Тема 28

Определение за полиноми на една променлива с коеф над поле, действия с полиноми, степен на полином, твърдение за степента на сумата и на произведението на полиноми (с д-во).
Теорема за деление с частно и остатък при полиноми (с д-во), схема на Хорнер
НОД на полиноми с коефициенти от поле – определение, теорема за съществуване на НОД на полиноми и тъждество на Безу (с д-во), алгоритъм на Евклид за намиране на НОД (с д-во, че се получава НОД на полиномите)
Корени на полином – определение, принцип за сравняване на коефициентите (само формулировка), формули на Виет за полином от степен n.

I. Определение за полиноми на една променлива с коеф над поле, действия с полиноми, степен на полином, твърдение за степента на сумата и произведението

~~Ще дефинираме следния понятия~~

~~Деф: Комутативен пръстен с единица е непразно множество A с дефинирани операции събиране и умножение т.е. $\forall a, b \in A \rightarrow$ $c = a+b \in A$, $d = a \cdot b \in A$~~

Деф: Нека A е комутативен пръстен с единица. Да означим с B мн-вото от всички безкрайни редици $(a_0, a_1, a_2, \dots)$ с елементи от A, в които само краен брой елементи са различни от нула. От дадено място нататък, всички останали елементи са 0.

$$B = \{ f = (a_0, a_1, \dots, a_n, 0, 0, \dots) \mid a_i \in A \}$$

Нека $f = (a_0, a_1, \dots, a_n, 0, 0, \dots)$ и $g = (b_0, b_1, \dots, b_m, 0, 0, \dots)$ и $m \le n$ $\in B$. В множеството B въвеждаме операциите "+" и "·" в B:

$f + g := (a_0 + b_0, a_1 + b_1, \dots, a_m + b_m, a_{m+1}, \dots a_n, 0, 0, 0, \dots) \in B$, т.е. събиране покомпонентно

$f \cdot g := (c_0, c_1, c_2, \dots, c_k, 0, 0, \dots) \in B$, където $c_n = \sum\limits_{i+j=n} a_i b_j$

$c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$ и т.н.

С така въведените операции B е комутативен пръстен с единица

В B означаваме:

$0 = (0, 0, 0, \dots)$ нулата в B

$1 = (1, 0, 0, \dots)$ единицата в B

$x = (0, 1, 0, 0, \dots)$ $\quad x^2 = (0, 0, 1, \dots)$, $x^3 = (0, 0, 0, 1, \dots)$

$x^n = (0, 0, \dots, 0, 1, 0, \dots) \rightarrow$ 1-цата стои на $(n+1)$ позиция

ако $a \in A$, то $ax^n = (0, 0, \dots, 0, a, 0, 0, \dots) \rightarrow a$ стои на $n+1$ позиция

с f бележим $f = (a_0, a_1, a_2, \dots, a_n, \dots) = (a_0, 0, 0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, \dots, 0, a_n, 0, \dots) = a_0 + a_1 x^1 + a_2 x^2 + \dots + a_n x^n$.

$(-f) = (-a_0, -a_1, -a_2, \dots, -a_n, 0, 0, \dots)$

Елементите на B наричаме полиноми на една променлива с коеф. над A ~~с коеф~~

! Ако F е поле, то B е област
област ии

- Всеки полином се записва по еднакъв начин във позната вид $a_0+a_1x^1+\dots+a_nx^n$

Пръстена B се означава с $A[x]$ и се нарича пръстен на полиномите на една променлива x с коеф. от A, а елементите му полиноми

Нека $f = a_0x^0 + a_1x^1 + \dots + a_nx^n$ е полином, тогава наричаме
- старши коефициент – коефициентът пред най-високата степен на полинома
- коефициент на f – коефициент a_i за $i=\overline{1,n-1}$
- свободен коефициент – коефициент, където степента на x е нула

f ще го бележим вече с уговорката $f = \cancel{a_0+a_1x+a_2x}$ $a_0x^n+a_1x^{n-1}+\dots$
a_0 – старши коеф, a_n е свободен член

- степен на полином f – $\deg f := n$ – числото n се нарича степен на полинома, най-високата степен на x с к...
  - $\deg f = 0$, ако f е ненулев константен полином $(a,0,0,0,\dots)$ и $a \in A$, но $a \neq 0$
  - степента на нулевия полином $(0,0,0,0,\dots)$ е $-\infty$.

Тв: Нека A е комутативен пръстен с единица. За $\forall$ $f,g \in A[x]$, т.ч. ~~Нека~~ $\deg f = n$, $\deg g = m$
- $\deg(f+g) \leq \max(\deg f, \deg g)$
- Ако A е област, то $\deg(f.g) = \deg f + \deg g$

Д-во:

II. Теорема за деление с частно и остатък при полиноми (с д-во)

~~- Нека F е поле и $F[x]$ е полиномиалния пръстен на променлива x с коефициенти от полето F и $F[x]$ е област.~~
~~Нека $f = a_0x^n + a_1x^{n-1} + \dots + a_n$, $a_0 \neq 0$ и $g = b_0x^m + b_1x^{m-1} + \dots + b_m$, $b_0 \neq 0$~~
~~$f, g \in F[x]$ и $g \neq 0$~~

Теорема: Нека F е поле и $f, g \in F[x]$, $g \neq 0$. Тогава съществува единствена двойка полиноми $q, r \in F[x]$, т.ч. $f = g.q + r$ и $\deg r < \deg g$
(q се нарича частно, а r се нарича остатък)

Д-во: Съществуване: Нека $f = a_0x^n + \dots + a_n$, $a_0 \neq 0$
$g = b_0x^m + \dots + b_m$, $b_0 \neq 0$.

1а) ако $g = b_0 \neq 0$, т.е. g е константа и $f = b_0 . \underbrace{(b_0^{-1} f)}_{q} + \underbrace{0}_{r}$

Тук, ако F не беше поле, нямаше да може да се вземе обратния елемент на b_0.

$\deg 0 = \deg r = -\infty <$ [illegible] $\deg g = 0$

2а) нека $\deg f < \deg g$, то тогава $f = g.0 + \underbrace{f}_{r}$ и $\deg r = \deg f < \deg g$

3а.) нека $\deg f \geq \deg g \geq 0$ и $g \neq 0$, т.е. $f = a_0x^n + a_1x^{n-1} + \dots + a_n$, $a_0 \neq 0$
$g = b_0x^m + \dots + b_m$, $b_0 \neq 0$

Ще го докажем с индукция по степента на полинома f (с по-висока степен е)

$$\begin{array}{l|l} f = a_0x^n + \dots & g = b_0x^m \\ \hline -a_0x^n + \dots & q_1 = b_0^{-1}a_0x^{n-m} \\ \hline f_1,\ \deg f_1 < n & \end{array}$$

~~Съображение:~~ - По какво да умножим, за да се получи a_0?

$f_1 = f - a_0 . b_0^{-1} x^{n-m} . g$ е от степен по-малка от n. От индукционното предположение, съществуват $q_1, r_1 \in F[x]$, т.ч. $f_1 = g.q_1 + r_1$ и $\deg r_1 < \deg g$

Така $f = f_1 + a_0b_0^{-1}x^{n-m} . g = gq_1 + r_1 + a_0b_0^{-1}x^{n-m} . g = g(q_1 + a_0b_0^{-1}x^{n-m}) + r_1$

Полагаме $q = q_1 + a_0b_0^{-1}x^{n-m}$ и $r = r_1$. Тогава $f = g.q + r$ и $\deg r < \deg g$

- Единственост: Нека допуснем, че има втора двойка, удовлетворяваща теоремата, т.е.
$f = gq + r = g.q' + r'$ и $\deg r < \deg g$ и $\deg r' < \deg g$.

$\Rightarrow$ ~~$g(q'-q)$~~ $g(q - q') = r' - r$. Ако $q \neq q'$ $\Rightarrow$ $\deg(g(q - q')) =$
$= \deg g + \deg(q - q') \geq \deg g > \deg(r' - r)$, противоречие,

$\deg r < \deg g$ и $\deg r' < \deg g$, но $\deg(g(q-q')) = \deg(r'-r) \Rightarrow$ е противоречие

~~$\deg(g(q-q')) = \deg g + \deg($~~

Следователно $q = q'$, откъдето следва че и $r = r'$ $\Rightarrow$ теоремата е доказана

! Ако сме в област, то някой елемент може да нямат обратни елементи, ...
Теоремата е в сила над поле. или ако b_0 е обратим и така за всяка област
Това доказателство дава и практически алгоритъм за намиране на полиномите q и r.

Схема на Хорнер

Нека $f = a_0x^n + \dots + a_n$, $a_0 \neq 0 \in F[x]$

нека $g(x) = x - \alpha \in F[x]$

От теоремата за деление с частно и остатък имаме, че
$f = g.q + r$, $\deg r < \deg g = 1$, т.е. $r \in F$ – r е константа

и $q = b_0x^{n-1} + \dots + b_{n-1}$

Тогава са в сила следните равенства:

	a_0	a_1	a_2	a_3	$\dots$	a_{n-1}	a_n
α	b_0	b_1	b_2	b_3	$\dots$	b_{n-1}	r

$b_0 = a_0$
$b_1 = a_1 + \alpha . b_0$
$b_2 = a_2 + \alpha . b_1$
$\dots$

$b_{n-1} = a_{n-1} + \alpha . b_{n-2}$ $\qquad r = a_n + \alpha . b_{n-1}$

Следствие: Нека A е комутативен пръстен с единица и $f \in A[x]$, $\alpha \in A$.
Тогава $f(\alpha) = 0 \Leftrightarrow f = (x-\alpha).q$ за някой полином $q \in A[x]$

Следствие: Нека A е област и $f \in A[x]$, $f \neq const.$ и $\deg f \le n$.
Ако $\exists \beta_1, \beta_2, \dots, \beta_{n+1}$, т.ч. $\beta_i \in A$, $i = \overline{1,n+1}$ и $\beta_i \neq \beta_j$ за $i \neq j$
т.че $f(\beta_i) = 0$, $i = \overline{1,n+1}$. Тогава $f = 0$

Заб. От следствието следва, че ако $\deg f \le n$, то f има най-много n на брой два по два различни корена

С. (принцип за сравняване на коефициентите)
– Нека A е област и $f, g \in A[x]$, $f \neq const$, $g \neq const$ и $\deg f \le n$ и $\deg g \le n$. Ако съществуват два по два различни елемента $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$ за които $f(\alpha_i) = g(\alpha_i)$ $i = \overline{1,n+1}$, то $f = g$

III НОД:

Нека F е поле, а с F^* означаваме $F^* = F \setminus \{0\}$, че $F[x]$ е област

Деф. Нека $f, g \in F[x]$, $g \neq 0$. Казваме, че "g дели f" и пишем $g \mid f$, ако $\exists\, h \in F[x]$, т.ч. $f = gh$. В противен случай g не дели f и пишем $g \nmid f$

Някои св-ва:
1) $af \mid bf$, $a \in F^*$, $f \neq 0$, $b \in F$, $f \in F[x]$
2) ако $f \mid g$ и $g \mid f$, то $f = c.g$, $c \in F^*$
3) ако $f \mid g$ и $g \mid h$, то $f \mid h$
4) ако $f \mid g$, то $af \mid ag$ за $a \in F^*$
5) ако $f \mid h_1 + h_2$ и $f \mid h_1$, то $f \mid h_2$ за $h_1, h_2, f \in F[x]$
6) ако $f \mid h_i$, $i = \overline{1,k}$, то $f \mid t_1h_1 + t_2h_2 + \dots + t_kh_k$, $t_i \in F[x]$

Деф (НОД) Нека $f, g \in F[x]$ и поне единия от двата е ненулев. Казваме, че полином $d \in F[x]$ е най-голям общ делител (НОД) на f и g, ако:
1) $d \mid f$ и $d \mid g$
2) ако $d_1 \mid f$, $d_1 \mid g$, то $d_1 \mid d$

Бележим $d = (f, g)$

Деф. (НОД на k полинома) – Ако $f_1, f_2, \dots, f_k \in F[x]$, и поне един е ненулев, то $(f_1, f_2, \dots, f_k) = ((f_1, \dots, f_{k-1}), f_k)$

Деф. Казваме, че $f, g \in F[x]$ са взаимно прости полиноми, ако $(f, g) = Const$, като тази константа $\in F^*$ (т.е. е ненулева)

Заб. Тогава НОД на два полинома се определя с точност до ненулева константа $\in F$

Теорема: За всеки два полинома $f, g \in F[x]$, като поне единият е ненулев съществува НОД $d = (f, g)$.

Деф (идеал)

Д-во: Нека I е идеалът на пръстена $F[x]$, породен от f и g, т.е. $I = \{uf + vg \mid u, v \in F[x]\}$. и $I \neq \{0\}$.
В пръстена $F[x]$ всеки идеал е главен. Нека $I = (d)$. Ще док, че $d = (f, g)$. От $f, g \in (d) \Rightarrow f = df_1$ и $g = dg_1$, $f_1, g_1 \in F[x] \Rightarrow d \mid f$ и $d \mid g$. От $d \in I \Rightarrow \exists\, u, v \in F[x]$ $d = uf + vg$.

Сега, ако $d_1 | f$, $d_1 | g$, то $d_1 | d$. Следователно $d = (f, g)$

Т-во за съществуване на НОД (Алгоритъм на Евклид)
- това т-во дава и правило за намиране на НОД

Нека $f, g \in F[x]$ ~~и $g \neq 0$~~
- Ако $g = 0$, и $f \neq 0$, то $(f, g) = f$. Нека $g \neq 0$

$$f = g \cdot q_1 + r_1, \quad \deg r_1 < \deg g$$

Ако $r_1 \neq 0$, то

$$g = r_1 q_2 + r_2, \quad \deg r_2 < \deg r_1$$, Ако $r_2 \neq 0$, то

$$r_1 = r_2 q_3 + r_3, \quad \deg r_3 < \deg r_2$$ и така...

Всеки получен остатък го делим на следващия:
Степените на последователните остатъци намаляват строго, то този процес е к[раен]
След краен брой стъпки ще получим нулев остатък

. Последният ненулев остатък е НОД на g и f
- Ако $r_1 = 0$, то $g | f$ и $(f, g) = g$
- Нека r_{k+1} е последният остатък, т.е. $r_{k+1} = 0$

Тогава $r_{k-1} = r_k \cdot q_{k+1}$

$\Rightarrow r_k | r_{k-1}$ // $r_{k-2} = r_{k-1} \cdot q_k + r_k \Rightarrow$

$r_k | r_{k-2}$ и т.н. $r_k | r_2 \Rightarrow r_k | r_1 \Rightarrow r_k | g$ и

$r_k | f$ и така разглеждайки равенствата отдолу нагоре излиза, че [...]

Ако $d_1 | f$ и $d_1 | g$, т.е. сега ще проследим равенствата отгоре надолу

$d_1 \Downarrow$
$$f = g q_1 + r_1$$
$$g = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$\ldots$$
$$r_{k-2} = r_{k-1} q_k + r_k$$
$$r_{k-1} = r_k q_{k+1} + r_{k+1} = 0$$

. Тогава $d_1 | r_1$, $d_1 | r_2$ и т.н. $d_1 | r_k$. Това е изпълнено условие 2) от дефиницията за НОД

От двете доказателства се вижда: Твърдение на Безу (Тъждество на Безу)
ако $(f, g) = d$, то съществуват полиноми $u, v \in F[x]$, т.ч.
$$uf + vg = d$$

$r_{k-3} = r_{k-2} \cdot q_{k-1} + r_{k-1}$

$d = r_k = r_{k-2} - r_{k-1} q_k = \dfrac{r_{k-3} - r_{k-1}}{q_{k-1}} - r_{k-1} q_k = \dots$ връщайки нагоре но

равенствата се получава, че $\underset{u}{(\dots)} \cdot f + \underset{v}{(\dots)} \cdot g = r_k = d$, т.е.

тъждеството на Безу е доказано.

- Забл. Полиномите u, V от Тъждеството на Безу са взаимно прости

IV Корени на полином – определение, принцип за сравняване на коефициенти (само формулировка), формули на Виет за полином от степен n.

Нека F е поле, $f(x) \in F[x]$ и $F[x]$ е област

Деф: Нека K е разширение на полето F, $f \in F[x]$ и $\alpha \in K$. Казваме, че α е корен на f, ако $f(\alpha)=$ $f = (x-\alpha) \cdot g$, $g \in K[x]$ $= 0$!

т.е. $f(\alpha) = 0$.

Теорема: Нека $f \in F[x]$ и $\deg f > 0$. Тогава съществува разширение K на полето F, в което полиномът f има корен

Следствие: Нека $f \in F[x]$ и $\deg f = n > 0$. Тогава съществува разширение K на полето F, над което f се разлага в произведение на линейни множители, т.е. всички корени на f са в това разширение

$f = a_0 (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) \in K[x]$

Деф: Нека $f \in F[x]$ и $\deg f = n > 0$. Най-малкото разширение L на полето F, в което $f = a_0 (x - \alpha_1) \dots (x - \alpha_n)$ се разлага на линейни множители наричаме поле на разлагане на полинома f над полето F.

От следствие* следва, че ако $\deg f \le n$, то f има най-много n на брой два по два различни корена.

Принцип за сравняване на коефициентите
- Нека A е област и $f, g \in A[x]$, $f \ne const$, $g \ne const$, $\deg f \le n$ и $\deg g \le n$. Ако съществуват два по два различни елемента $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$ на A, за които $f(\alpha_i) = g(\alpha_i)$, $i = \overline{1, n+1}$, то $f = g$

Формули на Виет за полином от степен n

Нека $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in F[x]$, $a_0 \neq 0$
и нека L е полето на разлагане на полинома f над полето F, т.е. $L \supseteq F$.

$\Rightarrow f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n = a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n) \in L[x]$,
където $\alpha_i \in L$, $i = \overline{1,n}$ са корените на f.
Тогава са в сила следните формули:

$$\sigma_1 = \alpha_1 + \alpha_2 + \dots + \alpha_n = (-1)^1 \frac{a_1}{a_0}$$

$$\sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_2\alpha_3 + \dots + \alpha_{n-1}\alpha_n = (-1)^2 \frac{a_2}{a_0}$$

$$\sigma_3 = \alpha_1\alpha_2\alpha_3 + \dots + \alpha_{n-2}\alpha_{n-1}\alpha_n = (-1)^3 \frac{a_3}{a_0}$$

$$\dots$$

$$\sigma_n = \alpha_1\alpha_2 \cdot \dots \cdot \alpha_n = (-1)^n \frac{a_n}{a_0}$$

В общ вид $\sigma_i = \sum_i \alpha_1\alpha_2\dots\alpha_i = (-1)^i \frac{a_i}{a_0}$

Броят изрази в сумата е $\binom{n}{i}$ за σ_i

Пример за полином от 3 степен
$f(x) = ax^3 + bx^2 + cx + d$, $a \neq 0$, $f \in F[x]$
$\alpha_1, \alpha_2, \alpha_3 \in L[x]$

$$\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = \frac{-b}{a}$$

$$\sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \frac{c}{a}$$

$$\sigma_3 = \alpha_1\alpha_2\alpha_3 = \frac{-d}{a}$$

Използвани дефиниции: (пръстен, комутативен пръстен с 1, област, поле, идеал)