Дефиниция (неразложим полином над поле)

Нека F е поле и $f \in F[x]$.
f наричаме **неразложим над** F, ако:

- $\deg f \geq 1$
- $f = g.h \Longrightarrow$ или $\deg g = 0$ или $\deg h = 0$.

Примери

1. Всички полиноми от първа степен са неразложими.

2. $x^2 - 2 \in \mathbb{Q}[x]$ е неразложим над $\mathbb{Q}$, но е разложим над $\mathbb{R}$ и $\mathbb{C}$.

Следствие

Ако f е неразложим, то $f|gt \iff f|g$ или $f|t$.

Доказателство:
$| \Longleftarrow |$ е ясно.
$| \Longrightarrow |$ Ако $f|gt$, то $f = gth$, за някой полином h, което ще запишем като $f = g(th)$.
Съгласно дефиницията на неразложим полином, какъвто е f, $\deg th = 0$ или $\deg g = 0$:

Случай 1 - $\deg th = 0$:
Тогава $\deg g = \deg f$ и следователно $f = cg$ за някоя константа c, откъдето f/g.

Случай 2 - $\deg g = 0$:
Тогава $\deg th = \deg f$ и следователно $f = cth$ за някоя константа c, което означава, че th е неразложим[1].
Сега отново по дефиницията следва $\deg t = 0$ или $\deg h = 0$:

Случай 2.1. $\deg t = 0$, но тогава $\deg gt = \deg g + \deg t = 0$ и не е интересно, защото излиза, че $f/const$ и оттам $f = const \Longrightarrow f/g$, защото разглеждания Случай 2 - $\deg g = 0$ не означава нищо друго, освен $g = const$.

Случай 2.2. $\deg h = 0$, откъдето $h = const$ и следователно $f = t.const \Longrightarrow f/t$

Теорема (за разлагане на полином на неразложими множители)

Нека F е поле и $f(x) \in F[x]$, $\deg f \geq 1$
Тогава f може да се представи като произведение на неразложими полиноми с точност до наредбата на множителите и константа (обратим елемент от F)

Казано иначе:
$f(x) = t_1(x)t_2(x)\dots t_s(x)$, $\forall i = 1, 2, \dots, s:\ t_i(x)$ - неразложими полиноми, и ако $f(x) = p_1(x)p_2(x)\dots p_k(x)$, $\forall i = 1, 2, \dots, k:\ p_i(x)$ - неразложими, то $\Longrightarrow s = k$, $t_i = p_i d_i$, $d_i \in F$ (след пренареждане) и, освен това, $d_1 d_2 \dots d_s = 1$

Доказателство:

Съществуване:
Провеждаме индукция по $n = \deg f$

1. База: нека $n = 1 \Longrightarrow f$ е неразложим.

2. Индукционна хипотеза: нека твърдението е вярно за $\forall f:\ \deg f < n$

3. Нека $\deg f = n$
3.1. Ако f е неразложим $\Longrightarrow f = f$ е търсеното представяне.
3.2. Ако f е разложим: $f = gh$ като $\deg g < n$ и $\deg h < n$
$\Longrightarrow h$ и g се разлагат на неразложими множители (от индукционната хипотеза)

$h = h_1(x)h_2(x)\dots h_k(x), h_i$ - неразложими
$g = g_1(x)g_2(x)\dots g_s(x), g_i$ - неразложими

Тогава $f = h_1(x)h_2(x)\dots h_k(x)g_1(x)g_2(x)\dots g_s(x)$ е търсеното представяне.

Единственост:
Нека $f = p_1(x)p_2(x)\dots p_s(x)$ и $f = q_1(x)q_2(x)\dots q_r(x)$

$\Longrightarrow p_1(x)p_2(x)\dots p_s(x) = q_1(x)q_2(x)\dots q_r(x)$
$\Longrightarrow p_1 | q_1 q_2 \dots q_r \Longrightarrow \exists i \in \{1, 2, \dots, r\} : \ p_1 | q_i$

Безограничение на общността можем да считаме, че $p_1 | q_1$
Освен това, p_1 и q_1 са неразложими полиноми, т.е. $p_1 = d_1 q_1, \ d_1 \in F[x]$ - константа
(Тъй като d_1 е константен полином, можем да си мислим, че $d_1 \in F$).

$$p_1 p_2 \dots p_s | q_1 q_2 \dots q_r \Longrightarrow p_1 p_2 \dots p_s | d_1 p_1 q_2 \dots q_r \iff p_2 p_3 \dots p_s | d_1 q_2 \dots q_3$$

Аналогична е процедурата и за p_2.

Така след краен брой стъпки ще получим, че $s = r$. Освен това:
$p_1 = d_1 q_1, \ p_2 = d_2 q_2, \dots, p_s = d_s q_s$

$f = p_1 p_2 \dots p_s = d_1 q_1 d_2 q_2 \dots d_s q_s = d_1 d_2 \dots d_s q_1 q_2 \dots q_s = q_1 q_2 \dots q_s$
$\Longrightarrow d_1 d_2 \dots d_s = 1.$ □

Дефиниция (примарен полином)

Полином с цели коефициенти, такива че техният НОД е 1, наричаме **примарен полином**.

Твърдение

Нека $f(x) \in \mathbb{Q}[x] \Longrightarrow \exists \ g(x) \in \mathbb{Z}[x]$ - примарен,
такъв че $f(x) = \alpha g(x), \ \alpha \in \mathbb{Q}$

Доказателство:

$$f(x) \in \mathbb{Q}[x] \Longrightarrow f(x) = \frac{p_0}{q_0} x^n + \frac{p_1}{q_1} x^{n-1} + \dots + \frac{p_n}{q_n} \tag{1}$$

Нека $B =$ НОК $(q_0, q_1, \dots, q_n)$
Тогава:

$$
\begin{aligned}
f(x) &= \frac{B}{B}\left(\frac{p_0}{q_0}\,x^n + \frac{p_1}{q_1}\,x^{n-1} + \cdots + \frac{p_n}{q_n}\right) \\
&= \frac{1}{B}\left(\underbrace{\frac{Bp_0}{q_0}}_{c_0}x^n + \underbrace{\frac{Bp_1}{q_1}}_{c_1}x^{n-1} + \cdots + \underbrace{\frac{Bp_n}{q_n}}_{c_n}\right) \\
&= \frac{1}{B}\left(c_0x^n + c_1x^{n-1} + \cdots + c_n\right),\ c_i \in \mathbb{Z}\ \forall i = 0, 1, \ldots, n
\end{aligned}
\tag{2}
$$

Сега, нека $d = \text{НОД}(c_0, c_1, \ldots, c_n)$
$\Longrightarrow c_i = dt_i,\ \forall i = 0, 1, \ldots, n$ и $\text{НОД}(t_0, t_1, \ldots, t_n) = 1$

$$
\Longrightarrow f(x) = \underbrace{\frac{d}{B}}_{\alpha \in \mathbb{Q}}\left(\underbrace{t_0x^n + t_1x^{n-1} + \cdots + t_n}_{g(x)}\right),\ t_i = \frac{c_i}{d} \in \mathbb{Z}
\tag{3}
$$

Очевидно полиномът $g(x)$ е примарен (по "построение")

$\Longrightarrow f(x) = \alpha g(x)$ като $\alpha \in \mathbb{Q}$ и $g(x)$ е примарен. $\square$

Лема на Гаус

Произведение на два примарни полинома с цели коефициенти е също примарен полином.

Доказателство:
Нека $f(x) = b_0x^k + b_1x^{k-1} + \cdots + b_k$ и $g(x) = c_0x^s + c_1x^{s-1} + \cdots + c_s$ са два примарни полинома и $\deg f = k,\ \deg g = s$

Нека $h = fg \Longrightarrow \deg h = k + s$
$\Longrightarrow h = a_0x^{k+s} + a_1x^{k+s-1} + \cdots + a_{k+s}$

Допускаме, че h не е примарен.
$\Longrightarrow \exists\, p \in \mathbb{Z}$ - просто, такова, че $p | a_i,\ \forall i = 1, 2, \ldots, k + s$

Сега разглеждаме следното изображение:

$$
\varphi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]
\tag{4}
$$

$$
\varphi_p(h) = \overline{a_0}x^{k+s} + \overline{a_1}x^{k+s-1} + \cdots + \overline{a_{k+s}} = \bar{h}
\tag{5}
$$

Следните свойства са логични:

$$\varphi_p(u+v) = \varphi_p(u) + \varphi_p(v) \tag{6}$$

$$\varphi_p(uv) = \varphi_p(u)\varphi_p(v) \tag{7}$$

$\Longrightarrow \varphi_p$ е хомоморфизъм и $\varphi_p(h) = \bar{h}$

Тъй като p дели всички коефициенти на $h \Longrightarrow \bar{h} = \bar{0}$ (
$a_i \equiv 0 \pmod{p},\ \forall i = 1, 2, \ldots, k+s$)

$$\bar{0} = \bar{h} = \varphi_p(h) = \varphi_p(fg) = \bar{f}\bar{g} \Longrightarrow \bar{0} = \bar{f}\bar{g} \tag{8}$$

Освен това, в $\mathbb{Z}_p[x]$ няма делители на нулата
$\Longrightarrow \bar{f} = \bar{0}$ или $\bar{g} = \bar{0}$, т.е. f не е примарен или g не е примарен. Прочиворечие.

$\Longrightarrow h$ е примарен. $\square$

Твърдение

Нека $f(x) \in \mathbb{Z}[x]$ е примарен полином и $c \in \mathbb{Q}$.
Ако $cf(x) \in \mathbb{Z}[x]$, то $c \in \mathbb{Z}$.

Доказателство:
Нека $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$

$c \in \mathbb{Q} \Longrightarrow c = \frac{p}{q}\ ,\ p, q \in \mathbb{Z}$

$cf(x) \in \mathbb{Z}[x] \Longrightarrow q | a_i,\ \forall i = 0, 1, \ldots, n$

$\Longrightarrow q|$ НОД$(a_0, a_1, \ldots, a_n) \Longrightarrow q|1 \Longrightarrow q = \pm 1$

$\Longrightarrow c \in \mathbb{Z}$. $\square$

Теорема

Нека $f(x) \in \mathbb{Z}[x]$

1. $f(x)$ е разложим над $\mathbb{Q} \iff f(x)$ е разложим над $\mathbb{Z}$
2. $f(x)$ **не** е разложим над $\mathbb{Q} \iff f(x)$ **не** е разложим над $\mathbb{Z}$

Доказателство:
1.
$| \Longrightarrow |$
$f(x)$ е разложим над $\mathbb{Q} \Longrightarrow f(x) = g(x)h(x),\ g(x), h(x) \in \mathbb{Q}[x]$

$g(x) \in \mathbb{Q} \Longrightarrow \exists g_1(x) \in \mathbb{Z}[x]$ - примарен и $\alpha \in \mathbb{Q} :\ g(x) = \alpha g_1(x)$
Аналогично $h(x) = \beta h_1(x),\ h_1(x)$ - примарен и $\beta \in \mathbb{Q}$

$\Longrightarrow f(x) = g(x)h(x) = \alpha g_1(x) \beta h_1(x)$

$\Longrightarrow f(x) = \alpha\beta g_1(x) h_1(x)$
Тъй като $g_1(x)h_1(x)$ е примарен полином и $f(x) \in \mathbb{Z} \Longrightarrow \alpha\beta \in \mathbb{Z}$ (от предишното твърдение)

$$\Longrightarrow f(x) = \underbrace{\alpha\beta}_{\in \mathbb{Z}} \underbrace{g_1(x)}_{\in \mathbb{Z}} \underbrace{h_1(x)}_{\in \mathbb{Z}}$$
$\Longrightarrow f(x)$ е разложим над $\mathbb{Z}$.

$| \Longleftarrow |$
В тази посока е очевидно, защото $\mathbb{Z} \subset \mathbb{Q}$.

2.
Правим отрицанието на 1. и всичко е доказано. $\square$

Критерий на Айзенщайн

Нека $f(x) \in \mathbb{Z}[x]$
$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$

Ако съществува просто число p, такова, че:

1. $p \nmid a_0$
2. $p|a_1, p|a_2, \ldots, p|a_n$
3. $p^2 \nmid a_n$

$\Longrightarrow f(x)$ е неразложим над $\mathbb{Q}$ (и съответно над $\mathbb{Z}$)

Доказателство:
Допускаме, че $f(x)$ се разлага над $\mathbb{Q}$, т.е $f(x)$ се разлага и над $\mathbb{Z}$

Т.е $f(x) = g(x)h(x),\ g(x), h(x) \in \mathbb{Z}[x],\ \deg g = k \geq 1,\ \deg h = s \geq 1$

Нека $g(x) = b_0 x^k + b_1 x^{k-1} + \cdots + b_k$ и $h(x) = c_0 x^s + c_1 x^{s-1} + \cdots + c_s$

Тук малко плагиатстваме от Гаус вече познатото изображение:
$\varphi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$
$\varphi_p(f) = \overline{a_0} x^n + \overline{a_1} x^{n-1} + \cdots + \overline{a_n} = \bar{f}$

Гаус вече е доказал, че φ_p е хомоморфизъм.

$f = gh \Longrightarrow \varphi_p(f) = \varphi_p(gh) \Longrightarrow \bar{f} = \bar{g}\bar{h}$

От 2. следва, че
$$p|a_i,\ \forall i = 1, 2, \ldots, n \Longrightarrow \bar{f} = \overline{a_0} x^n + \underbrace{\overline{a_1}}_{\bar{0}} x^{n-1} + \cdots + \underbrace{\overline{a_n}}_{\bar{0}} = \overline{a_0} x^n$$

$\Longrightarrow \overline{a_0} x^n = \bar{g}\bar{h}$

$\bar{g}|x^n \Longrightarrow \bar{g} = \overline{b_0}x^k \Longrightarrow p|b_i,\ \forall i = 1, 2, \ldots, k$
$\bar{h}|x^n \Longrightarrow \bar{h} = \overline{c_0}x^s \Longrightarrow p|c_i,\ \forall i = 1, 2, \ldots, s$

Знаем, че $a_n = b_k c_s$

Но $p|b_k$ и $p|c_s$, т.е. $p^2|b_k c_s \Longrightarrow p^2|a_n$, което е противоречие с 3.

$\Longrightarrow f(x)$ е неразложим над $\mathbb{Q}$. $\square$

Footnotes

1. И че Дядо Коледа наистина съществува.

page revision: 20, last edited: 29 Jun 2012, 15:43 (372 days ago)