Πολυώνυμα μιάς μεταβλητής

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

$C[x]$: το *σύνολο* των πολυωνύμων μιάς μεταβλητής x με συντελεστές στο C

Πράξεις πολυωνύμων

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

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

$s1 + s2$	$\sum_{0 \le j \le N-1} (a_j + b_j) x^j$
$-s1$	$\sum_{0 \le j \le N-1} (-a_j) x^j$
$\alpha \bullet s1$	$\sum_{0 \le j \le N-1} (\alpha a_j) x^j$, $\alpha \in C$

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

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

Άσκηση 1

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

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

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

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

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

Η *αλγεβρική δομή* $(C[x] , + , - , \mathbf{0} , \circ , \mathbf{1})$ είναι **αντιμεταθετικός δακτύλιος**:

1 Με τις πράξεις $+ , - , \mathbf{0}$ είναι αβελιανή ομάδα

2 Ισχύουν οι ισότητες

$$(A1 \circ A2) \circ A = A1 \circ (A2 \circ A)$$

$$A \circ \mathbf{1} = \mathbf{1} \circ A = A$$

$$A \circ (A1 + A2) = (A \circ A1) + (A \circ A2)$$

$$(A1 + A2) \circ A = (A1 \circ A) + (A2 \circ A)$$

3 Ισχύει η ισότητα

$$A1 \circ A2 = A2 \circ A1$$

Παραδείγματα δακτυλίων

Οι γραμμικοί τελεστές, $A: C^N \to C^N$, με τις πράξεις $+ , - , \mathbf{0} , \circ , \mathbf{1}$

Τα μητρώα διαστάσεων $N \times N$, με τις πράξεις $+ , - , \mathbf{0}$, πολ/σμός, $\mathbf{I_N}$

Παραδείγματα αντιμεταθετικών δακτυλίων

R , C , Z ως προς *πρόσθεση* και *πολλαπλασιασμό*

Τα πολυώνυμα με συντελεστές στο R είτε C είτε Z,
ως προς *πρόσθεση* και *πολλαπλασιασμό*

Οι γραμμικοί τελεστές που είναι αναλλοίωτοι ως προς κυκλικές ολισθήσεις

Τα κυκλικά μητρώα διαστάσεων $N \times N$

Τα σήματα $s : Z \to C^N$, με τις πράξεις $+ , - , \mathbf{0}$, *κυκλική συνέλιξη*, $\mathbf{P_0}$

Διαίρεση πολυωνύμων

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

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

Συμβολίζουμε με $m1(x) = m2(x) \bmod d(x)$ ότι : $(m1(x)-m2(x)) \bmod d(x) = 0$.

Πράξεις πολυωνύμων $\bmod d(x)$

Ισχύουν οι ισότητες

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

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

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

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

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 μιάς μεταβλητής **mod d(x)**

Έστω $d(x)$ ένα πολυώνυμο βαθμού N.

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

Άσκηση 3 Ελέγξτε ότι:

Η αλγεβρική δομή $(C[x] / < d(x) > , + \bmod d(x) , - \bmod d(x) , \mathbf{0} , \bullet \bmod d(x))$ είναι *διανυσματικός χώρος*.

Τα μονώνυμα x^K, $0 \leq K \leq N-1$, αποτελούν *βάση* αυτού του χώρου.

Άσκηση 4 Επιβεβαιώστε ότι:

Η δομή $(C[x] / < d(x) > , + \bmod d(x) , - \bmod d(x) , \mathbf{0} , \circ \bmod d(x)) , \mathbf{1})$ είναι *αντιμεταθετικός δακτύλιος*.

Μέγιστος κοινός διαιρέτης πολυωνύμων

Το πολυώνυμο $d(x)$ είναι ΜΚΔ των πολυωνύμων $d_1(x)$, $d_2(x)$ άν:
το $d(x)$ *διαιρεί* τα $d_1(x)$, $d_2(x)$ και έχει τον *ελάχιστο δυνατό βαθμό*.

Ταυτότητα για τον ΜΚΔ πολυωνύμων

Άν το πολυώνυμο $d(x)$ είναι ΜΚΔ των πολυωνύμων $d_1(x)$, $d_2(x)$:
θα υπάρχουν πολυώνυμα $A(x)$, $B(x)$ ώστε $d(x) = A(x) \circ d_1(x) + B(x) \circ d_2(x)$.

Ιδιότητα πολυωνύμων πρώτων μεταξύ τους ανά δύο

Εστω πολυώνυμα $d_K(x)$, $0 \le K \le N-1$, όπου: κάθε πολυώνυμο
που είναι ΜΚΔ των $d_K(x)$, $d_j(x)$, $j \ne K$, είναι σταθερά.

Εστω $P(x)$, $Q(x)$ πολυώνυμα όπου $P(x) = Q(x) \mod d_K(x)$, $0 \le K \le N-1$.
Τότε $P(x) = Q(x) \mod \prod_{0 \le K \le N-1} d_K(x)$.

***Chinese Remainder Theorem* για πολυώνυμα**

Δίνονται πολυώνυμα $d_K(x)$, $\upsilon_K(x)$, $0 \le K \le N-1$, ώστε:

Κάθε πολυώνυμο $\upsilon_K(x)$ έχει βαθμό μικρότερο από τον βαθμό του $d_K(x)$.

Κάθε πολυώνυμο που είναι ΜΚΔ των $d_K(x)$, $d_j(x)$, $j \ne K$ είναι σταθερά.

Θα υπάρχει πολυώνυμο $P(x)$ ώστε:

$$P(x) \bmod d_K(x) = \upsilon_K(x), \qquad 0 \le K \le N-1.$$

<u>*Σημείωση*</u> Από την Ιδιότητα πολυωνύμων πρώτων μεταξύ τους ανά δύο:
το πολυώνυμο $P(x) \bmod \prod_{0 \le K \le N-1} d_K(x)$ θα είναι *μοναδικό*.

ΑΠΟΔΕΙΞΗ

Θεωρούμε ένα τυχαίο K, $0 \le K \le N-1$:
Για κάθε $j \ne K$, κάθε πολυώνυμο που είναι ΜΚΔ των $d_K(x)$, $d_j(x)$ είναι σταθερά:
επομένως θα υπάρχουν πολυώνυμα $A_{j,K}(x)$, $B_{j,K}(x)$ ώστε

$$1 = A_{j,K}(x) \circ d_K(x) + B_{j,K}(x) \circ d_j(x),$$

οπότε $B_{j,K}(x) \circ d_j(x) = 1 \bmod d_K(x)$ για κάθε $j \ne K$

Θέτουμε $g_K(x) = \prod_{j \ne K} B_{j,K}(x) \circ d_j(x)$:

Από τα παραπάνω $g_K(x) = 1 \bmod d_K(x)$

$g_K(x) = 0 \bmod d_j(x)$, για κάθε $j \ne K$

Θέτουμε $P(x) = \sum_{0 \le K \le N-1} g_K(x) \circ \upsilon_K(x)$:

$$P(x) \bmod d_K(x) = \left(\sum_{0 \le K \le N-1} 1 \circ \upsilon_K(x)\right) \bmod d_K(x)$$
$$= \upsilon_K(x), \qquad 0 \le K \le N-1.$$

ΕΦΑΡΜΟΓΗ *του* ***Chinese Remainder Theorem για πολυώνυμα***

Δίνονται πολυώνυμα $r_K(x) = x-\rho_K$, $0 \le K \le N-1$, όπου $\rho_j \ne \rho_K$ για $j \ne K$.
Δίνονται και σταθερές υ_K , $0 \le K \le N-1$.

Θα υπάρχει πολυώνυμο $P(x)$ ώστε: $P(x) \mod x-\rho_K = \upsilon_K$, $0 \le K \le N-1$.
Το πολυώνυμο $P(x) \mod \prod_{0 \le K \le N-1} x-\rho_K$ θα είναι *μοναδικό*.

ΚΑΤΑΣΚΕΥΗ

Θεωρούμε ένα τυχαίο K , $0 \le K \le N-1$:
Για κάθε $j \ne K$, θέτουμε $A_{j,K}(x) = (\rho_j - \rho_K)^{-1}$ $B_{j,K}(x) = -(\rho_j - \rho_K)^{-1}$.

Θα έχουμε $1 = A_{j,K}(x)\, r_K(x) + B_{j,K}(x)\, r_j(x)$,
οπότε $B_{j,K}(x)\, r_j(x) = 1 \mod r_K(x)$ για κάθε $j \ne K$.

Θέτουμε $f_K(x) = \prod_{j \ne K} B_{j,K}(x)\, r_j(x) = \prod_{j \ne K} (\rho_K - \rho_j)^{-1} (x-\rho_j)$.

Θα έχουμε $f_K(x) = 1 \mod r_K(x)$
$f_K(x) = 0 \mod r_j(x)$, για κάθε $j \ne K$.

Θέτουμε $P(x) = \sum_{0 \le K \le N-1} \upsilon_K\, f_K(x)$.

Άσκηση 5 Εστω $D(x) = \prod_{0 \le K \le N-1} d_K(x)$, όπου για κάθε $j \neq K$, κάθε πολυώνυμο που είναι ΜΚΔ των $d_K(x)$, $d_j(x)$ είναι σταθερά.

Υποθέτουμε ότι, για τα πολυώνυμα $g_K(x)$, $0 \le K \le N-1$:

$g_K(x) = 1 \mod d_K(x)$

$g_K(x) = 0 \mod d_j(x)$, για κάθε $j \neq K$.

Αποδείξτε ότι:

α Για $0 \le K \le N-1$, $d_K(x) \circ g_K(x) = 0 \mod D(x)$

$g_K(x) \circ g_K(x) = g_K(x) \mod D(x)$

Για κάθε $j \neq K$, $g_j(x) \circ g_K(x) = 0 \mod D(x)$.

β $\sum_{0 \le j \le N-1} g_j(x) = 1 \mod D(x)$.

Απάντηση

Για το (α) : Εφαρμόζουμε την Ιδιότητα πολυωνύμων πρώτων μεταξύ τους ανά δύο, στα πολυώνυμα που αναφέρονται.

Για το (β) : Υπολογίζουμε τους όρους του πολυωνύμου $\prod_{0 \le j \le N-1} 1 - g_j(x)$, και εφαρμόζουμε το (α) .

Άσκηση 6 Εστω $m(x) = \prod_{0 \le K \le N-1} x-\rho_K$, ρ_K σταθερά, $\rho_j \neq \rho_K$ για $j \neq K$.
Έστω ένα πολυώνυμο $h(x)$.

α Ελέγξτε ότι $h(x) \mod x-\rho_K = h(\rho_K)$.

β Αποδείξτε ότι: άν $H(x) \mod x-\rho_K = h(\rho_K)$, $0 \le K \le N-1$,
θα είναι $H(x) = h(x) \mod m(x)$.

Απάντηση

Για το (β) : Εφαρμόζουμε το Chinese Remainder Theorem για πολυώνυμα $r_K(x) = x-\rho_K$ και σταθερές $\upsilon_K = h(\rho_K)$, $0 \le K \le N-1$. Προκύπτει πολυώνυμο $P(x)$ για το οποίο $P(x) \mod x-\rho_K = h(\rho_K)$, $0 \le K \le N-1$: επίσης, το υπόλοιπο $P(x) \mod m(x)$ θα είναι *μοναδικό*.
Επομένως, $P(x) \mod m(x) = H(x) \mod m(x) = h(x) \mod m(x)$.