Лекция 14 05.01.22г

Нека $F[x]$ е комут. пр-н с 1 на полиномите на промен. x с коеф-ти от полето F, $F[x]$ – евклидов.
Да напомним, че Th (за дел. с ч. и ост. при f) гласи: $\forall f, g\neq 0$, $f, g \in F[x]$, $\exists!\, q, r \in F[x]$:

$$f = gq + r, \quad \deg r < \deg g.$$

<u>Тв (схема на Хорнер)</u>. Нека $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in F[x]$, $a_0 \neq 0$ и $g(x) = x - \alpha \in F[x]$. От Th за деление с частно и остатък имаме:

$$f = gq + r, \quad q = b_0x^{n-1} + b_1x^{n-1} + \ldots + b_{n-1} \in F[x]$$

$$\deg r < \deg g = 1 \Rightarrow r = \underset{\in F}{const}$$

Тогава са в сила следните равенства:

	a_0	a_1	a_2	$\ldots$	a_{n-1}	a_n
α	b_0	b_1	b_2	$\ldots$	b_{n-1}	r

като

$b_0 = a_0$

$b_1 = a_1 + \alpha b_0$

$b_2 = a_2 + \alpha b_1$

$\ldots$

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

$r = a_n + \alpha b_{n-1}$

Док: Както се покаже когато $f = gq + r$, то се сравнят коефициентите пред
$$(\ldots)x^k = (\ldots)x^k, \quad k = \overline{0,n}$$

Сл: В $F[x]$ всеки идеал $I \trianglelefteq F[x]$ е главен, т.е. $I = (f) = \langle f \rangle = \{ fg \mid g \in F[x] \}$ идеал, породен от пол. f.

Док: $I = \langle 0 \rangle \trianglelefteq F[x]$. Нека $I \neq \{0\}$ и тогава избираме $f \neq 0$, <u>$f \in I$ от най-малката възможна степен.</u> Ще покажем, че $I = \langle f \rangle$. Ясно е, че $\langle f \rangle \trianglelefteq I \trianglelefteq F[x]$.

Ако $h \in I \Rightarrow h = fq + r$, $\deg r < \deg f$
$$\Rightarrow r = 0 \Rightarrow h = fq,\ q \in F[x] \Rightarrow h \in \langle f \rangle$$
$$\Rightarrow I \trianglelefteq \langle f \rangle \Rightarrow I = \langle f \rangle$$

Сл: Ако A - комут. пр. с 1, $A[x]$, $f \in A[x]$, $\alpha \in A$. Тогава
$$f(\alpha) = 0 \iff f = (x-\alpha)g,\ g \in A[x]$$

Док: $f = (x-\alpha)g + r$, $\deg r < 1 \Rightarrow r = const \in A$ и $r = 0 \iff f = (x-\alpha)g$

<u>Сл</u>: Нека A - област и $f \in A[x]$, $f \neq const.$ и $\deg f \leq n$. Ако $\exists\ \beta_1, \beta_2, \ldots, \beta_{n+1}$ $\underline{\beta_i \in A}_{\ i=\overline{1,n+1}}$ и $\beta_i \neq \beta_j$, $i \neq j$ и такива, че

$$f(\beta_i) = 0,\ i = \overline{1, n+1}.\ \text{То тогава } f = 0.$$

<u>Заб</u>: $Ð +$ Сл $\Rightarrow f$ има най-много $\underline{n}$ на брой два или два различни ~~корена~~

<u>Док</u>: $f \neq 0$, $f(\beta_1) = 0 \underset{\text{Сл}}{\Rightarrow} f(x) = (x - \beta_1) g(x)$
$\deg g < \deg f$

$\Rightarrow g \in A[x]$, $\deg g \leq n-1$ и $f(\beta_2) = 0 \Rightarrow$

$$0 = f(\beta_2) = \underbrace{(\beta_2 - \beta_1)}_{\neq 0} g(\beta_2) \underset{j=\overline{2,n+1}}{\Rightarrow} g(\beta_2) = 0$$

$g(\beta_2) = 0 \underset{\text{Сл}}{\Rightarrow} g(x) = (x - \beta_2) h(x)$, $\deg h(x) \leq n-2$

и $f(\beta_3) = g(\beta_3) = 0 \Rightarrow h(\beta_3) = 0$

като $f(x) = (x - \beta_1)(x - \beta_2) h(x)$

и така след n-стъпки ще имаме

$$f=(x-\beta_1)(x-\beta_2)\ldots(x-\beta_n)t(x),\ \deg t\le 0$$

$$\Downarrow$$

$$t=\text{const}$$

$f(\beta_{n+1})=0=t(\beta_{n+1})$ противоречие

$$\Rightarrow f=0 \qquad \square$$

$$f=a_0(x-\beta_1)\ldots(x-\beta_n)\in A[x]$$

<u>Сл (принцип за сравняване на коефициентите)</u>:
Нека A-област, $f,g\in A[x]$, $\deg f\le n$, $f\ne\text{const}$, $\deg g\le n$, $g\ne\text{const}$ и $\exists\ \beta_1,\ldots,\beta_{n+1}\in A$, два по два различни елта ($\beta_i\ne\beta_j$, $i\ne j$), за които $f(\beta_i)=g(\beta_i)$, $i=\overline{1,n+1}$. Тогава

$$f=g.$$

<u>Дво</u>: $h=f-g\in A[x]$ и предното

Сл $\Rightarrow h=0 \Rightarrow f=g.$ $\square$

<u>Пример</u>: $f=x^2\in\mathbb{Z}_{16}[x]$; $f(\alpha_i)=\bar{0}$, $\alpha_i\in\mathbb{Z}_{16}$
$\deg f=2$; $\mathbb{Z}_{16}$ не е област $\alpha_i=\bar{0},\bar{4},\bar{8},\overline{12}$

Нека F-поле, $F^* = F \setminus \{0\}$, $F[x]$-област.

Аритметика в пр на полиноми $F[x]$

Def: Нека $f, g \in F[x]$, $g \neq 0$. Казваме че "g дели f" и означаваме g/f, $g|f$, ако $\exists h \in F[x] : f = gh$. В противен случай ще пишем $g \nmid f$.

Св-ва:

1) $af | bf$, $a \in F^*$, $f \neq 0$, $b \in F$, $f \in F[x]$

2) $f|g$ и $g|f \Rightarrow f = cg$, $c \in F^*$
ако f, g - унитарни $\Rightarrow f = g$

3) $f|g$ и $g|h \Rightarrow f|h$

4) $f|g \Rightarrow af|ag$, $a \in F^*$

5) $f | h_i$, $i = \overline{1,k} \Rightarrow f \mid t_1h_1 + t_2h_2 + \dots + t_kh_k$, $t_i \in F[x]$ ✓

6) $f | h_1 + h_2$ и $f|h_1 \Rightarrow f|h_2$

В частност ако $h_1 + h_2 = 0$, то $f|h_1 \Rightarrow f|h_2$.

Деф. Нека $f, g \in F[x]$, $g \neq 0$. Казваме че един полином $d \in F[x]$ е най-голям общ делител на f и g и означаваме $d = (f, g)$, ако d изпълнява следните две условия:

1) $d \mid f$ и $d \mid g$
2) $d_1 \mid f$ и $d_1 \mid g \Rightarrow d_1 \mid d$.

Деф. По-общо, ако $f_1, \dots, f_k \in F[x]$, $f_i \not\equiv 0$, то

$$(f_1, \dots, f_k) := ((f_1, \dots, f_{k-1}), f_k).$$

Деф: Казваме че f, g са взаимно прости ако $(f, g) = 1$. $\left((f, g) = a \in F^* \right)$.

Забел. Ако $a \in F^*$ и $d = (f, g)$, то $ad = (f, g)$, т.е. НОД на f и g се определя с точност до ненулева константа от F.

Ако търсиме еднозначност на d, искаме d да е унитарен полином.

Th: За всеки два полинома $f, g \in F[x]$, $g \neq 0$, $\exists\, d = (f,g)$.

Док: (I д-во) Нека $I = \langle f, g \rangle = \{uf + vg \mid u, v \in F[x]\}$

I - идеал, породен от f и g

и т.к. всеки идеал в $F[x]$ е главен, то

$I = \langle f, g \rangle = \langle d \rangle$, където $d = (f,g)$

и като резултат е в сила тъждеството на Безу, т.е. $\exists\, u, v \in F[x]$: $d = uf + vg$.

(II д-во) Алгоритъм на Евклид: $f, g \neq 0$, $F[x]$

$d_1 \downarrow$ $f = gq + r$, $\deg r < \deg g$

ако $r = 0 \Rightarrow d = (f,g) = g$, иначе

$g = r q_1 + r_1$, $\deg r_1 < \deg r$

$r = r_1 q_2 + r_2$, $\deg r_2 < \deg r_1$

$r_{k-2} = r_{k-1} q_k + \boxed{r_k}$, $\deg r_k < \deg r_{k-1}$

$r_{k-1} = \boxed{r_k} q_{k+1}$, $r_{k+1} = 0$

$r_k = d a,\ a \in F^*,\ d = (f, g)$

$d = r_k = r_{k-2} - r_{k-1} q_k = \underset{\substack{\text{само} \\ f, g, q_i}}{\cdots} = (\ _u\ ) f + (\ _v\ ) g$

и имаме тъждество на Безу, че

$d = fu + gv.$

<u>Заб.</u> 1) $d = (f, g) \Rightarrow \exists\, u, v :\ uf + vg = d$

в общия сл. u, v <u>не са</u> определени!

2) $(f, g) = 1 \Leftrightarrow \exists\, u, v :\ uf + vg = 1$

като u, v <u>не са</u> еднозначно определени.

<u>Сл:</u> 1) $f, g, h \in F[x] \Rightarrow f \mid gh$ и $(f, g) = 1$

$\Rightarrow f \mid h$

<u>Док:</u> $(f, g) = 1 \Rightarrow uf + vg = 1 \ / \cdot h$

$ufh + vgh = h$

$f \mid \quad f \mid gh \Rightarrow f \mid h$

2) $\left.\begin{array}{l}(f,g)=1 \\ (f,h)=1\end{array}\right\} \Rightarrow (f,gh)=1$

Док. $\left.\begin{array}{l}uf+vg=1 \\ af+bh=1\end{array}\right\} \text{"}\cdot\text{"} \Rightarrow ua\underline{\underline{f}}^2+ub\underline{\underline{f}}h+av\underline{\underline{f}}g+$

$+bvgh=1$

$\underbrace{(uaf+ubh+av g)}_{U}f+\underbrace{(bv)}_{W}gh=1 \Rightarrow Uf+Wgh=1$

$\Rightarrow (f,gh)=1$

3) $f,g,h\in F[x]$, $g|f$ и $h|f$ и $(g,h)=1$

$\Rightarrow gh|f$.

Док: $g|f \Rightarrow f=gg_1$, $g_1\in F[x]$

$\left.\begin{array}{l}(g,h)=1 \\ h|f=gg_1\end{array}\right\} \Rightarrow h|g_1 \Rightarrow$

$\cancel{h=g_1h_1}$ $g_1=h_1h \Rightarrow f=\underbrace{gh}h_1$

$\Rightarrow gh|f$.

Извод: $\forall f, g \neq 0 \; \exists!$ (с точност до константа) НОД на f, g, т.е. $d = (f, g)$.

Деф: Нека $f, g \in F[x]$, $f, g \neq 0$. Казваме че $m \in F[x]$ е най-малкото общо кратно на f и g и означаваме $m = [f, g]$, ако m изпълнява следните две условия:

1) f / m и g / m
2) f / m_1 и $g / m_1 \Rightarrow m / m_1$.

Деф. По-общо, ако $f_1, \dots, f_k \in F[x]$, $f_i \neq 0, i = \overline{1,k}$, то $[f_1, \dots, f_k] := [[f_1, \dots, f_{k-1}], f_k]$.

Тв: Ако $f, g \in F[x]$, $f \neq 0$ $g \neq 0$, то е в сила следното равенство

$$(f, g)[f, g] = a f g, \; a \in F^*$$

Th Нека $I = \langle f \rangle \trianglelefteq F[x]$ и $J = \langle g \rangle \trianglelefteq F[x]$.

Тогава са изпълнени следните ~~уст~~ равенства $\trianglelefteq F[x]$:

1) $I + J = \langle f \rangle + \langle g \rangle = \langle d \rangle$, $d = (f, g)$
$= (f) + (g) = (d) = ((f, g))$

2) $I \cap J = \langle f \rangle \cap \langle g \rangle = (f) \cap (g) = \langle m \rangle =$
$= (m) = ([f, g]) = \langle [f, g] \rangle \trianglelefteq F[x]$

3) $IJ = (f)(g) = \langle f \rangle \langle g \rangle = \langle fg \rangle = (fg) \trianglelefteq F[x]$

Неразложимост на полиноми, $f \in F[x]$.

Нека $f \in F[x]$, $\deg f > 0$.

Def. Казваме, че f е неразложим над полето F полином, ако не съществуват полиноми $g, h \in F[x]$, $\deg g < \deg f$, $\deg h < \deg f$, за които $f = gh$, т.е. единствените делители на f са от вида af, $a \in F^*$.

Заб. Над полето F е съществено, т.к.

$f = x^2 - 7 \in \mathbb{R}[x]$, то f е разложим
$\in \mathbb{C}[x]$ над $\mathbb{R}$ и над $\mathbb{C}$ които
$f = (x-\sqrt{7})(x+\sqrt{7}) \in \mathbb{R}[x], \in \mathbb{C}[x]$.

$f = x^2 - 7 \in \mathbb{Q}[x]$, то f е неразложим над полето $\mathbb{Q}$ които.

Извод: Полиномите от първа степен т.е от вида $ax+b \in F[x], a \neq 0$ са неразложими над полето F полиноми.

Тв. Нека $f \in F[x]$ и $p \in F[x]$, p-неразложим над F полином.

Тогава $p \nmid f \iff (p, f) = 1$.

Тв. Нека $p \in F[x]$, p-неразложим над F полином

и $f, g \in F[x]$. Ако $p \mid fg$, то p дели поне единия от тях, т.е. $p \mid f$ и/или $p \mid g$.

Th (**еднозначно разлагане на неразложими множители**) Нека $F[x]$, $f \neq const$. Тогава f се разлага в произведение на неразложими над полето F полиноми и това разлагане е единствено с точност до реда на множителите, т.е. ако $f = p_1 p_2 \dots p_k = q_1 q_2 \dots q_s$, то $k=s$ и след евентуално преномериране са в сила равенствата $q_j := a_j . p_j$, $a_j \in F^*$, $j = \overline{1,k}$.

Док: $\underline{\exists}$) Индукция по $\deg f = \underline{n} \geq 0$:

Ако f е неразложим над F полином, то

$$f = f.1 = p_1.$$

Ако f е разложим над F полином, т.е.

$$f = gh, \quad \deg g < \deg f \text{ и } \deg h < \deg f$$

то по ИП: $g = p_1 \dots p_l$, $h = p_{l+1} \dots p_k$

$$\Rightarrow f = p_1 \dots p_k.$$

!) Нека $f = p_1 p_2 \dots p_k = q_1 q_2 \dots q_s$, където p_i, q_j са неразложими над F полиноми $(p_i, p_j) = 1$, $i \neq j$. Индукция по $\underline{k}$

$$f = \underbrace{p_1 p_2 \dots p_k}_{p_1 |} = \underbrace{q_1 q_2 \dots q_s}_{p_1 |} \quad \text{и база } \underline{p_1}$$

$p_1, q_j, j = \overline{1,s}$ нер. $\Rightarrow$ с точност до преномериране $p_1 \mid q_1$

$\Leftrightarrow \quad q_1 = a_1 p_1, \; a_1 \in F^*$. (от нер. над F p_1, q_1 които)

$$\Rightarrow f = \cancel{p_1} p_2 \dots p_k = (a_1 p_1) q_2 \dots q_s = \cancel{p_1} (a_1 q_2) \dots q_s$$

и от ИП $\quad p_2 \dots p_k = (a_1 q_2) \dots q_s$

имаме, че $\quad q_l = a_l p_l, \; l = \overline{2,k}, \; \underline{k = s}$

$\Rightarrow f = p_1 p_2 \dots p_k$, където p_i – неразложими над полето F полиноми.

Def. Казваме че едно поле F е алгебрически затворено поле, ако всеки неконстантен полином f с коефиц. от F има корен в F, т.е. $f=(x-\alpha)g$, $g\in F[x]$, $\alpha\in F$.

Сл: $f\in F[x]$, $f\neq const$, F – алг. затворено поле, то $\deg f = n > 0$

$$f=a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n),\ a\in F^*$$

т.е. ако алг. затв. поле F и $f\in F[x]$, f се разлага на линейни множители

Th (Основната Th на алгебрата, Th на Даламбер) Полето на комплексните числа $\mathbb{C}$ е алгебрически затворено поле.

Извод! Неразложимите над полето на $\mathbb{C}$ числа полиноми са само от вида $ax+b$, $a,b\in\mathbb{C}$, $a\neq 0$, т.е. само от 1 deg

$\mathbb{Z}$

Над полето на $\mathbb{R}$ числа:

Лема на Гаус: Всеки неконстантен полином f с реални коефициенти притежава поне един комплексен корен.

в $\mathbb{R}[x]$: $f = (x-\alpha_1)\dots(x-\alpha_s)(a_1x^2+b_1x+c_1)\dots(a_\ell x^2+b_\ell x+c_\ell)$

$\deg f = n > 0 \qquad \underset{i=\overline{1,s}}{\alpha_i \in \mathbb{R}}\ , \quad s+\frac{\ell}{2}=n$

$$\underset{\in \mathbb{C}[x]}{(x-\gamma)(x-\bar{\gamma})} = ax^2+bx+c \in \mathbb{R}[x]$$

$$D = b^2-4ac < 0$$

$\gamma+\bar{\gamma} \in \mathbb{R}$

$\gamma\bar{\gamma} \in \mathbb{R}$

Извод: В полето на реалните числа $\mathbb{R}$ неразложимите полиноми са от вида:

$ax+b, \quad a,b \in \mathbb{R}, \ a \neq 0$

$ax^2+bx+c, \quad a,b,c \in \mathbb{R}, \ a \neq 0$

$D = b^2-4ac < 0.$

Над полето на рационалните $\mathbb{Q}$ числа:

$f = c_0 x^n + c_1 x^{n-1} + \dots + c_n \in \mathbb{Q}[x]$, $c_i = \frac{p_i}{q_i}$, $(p_i, q_i) = 1$

I) Нека $q = [q_0, \dots, q_n]$ и

$f = \frac{1}{q}(b_0 x^n + \dots + b_n)$, $b_i \in \mathbb{Z}$.

$f = c_0 x^n + \dots + c_n$ и $b_0 x^n + \dots + b_n$ са едновременно разложими (неразложими) над полето $\mathbb{Q}$ полиноми

$\Rightarrow$ работим в комут. пръстен с 1 на целите числа $\mathbb{Z}$, но правим извод за f в полето на рац. числа $\mathbb{Q}$.

II) $f = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in \mathbb{Z}[x]$, $a_0 \neq 0$

Избираме просто число $p \nmid a_0$ и $\overline{a_i} = a_i + p\mathbb{Z}$

$\overline{a_i} \in \mathbb{Z}_p$ поле

Тогава разглеждаме редуцирания по модул p полином на f:

$\mathbb{Z}_p[x] \ni \overline{f} = \overline{a_0} x^n + \overline{a_1} x^{n-1} + \dots + \overline{a_{n-1}} x + \overline{a_n}$.

в $\mathbb{Z}_7[x]$, $f = 3x^6 + 2x^5 + 15x^4 + 35x^3 + 17 \in \mathbb{Z}[x]$

$\Rightarrow \overline{f} = \overline{3}x^6 + \overline{2}x^5 + x^4 + \overline{3} \in \mathbb{Z}_7[x]$.

III.