POLINOMI NAD PROIZVOLJNIM POLJEM

Nad poljem $\mathbb{R}$ polinom: $f(x) = a_0 + a_1 x + \dots + a_m x^m$
$(a_0, a_1, \dots a_m \in \mathbb{R})$ beskonačno polje

$(f \equiv g) \Leftrightarrow (\forall x \in \mathbb{R})\ f(x) = g(x)$ tj. ako su iste vrijednosti fja f i g

konačno polje
Polje $(\{-1,0,1\},+,\cdot)$: $f(x)=x$ i $g(x)=x^3$ imaju iste vrijednosti za $\forall x \in \{-1,0,1\}$, ali $f \not\equiv g$

Zato polinom možemo definisati pomoću uređenih m-torki
negdje se koriste ∞ niz kod koga su ostali br. nule
ovdje nije bitno koje polje (∞, konačno)

DEF: Ako je F polje $F^1 \cup F^2 \cup \dots \cup F^m \cup \dots = \bigcup_{i=1}^{\infty} F^i$
tada elemente ove unije $F^1 \dots F^m$ zovemo polinomi nad poljem F.

unija treba da bi dobili polinome bilo kojeg stepena

To znači: F^1 sadrži (a_0)

F^2 sadrži (a_0, a_1)

$\vdots$

F^m sadrži $(a_0, a_1, \dots a_m)$

DEF: Ako je $P \neq 0$ i $P \in F^{m+1}$ tada je stepen polinoma $\deg P = m$.

DEF: Ako je $P = (a_0, a_1, \dots a_m)$ a $Q = (b_0, b_1, \dots b_n)$
tada definišemo $P + Q = (c_0, c_1, \dots c_s)$ gdje je:
$c_j = a_j + b_j$ $(j = 0, 1, \dots s)$, $s = \max\{m, n\}$

$P \cdot Q = (d_0, d_1, \dots d_{m+n})$ gdje je $d_j = \sum_{i=0}^{j} a_i \cdot b_{j-i}$ za $(j = 0, 1, \dots m+n)$

$d_1 = a_0 \cdot b_1 + a_1 \cdot b_0$ $\quad \boxed{i + j - i = j}$ bitno

Primjer 1: $(2,-1,4)+(1,2,-5,7)=(3,1,-1,7)$

Pr. 2: $(1,2,4)+(3,-1,-4)=(4,1)$

Pr. 3: $(a_0,a_1,a_2)\cdot(b_0,b_1)=(a_0b_0,\ a_0b_1+a_1b_0,\ a_1b_1+a_2b_0,\ a_2b_1)$

Kod množenja: $\deg(P\cdot Q)=\deg P+\deg Q$

DEF: $(0,1)\overset{\text{def}}{=}t$

T/ $(a_0,a_1,\dots a_m)=a_0+a_1t+\dots+a_mt^m$

Dokaz: (mat. indukcijom)

$$(0,1)^k=(\underbrace{0,\dots,0}_{k\text{ nula}},1)$$

za $k=1$ to vrijedi po def. t

za $k=2$: $(0,1)^2=(0,1)(0,1)=(0\cdot0,\ 0\cdot1+1\cdot0,\ 1\cdot1)=(0,0,1)$

Iz pretpostavke za bilo koje k tj.:

$$(0,1)^k=(\underbrace{0,\dots,0}_{k\text{ nula}},1)\quad \text{dobijamo:}$$

$$(0,1)^{k+1}=(0,1)^k\cdot(0,1)=(0,\dots,0,1)(0,1)=(\underbrace{0,\dots,0}_{k+1\text{ nula}},1)$$

$\Rightarrow$ vrijedi tvrdnja za $\forall k\in\mathbb{N}$

To znači da je:

$$(\underbrace{0,\dots,0}_{k\text{ nula}},1)=(0,1)^k=t^k$$

$$(a_0,a_1,\dots a_m)=(a_0)+(0,a_1)+(0,0,a_2)+\dots+(0,0,\dots0,a_m)$$
$$=a_0(1)+a_1(0,1)+\dots+a_m(\underbrace{0,0,\dots,0}_{m\text{ nula}},1)$$
$$=a_0+a_1t+\dots+a_mt^m$$

T: Hornerov teorem:

Pri dijeljenju polinoma $f(x)=a_0+a_1x+\dots+a_mx^m$ sa $x-\alpha$ dobije se količnik $g(x)=b_0+b_1x+\dots+b_{m-1}x^{m-1}$ i ostatak R, pri čemu je:

$$b_{m-1}=a_m$$

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

$$\vdots$$

$$b_0=a_1+\alpha b_1$$

$$R=a_0+\alpha b_0$$

$$a_0+a_1x+\dots+a_mx^m=(x-\alpha)(b_0+b_1x+\dots+b_{m-1}x^{m-1})+R$$

$$a_0+a_1x+\dots+a_mx^m=b_0x+b_1x^2+\dots+b_{m-1}x^m-\alpha b_0-\alpha b_1x-\dots-\alpha b_{m-1}x^{m-1}+R$$

Izjednačavanjem koeficijenata uz iste stepene od x imamo:

$$a_m=b_{m-1}$$

$$a_{m-1}=b_{m-2}-\alpha b_{m-1}$$

$$\vdots$$

$$a_1=b_0-\alpha b_1$$

$$a_0=R-\alpha b_0$$

Koeficijente polinoma $g(x)$ i ostatak R možemo izračunati primjenom Hornerove šeme:

α	a_m	a_{m-1}	$\dots$	a_1	a_0
	$\underbrace{b_{m-1}}_{a_m}$	$\underbrace{b_{m-2}}_{\alpha b_{m-1}+a_{m-1}}$	$\dots$	$\underbrace{b_0}_{\alpha b_1+a_1}$	$\underbrace{R}_{\alpha b_0+a_0}$

T_2: Bezuov teorem:

Vrijednost polinoma $f(x)$ u tački $x=\alpha$ jednaka je ostatku dobijenom pri dijeljenju polinoma $f(x)$ sa $(x-\alpha)$.

Dokaz:

$f(x)=(x-\alpha)(b_0+b_1x+\dots+b_{m-1}x^{m-1})+R$

gdje su $b_0, \dots b_{m-1}$, (koeficijenti) i R neodređeni (nezavise od

Ako stavimo $x=\alpha$ imamo:

$$f(\alpha)=R$$

Posljedica: Ako je $f(\alpha)=0$ tada je polinom $f(x)$ djeljiv sa $(x-\alpha)$ i $x=\alpha$ nazivamo nulom polinoma $f(x)$.

T_3: Vietov teorem:

Ako je $f(x)=a_0+a_1x+\dots+a_mx^m$ i $x_1, x_2, \dots, x_m$ nule polinoma $f(x)$, tada vrijedi:

$$x_1+x_2+\dots+x_m=\sum_{i=1}^{m}x_i=\frac{-a_{m-1}}{a_m}$$

$$x_1x_2+x_1x_3+\dots+x_{m-1}x_m=\sum_{i<j}x_ix_j=\frac{a_{m-2}}{a_m}$$

$$x_1x_2x_3+x_1x_2x_4+\dots+x_{m-1}x_{m-2}x_m=\sum_{i<j<k}x_ix_jx_k=\frac{-a_{m-3}}{a_m}$$

$$\vdots$$

$$x_1\cdot x_2\cdot\ldots\cdot x_m=(-1)^m\frac{a_0}{a_m}$$

Ove formule dobijemo tako što fju $f(x)$ prikažemo u obliku $f(x)=a_m(x-x_1)(x-x_2)\dots(x-x_m)$, a zatim množimo i upoređujemo koeficijente uz iste stepene od x.

Npr. $f(x)=a_2x^2+a_1x+a_0$; x_1, x_2

$$a_2x^2+a_1x+a_0=a_2(x-x_1)(x-x_2)$$

$$a_2x^2+a_1x+a_0=a_2x^2-a_2x_1\cdot x-a_2x_2\cdot x+a_2x_1x_2$$

$$a_2=a_2$$

$$a_1=-a_2x_1-a_2x_2 \Rightarrow x_1+x_2=\frac{a_1}{-a_2}$$

$$a_0=a_2x_1x_2 \Rightarrow x_1\cdot x_2=\frac{a_0}{a_2}$$

Th: Teorem o racionalnim nulama polinoma:

Ako je $f(x)=a_0+a_1x+\ldots+a_mx^m$ polinom sa cjelobrojnim koeficijentima $a_0,a_1,\ldots,a_m$, i $\frac{p}{q}\in\mathbb{Q}$ nula polinoma $f(x)$, pri čemu je $(p,q)=1$, tada je $p|a_0$ i $q|a_m$.

Dokaz: Neka je $f(x)=a_0+a_1x+\ldots+a_mx^m$ $a_0,\ldots,a_m\in\mathbb{Z}$ i $\frac{p}{q}\in\mathbb{Q}$ nula polinoma $f(x)$, $(p,q)=1$, tada je:

$$f\left(\frac{p}{q}\right)=a_0+a_1\frac{p}{q}+a_2\left(\frac{p}{q}\right)^2+\ldots+a_m\left(\frac{p}{q}\right)^m=0 \quad \ldots(*)$$

$$(*)\cdot\frac{q^m}{p} \Rightarrow \quad a_0\cdot\frac{q^m}{p}+a_1\cdot q^{m-1}+a_2\cdot p\cdot q^{m-2}+\ldots+a_mp^{m-1}=0 \quad \ldots(1)$$

$$(*)\cdot q^{m-1} \Rightarrow \quad a_0\cdot q^{m-1}+a_1pq^{m-2}+a_2\cdot p^2q^{m-3}+\ldots+a_m\frac{p^m}{q}=0 \quad \ldots(2)$$

U jednakosti (1) svi sabirci osim prvog su cijeli, a kako su koeficijenti polinoma $f(x)$ cjelobrojni, to mora biti i prvi sabirak cijeli. Kako su p i q relativno prosti brojevi oni se ne mogu dijeliti pa se a_0 mora kratiti sa p tj. $p|a_0$. Analogno za jednakost (2) $q|a_m$.

T5: Potreban i dovoljan uslov da podskup vektorskog prostora i sam bude vektorski prostor:

Podskup W vektorskog prostora V nad poljem F je podprostor prostora V akko je W neprazan podskup od V i ako vrijedi: $(\forall x,y \in W)\ (\forall \alpha \in F)\ (x+y) \in W \wedge (\alpha x \in W)$.

Dokaz: Neka je W podprostor prostora V. Kako je W vekt. prostor $\Rightarrow (W,+)$ je Abelova grupa pa je $x+y \in W$ za $\forall x,y \in W$ zbog osobine zatvorenosti.

Množenje vektora skalarom je uvedeno po definiciji vektorskog prostora pa je $(\forall x \in W)(\forall \alpha \in F)$ $\alpha x \in W$.

$(\Leftarrow)$ $W \neq \emptyset$ i vrijedi $(\forall x,y \in W)(\forall \alpha \in F)\ (x+y) \in W \wedge (\alpha x \in W)$

Treba dokazati da je W vektorski prostor.

$W \subseteq V$ pa naslijeđuje osobine asocijativnosti i komutativnosti; $(\forall x,y \in W)\ (x+y) \in W \rightarrow$ zatvoren;

$\alpha x \in W$ za $(\forall x \in W) \wedge (\forall \alpha \in F) \Rightarrow$ specijalno za $\alpha = 0$

$0 \cdot x = 0 \rightarrow$ neutralni element; za $\alpha = -1$ $-1 \cdot x = -x$

$\Rightarrow \alpha = -1$ inverzni element $\Rightarrow (W,+)$ Abelova grupa

tj. vrijedi: $(V1)$ $(W,+)$ Abelova grupa;

$(V2)$ $\alpha \cdot (a+b) = \alpha a + \alpha b$

$(V3)$ $(\alpha + \beta) a = \alpha a + \beta a$

$(V4)$ $\alpha \cdot (\beta \cdot a) = (\alpha \cdot \beta) a$

$(V5)$ $1 \cdot a = a$

vrijede u W jer su naslijeđene iz V jer je $W \subseteq V$.

T_6: (Poopštenje T_5)

Podskup W vektorskog prostora V nad poljem F je podprostor prostora V akko je W neprazan podskup od V i vrijedi: $(\forall x, y \in W)(\forall \alpha, \beta \in F)\ (\alpha x + \beta y \in W)$.

T_7: Ako je V vektorski prostor nad poljem F i $(a_1, \dots, a_m) \in V^m$ m-torka vektora, tada je lineal $L(a_1, \dots a_m)$ podprostor prostora V.

Dokaz: Neka su $x, y \in L(a_1, \dots, a_m)$ - linearne kombinacije m-torke vektora $\Rightarrow$ $x = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_m a_m$, $\alpha_i \in F$

$y = \beta_1 a_1 + \beta_2 a_2 + \dots + \beta_m a_m$, $\beta_i \in F$

$x + y = (\alpha_1 + \beta_1) a_1 + (\alpha_2 + \beta_2) a_2 + \dots + (\alpha_m + \beta_m) a_m = \sum_{i=1}^{m} (\alpha_i + \beta_i) a_i$

Kako je $\alpha_i \in F$ i $\beta_i \in F$ $\Rightarrow$ $\alpha_i + \beta_i \in F$ $\Rightarrow$ $\underline{x + y \in L}$

$\alpha \cdot x = \alpha\alpha_1 a_1 + \alpha\alpha_2 a_2 + \alpha\alpha_3 a_3 + \dots + \alpha\alpha_m a_m = \sum_{i=1}^{m} (\alpha\alpha_i) a_i$

Kako $\alpha \in F$ i $\alpha_i \in F$ $\Rightarrow$ $\alpha \cdot \alpha_i \in F$ $\Rightarrow$ $\underline{\alpha \cdot x \in L}$.

T_8: Proizvoljna m-torka vektora $(a_1, \dots, a_m)$ je linearno zavisna akko se barem jedan od vektora $a_1, \dots, a_m$ može napisati u obliku linearne kombinacije preostalih vektora.

Dokaz: $(\Rightarrow)$ Pretpostavimo da je $(a_1, \dots, a_m)$ lin. zavisna. Tada postoji $\alpha_i \in F$ $\alpha_i \neq 0$ tako da vrijedi:

$\alpha_1 a_1 + \dots + \alpha_i a_i + \dots + \alpha_m a_m = 0$. Kako je F polje to postoji inverzni element α_i^{-1} pa slijedi:

$a_i = -\alpha_i^{-1} (\alpha_1 a_1 + \dots + \alpha_{i-1} a_{i-1} + \alpha_{i+1} a_{i+1} + \dots + \alpha_m a_m)$

tj. a_i je lin. kombinacija vektora $a_1, \dots a_{i-1}, a_{i+1}, \dots a_m$ $(1 < i < m$; analogno za $i = 1, i = m)$

$(\Leftarrow)$ $a_i = \beta_1 a_1 + \dots + \beta_i a_i + \beta_{i+1} a_{i+1} + \dots + \beta_m a_m$ $\rightarrow$ a_i je lin.

kombinacija vektora $a_1 \dots a_i \ a_m$ ...

$\Rightarrow a_i - \beta_1 a_1 + \ldots - \beta_m a_m = 0$

Koeficijent uz a_i je različit od nule $\Rightarrow$ n-torka je linearno zavisna.