Схема на Хорнер

$\Leftrightarrow f(\alpha)=0$

Зад. $f(x) = (x-\alpha)q + f(\alpha)$; α - кор. $\Leftrightarrow f = (x-\alpha)q$

Тв. $f = a_0 + a_1 x + \dots + a_n x^n \in F[x]$, $\alpha \in F$

$\Rightarrow \exists\, q = b_0 + b_1 x + \dots + b_{n-1} x^{n-1} \in F[x]$ и $r \in F$:

$f = (x-\alpha)q + r$, където

$b_0 = a_1 + b_1 \alpha$

$b_1 = a_2 + b_2 \alpha$; $r = a_0 + b_0 \alpha$

$\dots$

$b_{n-2} = a_{n-1} + \alpha b_{n-1}$

$b_{n-1} = a_n$

Д-во $(x-\alpha)q + r = (x-\alpha)(b_0 + b_1 x + \dots + b_{n-1}x^{n-1}) + r =$

$$= b_{n-1}x^n + (b_{n-2} - \alpha b_{n-1})x^{n-1} + \dots + (b_0 - b_1\alpha)x + (r - b_0\alpha)$$

$$= f = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$$

$$\Uparrow \left| \begin{aligned} b_{n-1} &= a_n \\ b_{n-2} - \alpha b_{n-1} &= a_{n-1} \\ &\dots \\ b_0 - b_1\alpha &= a_1 \\ r - b_0\alpha &= a_0 \end{aligned} \right. \iff \left| \begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= a_{n-1} + \alpha b_{n-1} \\ &\dots \\ b_0 &= a_1 + b_1\alpha \\ r &= a_0 + b_0\alpha \end{aligned} \right.$$

Забл. Обикновено F е поле, но работи и за произволен пръстен

Зад.

	a_n	a_{n-1}	...	a_1	a_0
α	b_{n-1}	b_{n-2}	...	b_0	r
	$\parallel$	$\parallel$		$\parallel$	$\parallel$
	a_n	$a_{n-1}+\alpha b_{n-1}$		$a_1+\alpha b_1$	$a_0+\alpha b_0$

Аритметика в пръстен от полиноми на 1 променлива с коеф. от поле

Зад. F - поле

Теорема за дел. с частно и остатък

$$\forall f, g \in F[x],\ g \neq 0 \Rightarrow \exists!\, q, r \in F[x]: \begin{cases} f = gq + r \\ \deg r < \deg g \end{cases}$$

__Д-во__ ($\exists$) / $\deg f = n$, $\deg g = m$

Инд. по $\underline{n}$ $\left(\in \{-\infty, 0, 1, 2, \dots\}\right)$

$n = -\infty \to f = 0 \to f = g \cdot 0 + \underset{r}{\underset{\shortparallel}{f}}$, $\deg r = \deg f = 0 < \deg g$

Нека е вярно за $\deg f < n$ $> -\infty$, ≥ 0. Виж горе. За $\deg f = n$

$f = a_n x^n + \dots + a_0$; $g = b_m x^m + \dots + b_0$

$a_n \neq 0$ $\qquad b_m \neq 0$

- $n < m$ $\qquad f = g \cdot 0 + \underset{r}{\underset{\shortparallel}{f}}$
- $n \geq m$ $\qquad f_1 = f - \dfrac{a_n}{b_m} x^{\overbrace{n-m}^{\geq 0}} \cdot g$; $\deg f_1 < \deg f = n$

$$- \; f_1 = 0 \;\to\; f = \underbrace{\frac{a_n}{b_m}x^{n-m}}_{q}\cdot g + \underbrace{0}_{r}$$

$$- \; f_1 \neq 0 \;\xrightarrow[\text{quin.}]{\text{ucg}}\; \exists\, q_1, r_1 : \left| \begin{array}{l} f_1 = g q_1 + r_1 \\ \deg r_1 < \deg g \end{array} \right.$$

$$\Rightarrow f = \underbrace{g q_1 + r_1}_{f_1} + \frac{a_n}{b_m}x^{n-m}\cdot g =$$

$$= \underbrace{\left(q_1 + \frac{a_n}{b_m}x^{n-m}\right)}_{q} g + \underbrace{r_1}_{r}$$

Зад. Алгоритъм за деление

$$f = 3x^4 + 2x^2 + x - 5 \qquad g = 2x^2 + x + 1$$

$$q = \frac{3}{2}x^2 - \frac{3}{4}x + \frac{5}{8}$$

$$\frac{3x^4}{2x^2} \qquad \frac{-\frac{3}{2}x^3}{2x^2} \qquad \frac{\frac{5}{4}x^2}{2x^2}$$

$\left(\frac{3}{2}x^2 \cdot g\right)$ $$-\;\; 3x^4 + \frac{3}{2}x^3 + \frac{3}{2}x^2$$

$$-\frac{3}{2}x^3 + \frac{1}{2}x^2 + x - 5$$

$\left(-\frac{3}{4}x \cdot g\right)$ $$-\;\; -\frac{3}{2}x^3 - \frac{3}{4}x^2 - \frac{3}{4}x$$

$$\frac{5}{4}x^2 + \frac{7}{4}x - 5$$

$\left(\frac{5}{8}g\right)$ $$\frac{5}{4}x^2 + \frac{5}{8}x + \frac{5}{8}$$

$$\frac{9}{8}x - \frac{45}{8} = r$$

$$f = g \cdot q + r$$

Доб. Неконструктивно

$$M = \{ f - qg \mid q \in F[x] \}$$

$r \in M$ – с най-ниска степен

$\Rightarrow r = f - qg$, т.е. $f = qg + r$

Ако $\deg r \geq \deg g$

$$r = a_0 x^n + \dots \; ; \; g = b_0 x^m + \dots$$

$$r_1 = r - \frac{a_0}{b_0} x^{n-m} g : \left| \begin{array}{l} \deg r_1 < \deg r \\ r_1 \in M \end{array} \right. \qquad \perp$$

Единственост: нека $f = g q_1 + r_1 = g q_2 + r_2$ и $\deg r_1, \deg r_2 < \deg g$

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

$$\deg g + \deg(q_1 - q_2) = \deg(r_2 - r_1) < \deg g$$

$$\deg(q_1 - q_2) < 0 \Rightarrow q_1 - q_2 = -\infty \Rightarrow q_1 - q_2 = 0$$

$$\Rightarrow q_1 = q_2 \Rightarrow r_1 = r_2$$

Зад. 1) сконструирайте полином за произволни функции с f и ст. коеф. на g е обратим ел.

2) в общия на целите полиноми единственост

Тв В $F[x]$ всеки идеал е главен

Д-во $I \triangleleft F[x]$; $I=\{0\} \Rightarrow I=(0)$

$I \neq \{0\}$; вземаме $f \in I$ с минимална степен

Ясно е, че $(f) \subseteq I$

$$g \in I \setminus (f) \Rightarrow \exists q, r : \left| \begin{array}{l} g = fq + r \rightarrow r = g - fq \in I \\ \deg r < \deg f \end{array} \right.$$

$$\Rightarrow I \setminus (f) = \emptyset \Rightarrow I = (f)$$

Заб. $(2, x) \triangleleft \mathbb{Z}[x]$ не е главен

Опр. 1) $d = (f, g)$: $(f) + (g) = (d)$ (НОД)

2) $m = [f, g]$: $(f) \cap (g) = (m)$ (НОК)

Опр. $f \mid g \overset{def}{\Longleftrightarrow} \exists h : g = fh$ $\qquad (\in F[x])$

Св-ва

1) $f \mid g \Longleftrightarrow (f) \supseteq (g)$

2) $f \mid g$ и $g \mid f \Longleftrightarrow \exists c \in F^* : f = cg$

$f = 0$ или $g = 0 \Rightarrow f = g = 0$

пусть $f \neq 0$, $g \neq 0$

$(\Rightarrow)$ $g = fh_1$, $f = gh_2 \rightarrow g = h_1 h_2 g \Rightarrow \deg h_1 h_2 = 0$

$\xRightarrow[h_2 \neq 0]{h_1 \neq 0} \deg h_1 = \deg h_2 = 0 \Rightarrow h_1, h_2 \in F \setminus \{0\} = F^*$

$(\Leftarrow)$ $f = cg \Rightarrow g \mid f$

$\Rightarrow g = c^{-1} f \Rightarrow f \mid g$

3) $(f) = (g) \iff \exists c \in F^*: f = cg$

4) $f / g \Rightarrow f / gh$

5) $f / g_1, g_2 \rightarrow f / g_1 \pm g_2$

6) f / f ;

7) f / g и $g / h \Rightarrow f / h$

Тв (опр.) 1) $d = (f, g) \iff$

1) d / f и d / g

2) Ако d' / f и $d' / g \Rightarrow d' / d$

2) $m = [f, g] \iff$

1) f / m и g / m ; 2) f / m' и $g / m' \Rightarrow m / m'$

Тв $\forall f, g \ \exists u, v : uf + vg = \underline{(f, g)}_{\text{НОД}}$ Безу

Заб. (f, g) не е определен еднозначно — с точност до обратим ел. на F

Д-во $(f, g)_{\text{НОД}} \in (f) + (g)$

Заб. $d / f \Rightarrow f = d \cdot \frac{f}{d}$ — „съкратено", ако $\deg d \neq 0, \deg f$

Заб. 1/ $(f, g)[f, g] = cfg$, $c \in F^*$

2/ $(fg, fh) = f(g, h)$

3/ Алгоритъм на Евклид — аналогично на числа

— $f / g \Rightarrow (f, g) = f$;

— Ако $\underline{f} = \underline{\bar{g}}\, q + \bar{r}$, то

за g-то във АЕ: $(f, g)\ \exists \iff \exists\ (g, r)$ и освен $\exists$ са равни

— Безу

Опр. $f \overset{\neq 0}{}$ е неразл., ако от $f = gh$ следва, че $\deg g = 0$ или $\deg h = 0$

Забел. $\iff \deg g = 0$ или $\deg g = \deg f$ и т.н.

Тв. $f \neq 0$ е неразл. $\iff$ от $d \mid f$ следва, че $\deg d = 0$ или $\deg d = \deg f$

Сл. f е неразл. $\Rightarrow$ $(f, g) = 1$ или f (с точност до F^*) ако $f \mid g$

Тв. $f \mid gh$, $(f, g) = 1 \Rightarrow f \mid h$

Д-во $\exists u, v: uf + vg = 1 \Rightarrow ufh + vgh = h \Rightarrow f | h$

Сл. f - неразл. и $f | gh \Rightarrow f | g$ или $f | h$

Т. $\forall f \neq 0 \; \exists p_1, \dots, p_n : f = p_1 \dots p_n$ и p_i - неразл.

Представление единственно с точностью до перест. на множители и умножение с эл-ма F^* по пол.

Зам. Единственность. $p_1 \dots p_n = q_1 \dots q_m$ p_i, q_i - неразл.

$\Rightarrow n = m$; $\exists \sigma \in S_n \; \exists c_i \in F^* : \forall i \;\; q_i = c_i p_{\sigma(i)}$

Зам. Неразложимость над поле

$x^2 - 2$ - неразл. над $\mathbb{Q}$; разл. над $\mathbb{R}$

$x^2 + 1$ - неразл. над $\mathbb{Q}$ и $\mathbb{R}$ | разл. над $\mathbb{C}$

Тв. f - неприв. $\Leftrightarrow$ $(f) \triangleleft F[x]$ максимален

Д-во $(\Rightarrow)$ Нека $\exists g: (f) \subseteq (g) \subseteq F[x]$

$\Rightarrow g / f \Rightarrow (g) = (1)$ или $(g) = (f)$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad$ " $F[x]$ $\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \uparrow$

$(\Leftarrow)$ $f = gh$, $\underline{\deg g \neq 0, \deg f}$ $\quad\quad$ $\underset{\uparrow}{\deg g} = \deg f$ $\quad \underset{\uparrow}{\deg g} = 0$

$g / f \Rightarrow (f) \subseteq (g) \subseteq F[x] \overset{\max}{\Rightarrow} (g) = (f)$ или $(g) = (1)$

Сл. f - неприв. $\Leftrightarrow F[x]/(f)$ - поле

Заб. $|F| < \infty \to \operatorname{char} F = p \neq 0 \to \mathbb{Z}_p < F$

F е ЛП над $\mathbb{Z}_p$ ... КМЛП ; $\dim_{\mathbb{Z}_p} F = n \to |F| = p^n$

обратно ; $n = 1 \to \mathbb{Z}_p$ е поле

Ако $f \in \mathbb{Z}_p[x]$ е неразл. и $\deg f = n$, то

$$\left| \underbrace{\mathbb{Z}_p[x] / (f)}_{\text{поле}} \right| = p^n$$

__Зад.__ K - ком. пр. с 1, $f \in K[x]$ със ст. коеф. от K^*

$$K[x]/(f) = \{ g + (f) \mid g \in K[x] \}$$

$$= \{ g + (f) \mid g \in K[x], \deg g < \deg f \}$$

$g = fq + r$ $\quad$ $g - r = fq \in (f) \Rightarrow g + (f) = r + (f)$

$\deg r < \deg f$

За единственост трябва K да е област

~~Ако K е поле~~

Зад. $\mathbb{R} \to \mathbb{C}$ с $f = x^2+1$

- x^2+1 – неразл. над $\mathbb{R}$

Ако е разл. $\Rightarrow \exists \alpha, \beta \in \mathbb{R}$ $x^2+1 = \underline{(x-\alpha)}\underline{(x-\beta)}$

$\Rightarrow \overbrace{\alpha^2+1}^{\geq 1} = 0$?!

полин. от 1 ст. $\neq 0, 2$

- $\mathbb{R}[x]/(x^2+1) = \mathbb{C}_0$ е поле

$\left(\mathbb{C}_0 = \{ \overbrace{g + (x^2+1)}^{=\bar{g}} \mid \deg g < 2 \} = \{ \overline{ax+b} \mid a, b \in \mathbb{R} \} = \right.$

$= \{ \bar{a}\,\bar{x} + \bar{b} \mid a, b \in \mathbb{R} \}$

$\varphi : \mathbb{R}[x] \to \mathbb{C}_0 = \mathbb{R}[x]/(x^2+1)$

$x \longmapsto \alpha$ (реално $\alpha = \bar{x}$)

$\psi = \varphi|_{\mathbb{R}} : \mathbb{R} \to \mathbb{C}_0$ $\quad \ker \varphi|_{\mathbb{R}} \lhd \mathbb{R} \Rightarrow = (0), \mathbb{R}$

$\mathbb{R} \Rightarrow \varphi = 0$

$= (0) \Rightarrow$ [illegible].

$\varphi|_{\mathbb{R}}(\mathbb{R}) = \mathbb{R}_0 < \mathbb{C}_0$, $\mathbb{R}_0 \cong \mathbb{R}$

$\mathbb{C}$

$\mathbb{C}_0$ rozgr[illegible]

$\mathbb{R} \xrightarrow{\cong} \mathbb{R}_0$

$\theta : \mathbb{R}[x] \to \mathbb{C}_0[x]$

$g = \sum a_i x^i \longmapsto \sum \psi(a_i) \cdot x^i = \theta(g)$

$(\theta(f))(\alpha) = (\psi(1) \cdot x^2 + \psi(1))(\alpha) = \psi(1) \cdot \alpha^2 + \psi(1) =$

$f = x^2+1$

$= \underbrace{\varphi|_{\mathbb{R}}(1) \cdot \varphi(x)^2}_{= \varphi(1)} + \varphi|_{\mathbb{R}}(1) = \varphi(x^2+1) = 0$