Dodatek D

Osnovni izrek algebre

Naj bo x spremenljivka in $\mathcal{O}$ komutativen obseg. *Polinom* je linearna kombinacija potenc $x^0 = 1, x, x^2, \ldots$ spremenljivke x:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

s koeficienti $a_n, a_{n-1}, \ldots, a_1, a_0$ iz obsega $\mathcal{O}$.

Množico vseh polinomov s koeficienti v $\mathcal{O}$ označimo z $\mathcal{O}[x]$. V poglavju V smo izvedeli, da je $\mathcal{O}[x]$ komutativen kolobar z enoto.

Polinom p določa preslikavo $p : \mathcal{O} \to \mathcal{O}$ in sicer se $\alpha \in \mathcal{O}$ preslika v $p(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$. V splošnem polinomov ne moremo enačiti s polinomskimi preslikavami:

Zgled D.1 Vzemimo $\mathcal{O} = \mathbb{Z}_3$ in polinoma $p(x) = x + 1$ ter $q(x) = x^3 + 1$. V $\mathbb{Z}_3[x]$ sta p in q različna polinoma. Obseg $\mathbb{Z}_3$ ima tri elemente $0, 1, 2$. Zanje velja $p(0) = 1 = q(0)$, $p(1) = 2 = q(1)$ in $p(2) = 0 = q(2)$. Zato p in q določata isto polinomsko preslikavo.

Če je $\mathcal{O}$ neskončen obseg, npr. $\mathcal{O} = \mathbb{Q}, \mathbb{R}$ ali $\mathbb{C}$, potem različni polinomi določajo različne preslikave. $\square$

Definicija D.2 Naj bo $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $a_n \neq 0$. Potem rečemo, da je n *stopnja* polinoma p. Označimo jo z $\operatorname{st} p$. Dogovorimo se, da je stopnja polinoma 0 enaka -1. $\Diamond$

Zgled D.3 Velja $\operatorname{st}(x^3 + 1) = 3$, $\operatorname{st}(x + 1) = 1$, $\operatorname{st}(5) = 0$ in $\operatorname{st}(0) = -1$. $\square$

Definicija D.4 Element $\alpha \in \mathcal{O}$ imenujemo *ničla* polinoma p, če je $p(\alpha) = 0$. $\Diamond$

Trditev D.5 *Naj bo p polinom stopnje vsaj 1 in $\alpha \in \mathcal{O}$ ničla polinoma p. Potem obstaja tak polinom $q \in \mathcal{O}[x]$, da je $p(x) = (x - \alpha)q(x)$.*

Dokaz Polinom p delimo s polinomom $(x-\alpha)$. Potem je $p(x) = q(x)(x-\alpha)+c$, kjer je c ostanek, ki je polinom stopnje manj od 1. Za x vstavimo α in dobimo

$$0 = p(\alpha) = q(\alpha) \cdot 0 + c = c\,.$$

Zato je $c = 0$ in je $p(x) = (x - \alpha)q(x)$. ■

Ali ima vsak polinom kako ničlo? Nasploh to ne drži.

Zgled D.6 Če vzamemo $\mathcal{O} = \mathbb{R}$, potem polinom $x^2 + 1$ nima ničle, saj za nobeno realno število r ne velja $r^2 = -1$. □

Nad obsegom kompleksnih števil $\mathbb{C}$, pa ni težav z obstojem ničel, kar nam pove naslednji izrek.

Izrek D.7 (*osnovni izrek algebre*) *Vsak polinom $p \in \mathbb{C}[x]$ stopnje vsaj 1 ima ničlo.*

Dokaz tega izreka je prezahteven in ga tu ne bomo navedli.

Definicija D.8 Število $\alpha \in \mathcal{O}$ je *k-kratna* ($k \geq 1$) *ničla* polinoma $p \in \mathcal{O}[x]$, če polinom $(x - \alpha)^k$ deli p, polinom $(x - \alpha)^{k+1}$ pa ne deli p. Rečemo, da je k *večkratnost* ničle α. ◊

Posledica D.9 *Polinom $p(x) \in \mathbb{C}[x]$ stopnje n (≥ 1) ima n ničel (štetih z večkratnostjo).*

Dokaz Naj bo $n = \operatorname{st} p$. Po osnovnem izreku algebre ima p ničlo α_1. Po trditvi D.5 je potem $p(x) = (x - \alpha_1)q_1(x)$. Pri tem je $\operatorname{st} q_1 = n - 1$. Če je $n - 1 \geq 1$, potem ima q_1 ničlo α_2 in velja $q_1(x) = (x - \alpha_2)q_2(x)$ in $p(x) = (x - \alpha_1)(x - \alpha_2)q_2(x)$. Postopek nadaljujemo, dokler ne dobimo

$$p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)q_n(x)\,,$$

kjer je $\operatorname{st} q_n = 0$. Vidimo, da ima p ničle $\alpha_1, \alpha_2, \ldots, \alpha_n$, od katerih so lahko nekatere večkratne. ■