_i = q_i \cdot d + r_i,\ \deg r_i < \deg d$. (т. о делении)

Проверим, что остаток нулевой:

$r_i = f_i - q_i \cdot d \qquad d = h_1 f_1 + \dots h_m f_m$. Подставляем:

$r_i = (-h_1 q_i) \cdot f_1 + \dots + (1 - h_i q_i) f_i + \dots + (-h_m q_i) f_m$.

Получили, что $r_i \in I$. А так как d ненулевой многочлен наименьшей степени в I и $\deg r_i < \deg g$, то $r_i = 0$.

$f_i = q_i \cdot d, \quad d | f_i$.

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

Теперь проверим наибольшесть делителя:

Пусть есть $e : e | f_1, \dots, e | f_m$.

$f_i = e \cdot \tilde{q}_i$.

Так как d допускает линейное представление:

$d = h_1 f_1 + \dots + h_m f_m = e(h_1 \tilde{q}_1 + \dots + h_m \tilde{q}_m) \implies e | d$

$\implies d = \gcd(f_1, \dots, f_m)$

По выбору $d \in I$, d допускает линейное представление.

2. Алгоритм Евклида

Докажем лемму:

Лемма. $f, g, q \in K[x]$.

$\gcd(f, g) = \gcd(f - qg, g)$ (как ассоциированные)

Доказательство:

$d = \gcd(f, g),\ e = \gcd(f - qg, g)$.

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

d - общий делитель $\{f - qg, g\} \implies \underline{d | e}$.

$e|(f-qg), e|g.$

$f = \underbrace{(f-qg)}_{e|} + \underbrace{qg}_{e|} \implies e|f$

$e|f,\ e|g \implies \underline{e|d}.$

$e|d,\ d|e \implies d = c\cdot e,\ c\in K^*.$

Таким образом, d и e ассоциированы.

Алгоритм Евклида (линейное представление НОД):

$r_0 = f,\ r_1 = g$

Процесс:

$r_0 = q_1 r_1 + r_2, \qquad \deg r_2 < \deg r_1$

$\dots\ \ \dots\ \ \dots$

$r_{i-1} = q_i r_i + r_{i+1}, \qquad \deg r_{i+1} < \deg r_i$

$\dots\ \ \dots\ \ \dots$

$r_{n-3} = q_{n-2} r_{n-2} + r_{n-1} \qquad \deg r_{n-1} < \deg r_{n-2}$

$r_{n-2} = q_{n-1} r_{n-1} + r_n, \qquad \deg r_n < \deg r_{n-1}$

$r_{n-1} = q_n r_n$

r_n - последний ненулевой остаток.

Процесс обрывается, так как степени ненулевых остатков строго убывают: $r_{i+1} = r_{i-1} - q_i r_i,\ \ \deg r_{i+1} < \deg r_i$.

По лемме $\gcd(r_{i-1}, r_i) = \underline{\gcd(r_{i+1}, r_i) = \gcd(r_i, r_{i-1})} \implies$

$$\gcd(f,g) = \gcd(r_o, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_{n-1}, r_n) = r_n$$

Линейное представление $r_n = \gcd(f,g)$ - читаем процесс снизу вверх и выражаем остатки:

$$r_n = r_{n-2} - q_{n-1} r_{n-1} = r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2}) = \dots$$

> *Упражнение: докажите, что*
> $\gcd(f_1, \ldots, f_m) = \gcd(\gcd(f_1, \ldots, f_{m-1}), f_m)$

3. Взаимно простые многочлены

$f_1, \ldots, f_m \in K[x]$ **взаимно простые**, если их НОД = 1 (конст.)

Следует различать простоту **взаимную** и **попарно взаимную**.

> $x(x-1),\ x(x+1),\ (x+1)(x-1)$ взаимно просты в $\mathbb{Q}$, но не попарно.

Теорема 1. Многочлены $f_1, \ldots, f_m$ взаимно просты, тогда и только тогда, когда существует линейное представление единицы: $h_1 f_1 + \ldots + h_m f_m = 1$.

Доказательство:

$\boxed{\Rightarrow}$ $1 = \gcd$. По теореме из параграфа 1, 1 допускает линейное представление.
$\boxed{\Leftarrow}$ 1 - общий делитель $f_1, \ldots, f_m$. Пусть d - тоже их общий делитель. Тогда d делит и правую часть равенства $h_1 f_1 + \ldots h_m f_m = 1$, то есть $d | 1$.
Отсюда $1 = \gcd(f_1, \ldots, f_m)$

Теорема 2. $f, g_1, \ldots, g_m \in K[x]$.
f, g_i взаимно просты для всех $i = 1, \ldots, m$. Тогда f взаимно

прост с $g_1 \cdot \ldots \cdot g_m$.

Доказательство:

f, g_i взаимно просты, значит $1 = f \cdot u_i + g_i v_i,\ u_i, v_i \in K[x]$.
$1 - fu_i = g_i v_i \quad i = 1, \ldots, m$.
Почленно перемножим:
$\prod_{i=1}^{m}(1 - fu_i) = g_1 \ldots g_m v_1 \ldots v_m$.
Обозначим левую часть за $1 + fA$, где $A \in K[x]$.
$1 = -fA + g_1 \ldots g_m v_1 \ldots v_m$.
$1 = -A\underline{f} + \underline{g_1 \ldots g_m} v_1 \ldots v_m$. По первой теореме f и $g_1 \ldots g_m$ взаимно просты.

Теорема 3. (о сокращении) $f, g, h \in K[x]$.
$f|gh$, f и g взаимно просты.
Тогда $f|h$.

Доказательство:

$u, v \in K[x]$.
$fu + gv = 1 \qquad | \cdot h$
$\underline{f}hu + \underline{gh}v = h \implies f|h \qquad$ (f делит f и gh)

4. Неприводимые многочлены. ОТА в кольце многочленов

$f \in K[x] \setminus K$.
Многочлен f **составной**, если $\exists h, g \notin K^* : f = hg$ (строго меньшие степени).
Если таких h и g не существует, то f **неприводимый**.

f неприводимый $\implies f = hg \implies h \in K^*$ или $g \in K^*$. Это значит, что второй сомножитель ассоциирован с f (h или g).

> f неприводим, если его делители - в точности константы и ассоциированные многочлены.

Теорема. (основная теорема арифметики для $K[x]$)
$0 \neq f \in K[x]$. Тогда $\exists c \in K^*$ и неприводимые $h_1, \ldots, h_m$ со старшими коэффициентами 1 такие, что

$$f = c \cdot h_1 \ldots h_m$$

и такое разложение единственно с точностью до порядка сомножителей.

Доказательство:

Доказывать будем в несколько этапов. Сначала покажем существование, а затем единственность.
Существование:
Если $f \in K^*$, то теорема очевидна: $c = f, m = 0$.
Если $\deg f > 0$:
f неприводим $\implies$ остановимся.
f составной $\implies$ разложим его на множители:
$f = u \cdot v, \qquad \deg u, \deg v < \deg f$.
Так же поступаем с каждым сомножителем (раскладываем на множители):

$f \to v \cdot u \to kd \cdot yt \to \dots$

Этот процесс конечен. В конце получим:

$f = j_1 \cdot \ldots j_m, \quad j_i$ неприводимы.

$j_i = c_i \cdot h_i, \quad h_i$ неприводимы, со старшим коэфф. 1.

$f = \underbrace{c_1 \ldots c_m}_{c} \cdot h_1 \ldots h_m.$

Единственность:

$f = c \cdot h_1 \ldots h_m = e \cdot g_1 \ldots g_n, \quad h_i, g_i$ неприводимы, со старшим коэфф. 1.

Хотим доказать, что $c = e,\ m = n$, и $h_i = g_i$ после перенумерации.

Не умаляя общности, $m \leq n$. Будем доказывать индукцией по m - числу неприводимых многочленов в разложении.

База: $m = 0$. $f = c = eg_1 \ldots g_n$.

$\deg f = 0 \implies n = 0 = m \implies c = e$.

Индукционный переход: $m \geq 1,\ h_m | eg_1 \ldots g_m$.

Два неприводимых многочлена либо ассоциированы, либо взаимно просты. Если h_m не ассоциирован ни с одним из $g_1, \ldots, g_n$, то он взаимно прост с каждым из $g_1 \ldots, g_m$, и как следствие, взаимно прост с их произведением (по теореме 2 из прошлого параграфа). Но это противоречие с $h_m | eg_1 \ldots g_m$ (из этого следует, что $\underset{\notin K^*}{h_m} = \gcd(h_m, eg_1 \ldots g_m)$), поэтому h_m не взаимно прост со всеми g_i.

Отсюда $\exists i : h_m$ ассоциирован с g_i.

Не умаляя общности, положим $i = n$. Так как h_m, g_n со старшими коэффициентами 1, то $h_m = g_n$.

$ch_1 \ldots h_m = eg_1 \ldots g_{n-1} h_m$.

$ch_1 \ldots h_{m-1} = eg_1 \ldots g_{n-1}$.

По индукционному предположению $m - 1 = n - 1$.

Отсюда $c = e$ и после перенумерации

$g_1 = h_1, \ \ldots, \ g_{m-1} = h_{m-1} \implies m = n$ и $g_n = h_m$.

5-6 нет в билетах :)