

Posten polinoma.

Neka je F polje. Bestovajemo niz $(a_0, a_1, a_2, \dots)$ elemenata iz polja F od kojih je najviše konačno mnogo različit od nule nazivamo polinomom nad poljem F ili polinomom sa koeficijentima iz polja F . a_i - koeficijenti polinoma. Ako je $a_n \neq 0$, $a_m = 0$, $\forall m > n$ onda je n stepen gorejeg polinoma. Tada, pišemo, $P = (a_0, a_1, a_2, \dots, a_n)$ i kažemo da je $\deg P = n$ ($\text{st } P = n$). a_n - vodeći koeficijent. Ako je $a_n = 1$, onda je polinom prvostepeni.

Koeficijent a_0 je slobodni član. $P = (a_0, a_1, \dots, 0)$ $a_0 \in F$ suvremeni konstantni polinom. Njegov stepen je 0. Ako je i $a_0 = 0$ onda je polinom $(a_1, a_2, \dots, 0)$ nula polinom. (Njegov stepen je po definiciji $-\infty$). Polinom stepena 1 je linearni polinom. Označimo sa $[F[x]]$ skup svih polinoma nad poljem F .

Na ovom skupu se definišu binarne operacije $+$ i $\cdot$ na sledeći način:

$$P + Q = (a_0, a_1, \dots, a_n) + (b_0, b_1, \dots, b_m), \quad n < m, = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, b_{n+1}, \dots, b_m)$$

$$P \cdot Q = (c_0, c_1, \dots, c_r), \text{ gde je } c_k = \sum_{j=0}^k a_j b_{k-j}$$

Teorema Ako su P i Q nenula polinomi nad poljem F onda je $P \cdot Q = (c_0, c_1, \dots, c_r)$, gde je $c_r = c_{n+m} = a_n \cdot b_m$.

Dokaz. $C_{n+w} = \sum_{j=0}^{n+w} a_j b_{n+w-j}$. Za $j=0, 1, \dots, n-1$ znamo da je $n+w-j > w$, $b_{n+w-j} = 0$. Za $j=n, \dots, n+w$: $a_j = 0$. Jedini preostali $\neq 0$ se dobija za $j=n$: $C_{n+w} = a_n \cdot b_w \neq 0$, jer su a_n i $b_w \in F$, $a_n \neq 0$, $b_w \neq 0$ pa je i njihov proizvod $\neq 0$ jer u polju F nema dijeljaca nula.

Primijemo da je $a_i = 0$, $i > n+w$

Posljedica. Ako su P i Q nenula polinomi nad poljem F onda je:

a) $P \cdot Q \neq 0$

b) $\deg(P \cdot Q) = \deg P + \deg Q$.

Na sledeći način se definiše polinomi nad prstenom R :

Polinomi $(0, 1)$ nad nenula prstenom R su jedinice, označimo sa: $(0, 1) = 1$. Tada važi sledeća teorema:

Teorema Svaki polinom $P = (a_0, a_1, \dots, a_n)$ nad prstenom R sa jedinicom se može zapisati u obliku $(a_0, a_1, \dots, a_n) = a_0 + a_1 t + \dots + a_n t^n$

Dokaz. (*) +

Teorema. $(R[t], +, \cdot)$ je integralni domeni (komutativni asocijativni prsten sa 1 bez delitelja nule).

Dokaz. sami.

Primijemo da važi sledeće:

Teorema. a) Ako je R prsten sa jedinicom, onda je i $R[t]$ prsten sa 1.

b) Ako je R komutativan prsten sa 1, onda je i $R[t]$ takav.

c) Ako je R integralni domeni, onda je i $R[t]$ integralni domeni.

Au, ni za kakav prsten R sa 1 $R[t]$ nije polje. (pa čak kad je $R=F$)

Teorema (o dijeljenju polinoma). Za svaka dva polinoma S i T ($T \neq 0$) $\exists$ jedinstveni polinomi Q i R takvi da je $S = Q \cdot T + R$, $R = 0$ ili $\deg R < \deg T$.
↓ ↓
kvan ostatak

Dokaz (**) +

- 2 -

2*) Kako je $(a_0, a_1)(b_0, b_1) =$
 $= (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0)$

mo je:

$$(0, 1)^2 = (0, 1)(0, 1) = (0, 0, 1), \text{ jer } a_0 = b_0 = a_2 = b_2 = 0, a_1 = b_1 = 1.$$

Analognom se lahko pokaže da je

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

Za $k=2$, T. je pokazano.

Pretpostavimo da je tako za k in

okažemo da je tako za $k+1$. Ako je

$$(0, 1) = (a_0, a_1), \quad (\underbrace{0, 0, \dots, 0}_{k+1}, 1) = (b_0, b_1, \dots, b_k) \text{ in}$$

$$(\underbrace{0, 0, \dots, 0}_{k+2}, 1) = (\underbrace{c_0, c_1, \dots, c_{k+1}}_{k+1}), \text{ to je}$$

$$(0, 1)^{k+1} = (0, 1)(0, 1)^k = (0, 1)(\underbrace{0, 0, \dots, 0}_{k+1}, 1) = (\underbrace{0, 0, \dots, 0}_{k+2}, 1)$$

$$\text{jer je } c_{k+1} = a_1 b_k = 1 \cdot 1 = 1,$$

$$\text{a za } i < k+1 \text{ je } c_i = \sum_{j=0}^i a_j b_{i-j} = 0,$$

$$\text{jer je: } b_0 = b_1 = \dots = b_{k-1} = 0 \text{ in } a_0 = 0.$$

Dakle je očitno, jer za $a_i \neq 0$ je

$$a_i (0, 0, \dots, 1) = (0, 0, \dots, a_i) \text{ in}$$

$$0 \cdot (0, 0, \dots, 1) = 0.$$

2.**) Ako je $S=0$, tada je $-QT=R \Rightarrow Q=0$ u $R=0$,
jer da u protivnom imamo da je antena u osnovu
na desnoj strani jednaka $-QT=R$ kao i na
of antena u osnovu na levoj strani.

Ako je $S \neq 0$ u $\deg(S) < \deg(T)$, tada je $Q=0$
u $S=R$, jer da u protivnom imamo u osnovu
različite antene na desnoj i levoj strani
jednaka $S=QT+R$.

- Ako je $S \neq 0$ u $\deg(S) \geq \deg(T)$, tada ;

$$S = a_0 + a_1 t + \dots + a_n t^n, \quad T = b_0 + b_1 t + \dots + b_m t^m$$

Def. celi koeficijenti uz osnovu

$$S_1, S_2, \dots, S_k$$

koji su koeficijenti u pol. oznaci sa S_i ,
u sledećem nizu:

$$S_1 = S - a_n b_m^{-1} t^{n-m} T$$

$$S_2 = S_1 - s_1 b_m^{-1} t^{\deg(S_1)-m} T$$

$\vdots$

$$S_k = S_{k-1} - s_{k-1} b_m^{-1} t^{\deg(S_{k-1})-m} T$$

Je li k najmanji grup. broj za koji je $S_k=0$ u $\deg(S_k) < \deg(T)$. Dokazujemo da takav
broj k postoji. Ako je $S_k=0$, za neki grup. broj
 k , onda je jedan odob. u osnovu,
 $\deg(S) > \deg(S_1)$. Na isti način:

$\deg(S_1) > \deg(S_2) > \deg(S_3) > \dots$, što znači
da postoji takav grup. broj k za koji je
 $\deg(S_k) < \deg(T)$. Zamenom S_1 uz Q u
grup. jednaka, $S_2, \dots, S_{k-1}$, u R uz R
-vost, celom je $S=QT+R$, je li $R=S_k$

- 2¹¹¹

$$Q = a_n b_n^{-1} t^{u-m} + s_1 b_n^{-1} t^{\deg(S_1)-m} + \dots + s_{k-1} b_n^{-1} t^{\deg(S_{k-1})-m}$$

Ali ako su neposredno komparirane Q i R koji zasto-
-bovaju yeno de T. to otkriva da su komparirane
Q₁ i R₁ koji zasto-bovaju yeno de T, to otkriva
da su komparirane;

$$S = QT + R \quad \wedge \quad S = Q_1 T + R_1$$

$$\Rightarrow -(Q - Q_1)T = R - R_1 \leftarrow$$

$$\Rightarrow R - R_1 = 0 \quad \wedge \quad Q - Q_1 = 0,$$

jer su u istom yeno de y jeno de
da se je otkriva komparirane na reboj strani
betu of otkriva komparirane na fleboj strani