

Πολυώνυμα μιάς μεταβλητής

Πολυώνυμο βαθμού $N-1$: $a_0 + a_1 x + \dots + a_{N-1} x^{N-1}$, $a_j \in \mathbb{C}$, $a_{N-1} \neq 0$

$\mathbb{C}[x]$: το σύνολο των πολυωνύμων μιάς μεταβλητής x με συντελεστές στο $\mathbb{C}$

Πράξεις πολυωνύμων

$$s1 = \sum_{0 \leq j \leq N-1} a_j x^j$$

$$s2 = \sum_{0 \leq j \leq N-1} b_j x^j$$

$$s1 + s2 = \sum_{0 \leq j \leq N-1} (a_j + b_j) x^j$$

$$-s1 = \sum_{0 \leq j \leq N-1} (-a_j) x^j$$

$$\alpha \cdot s1 = \sum_{0 \leq j \leq N-1} (\alpha a_j) x^j , \quad \alpha \in \mathbb{C}$$

Η αλγεβρική δομή $(\mathbb{C}[x], +, -, 0)$ είναι **αβελιανή ομάδα**

Η αλγεβρική δομή $(\mathbb{C}[x], +, -, 0, \cdot)$, με βαθμωτά στο $\mathbb{C}$, είναι **διανυσματικός χώρος**

Άσκηση 1

Αποδείξτε ότι τα μονώνυμα x^K , $0 \leq K$, αποτελούν **βάση** του διανυσματικού χώρου $(\mathbb{C}[x], +, -, 0, \cdot)$.

Επιβεβαιώστε ότι τα πολυώνυμα βαθμού *το πολύ* $N-1$ αποτελούν **υπο-χώρο διάστασης** N .

Είναι σωστό ότι: τα πολυώνυμα βαθμού $N-1$ αποτελούν **υπο-χώρο διάστασης** N ;

Γινόμενο πολυωνύμων

$$s1 = \sum_{0 \leq j \leq N-1} a_j x^j$$

$$s2 = \sum_{0 \leq j \leq N-1} b_j x^j$$

$$s1 \circ s2 = \sum_{0 \leq K \leq 2N-2} \left(\sum_{0 \leq j \leq K} a_j b_{K-j} \right) x^K$$

Διαίρεση πολυωνύμων

Το υπόλοιπο της διαίρεσης ενός πολυωνύμου $m(x)$ με ένα πολώνυμο $d(x)$ βαθμού N , είναι το μοναδικό πολώνυμο $v(x)$ βαθμού το πολύ $N-1$, για το οποίο $m(x) = q(x) \circ d(x) + v(x)$.

Το υπόλοιπο της διαίρεσης του $m(x)$ με το $d(x)$ συμβολίζεται: $m(x) \bmod d(x)$.

Ορισμός $m1(x) = m2(x) \bmod d(x)$ όταν
 $m1(x) \bmod d(x) = m2(x) \bmod d(x)$.

Πράξεις πολυωνύμων $\bmod d(x)$

Ισχύουν οι ισότητες

$$(s1 + s2) \bmod d(x) = s1 \bmod d(x) + s2 \bmod d(x)$$

$$(-s) \bmod d(x) = -(s \bmod d(x))$$

$$(\alpha \cdot s) \bmod d(x) = \alpha \cdot (s \bmod d(x))$$

$$(s1 \circ s2) \bmod d(x) = [s1 \bmod d(x) \circ s2 \bmod d(x)] \bmod d(x)$$

Άσκηση 2 Ελέγξτε ότι ισχύει η ισότητα

$$(s1 \circ s2 \bmod d(x)) = [s1 \bmod d(x) \circ s2 \bmod d(x)] \bmod d(x)$$

Άλγεβρα πολυωνύμων μίας μεταβλητής mod $d(x)$

Έστω $d(x)$ ένα πολυώνυμο βαθμού N .

$C[x] / \langle d(x) \rangle$: το σύνολο των πολυωνύμων στο $C[x]$, βαθμού $\leq N-1$.

Άσκηση 3 Ελέγξτε ότι:

Η δομή $(C[x] / \langle d(x) \rangle, + \text{ mod } d(x), - \text{ mod } d(x), 0, \cdot \text{ mod } d(x))$

είναι *διανυσματικός χώρος*, και τα μονώνυμα x^K , $0 \leq K \leq N-1$,

αποτελούν *βάση* αυτού του χώρου.

Άσκηση 4 Ελέγξτε ότι:

Η δομή $(C[x] / \langle d(x) \rangle, + \text{ mod } d(x), - \text{ mod } d(x), 0, \circ \text{ mod } d(x)), 1)$

είναι *αντιμεταθετικός δακτύλιος*.

Περιγραφή σημάτων και φίλτρων μέσω πολωνύμων

Ένα σήμα διακριτού χρόνου $s : \mathbb{Z}_N \rightarrow \mathbb{C}$ μπορεί να περιγραφεί με ένα πολυώνυμο $\Pi(s)$, όπου: $\Pi(s)(x) = s(0) + s(1)x + \dots + s(N-1)x^{N-1}$.

Το πολυώνυμο $\Pi(s)$ είναι ένα στοιχείο του διανυσματικού χώρου

$$(\mathbb{C}[x] / \langle x^N - 1 \rangle, + \bmod x^N - 1, - \bmod x^N - 1, \mathbf{0}, \cdot \bmod x^N - 1).$$

Ισχύουν οι ιδιότητες

$$\Pi(s_1 + s_2) = \Pi(s_1) + \Pi(s_2)$$

$$\Pi(-s) = -\Pi(s)$$

$$\Pi(\alpha \cdot s) = \alpha \cdot \Pi(s), \quad \alpha \in \mathbb{C}$$

Κυκλική συνέλιξη των σημάτων s, h λέγεται το σήμα $s * h$, όπου :

$$(s * h)(j) = \sum_{0 \leq k \leq N-1} s(k) h(j-k \bmod N), \quad 0 \leq j \leq N-1.$$

Λήμμα

Ισχύει η ιδιότητα $\Pi(s * h) = \Pi(s) \circ \Pi(h) \bmod x^N - 1$.

Πόρισμα του Λήμματος

Έστω A ένας τελεστής που είναι γραμμικός και αναλλοίωτος ως προς κυκλικές ολισθήσεις: $A(s) = s * A(P_0)$, και από το Λήμμα

$$\Pi(A(s)) = \Pi(s) \circ \Pi(A(P_0)) \bmod x^N - 1.$$

Έστω h ένα στοιχείο του *αντιμεταθετικού δακτύλιου*

$$(\mathbb{C}[x] / \langle x^N - 1 \rangle, + \bmod x^N - 1, - \bmod x^N - 1, \mathbf{0}, \circ \bmod x^N - 1, \mathbf{1}).$$

Ορισμός: το h περιγράφει το γραμμικό φίλτρο $\varphi(h) : \mathbb{C}^N \rightarrow \mathbb{C}^N$,

$$\text{όπου} \quad \Pi(\varphi(h)(s)) = \Pi(s) \circ h \bmod x^N - 1.$$

Άσκηση 5 Έστω ότι h είναι το μονώνυμο x^K , $0 \leq K \leq N-1$.

Ελέγξτε ότι το $\varphi(h)$ είναι ο τελεστής κυκλικής ολίσθησης Tr_K .

Άσκηση 6 Επιβεβαιώστε ότι, για κάθε h , το φίλτρο $\varphi(h)$ είναι γραμμικό και αναλλοίωτο ως προς κυκλικές ολισθήσεις.

Άσκηση 7

α Έστω $h = h_0 + h_1 x + \dots + h_{N-1} x^{N-1}$, και $\varphi(h)(P_0)$ η κρουστική απόκριση του φίλτρου $\varphi(h)$: ελέγξτε ότι $\varphi(h)(P_0)(j) = h_j$, $0 \leq j \leq N-1$.

β Έστω A ένα φίλτρο γραμμικό και αναλλοίωτο ως προς κυκλικές ολισθήσεις. Έστω $A(P_0)$ η κρουστική απόκριση του A , και $A(P_0)(j) = h_j$, $0 \leq j \leq N-1$.

Θέτουμε $h = h_0 + h_1 x + \dots + h_{N-1} x^{N-1}$: Ελέγξτε ότι $\varphi(h) = A$.

Άσκηση 8 Ελέγξτε ότι $\varphi(h_1 \circ h_2) = \varphi(h_1) \circ \varphi(h_2)$

Η πράξη $h_1 \circ h_2$ είναι γινόμενο πολυωνύμων, και η πράξη $\varphi(h_1) \circ \varphi(h_2)$ είναι σύνθεση των τελεστών $\varphi(h_1)$, $\varphi(h_2)$.

Απόδειξη του Λήμματος

Ο συντελεστής του όρου βαθμού j του πολωνύμου $\Pi(s * h)$ είναι $\sum_{0 \leq K \leq N-1} s(K) h(j-K \bmod N)$, $0 \leq j \leq N-1$.

Ο συντελεστής του όρου βαθμού l του πολωνύμου $\Pi(s) \circ \Pi(h)$ είναι $\sum_{0 \leq K \leq l} s(K) h(l-K)$, $0 \leq l \leq 2N-2$
(θέτουμε $s(K) = 0$ όταν $K \geq N$, $h(l-K) = 0$ όταν $l-K \geq N$).

Ο συντελεστής του όρου βαθμού j του $\Pi(s) \circ \Pi(h) \bmod x^N - 1$, όπου $0 \leq j \leq N-1$, θα είναι το άθροισμα των όρων βαθμών j και $j+N$ του πολωνύμου $\Pi(s) \circ \Pi(h)$: επομένως, θα είναι το άθροισμα των

$$\sum_{0 \leq K \leq j} s(K) h(j-K) \quad \text{και} \quad \sum_{0 \leq K \leq j+N} s(K) h(j+N-K).$$

Επειδή στο δεύτερο άθροισμα πρέπει $j+N-K \leq N-1$, θα έχουμε $j+1 \leq K$, και το συνολικό άθροισμα θα είναι

$$\sum_{0 \leq K \leq j} s(K) h(j-K) + \sum_{j+1 \leq K \leq N-1} s(K) h(j+N-K),$$

και τελικά
$$\sum_{0 \leq K \leq N-1} s(K) h(j-K \bmod N).$$