

מבנים דיסקרטיים – תרגיל 8 – פתרון

שאלה 1

יהי R חוג חילופי עם יחידה, יהי $a \in R$ ויהי $u \in R$ הפיך. הוכיחו:

- א. $u|a$.
- ב. אם $a|u$ אז a הפיך.

הוכחה

נסמן ב- 1_R את היחידה של R .

סעיף א: $(u(u^{-1}a) = a$ כי $u|a$, לכן, $a = 1_R a = (uu^{-1})a = u(u^{-1}a)$.

סעיף ב: אם $a|u$ אז קיים $b \in R$ כך ש- $ab = u$. אם נכפול מימין ב- u^{-1} נקבל $abu^{-1} = uu^{-1} = 1_R$, כלומר $a(bu^{-1}) = 1_R$ ולכן a הפיך. (אנחנו הראינו הפיכות מימין. אין צורך לבדוק הפיכות משמאל כי R חילופי).

מש"ל.

שאלה 2

חשבו את ההופכי של 13 ב-

- א. \mathbb{Z}_{33}
- ב. \mathbb{Z}_{34}

פיתרון

סעיף א: נחפש בעזרת אלגוריתם אוקלידס $\alpha, \beta \in \mathbb{Z}$ כך ש- $13\alpha + 33\beta = 1$.

$$\begin{aligned} 33 &= 2 * 13 + 7 \rightarrow 7 = 33 - 2*13 \\ 13 &= 1 * 7 + 6 \rightarrow 6 = 13 - 7 = 13 - (33 - 2*13) = -33 + 3*13 \\ 7 &= 1 * 6 + 1 \rightarrow 1 = 7 - 6 = (33 - 2*13) - (-33 + 3*13) = 2*33 - 5*13 \\ 6 &= 6 * 1 + 0 \end{aligned}$$

לכן, $\alpha = -5, \beta = 2$. זה אומר שההופכי של 13 ב- \mathbb{Z}_{33} הוא $\alpha \bmod 33 = (-5) \bmod 33 = 28$.

סעיף ב: נחפש בעזרת אלגוריתם אוקלידס $\alpha, \beta \in \mathbb{Z}$ כך ש- $13\alpha + 34\beta = 1$.

$$\begin{aligned} 34 &= 2 * 13 + 8 \rightarrow 8 = 34 - 2*13 \\ 13 &= 1 * 8 + 5 \rightarrow 5 = 13 - 8 = 13 - (34 - 2*13) = -34 + 3*13 \\ 8 &= 1 * 5 + 3 \rightarrow 3 = 8 - 5 = (34 - 2*13) - (-34 + 3*13) = 2*34 - 5*13 \\ 5 &= 1 * 3 + 2 \rightarrow 2 = 5 - 3 = (-34 + 3*13) - (2*34 - 5*13) = -3*34 + 8*13 \\ 3 &= 1 * 2 + 1 \rightarrow 1 = 3 - 2 = (2*34 - 5*13) - (-3*34 + 8*13) = 5*34 - 13*13 \\ 2 &= 2 * 1 + 0 \end{aligned}$$

לכן, $\alpha = -13, \beta = 5$. זה אומר שההופכי של 13 ב- \mathbb{Z}_{34} הוא $\alpha \bmod 34 = (-13) \bmod 34 = 21$.

שאלה 3

- א. מצאו פולינומים $a(x), b(x) \in \mathbb{R}[x]$ כך ש-
 $a(x)(x^3 - x) + b(x)(x^4 - x^3 - x^2 + 2) = \gcd(x^3 - x, x^4 - x^3 - x^2 + 2)$
- ב. מצאו פולינומים $a(x), b(x) \in \mathbb{Z}_2[x]$ כך ש-
 $a(x)(x^4 + x + 1) + b(x)(x^4 + x^3) = \gcd(x^4 + x + 1, x^4 + x^3)$

הערה: שימו לב ש- \mathbb{Z}_2 הוא שדה וחיבור של פולינומים מעל \mathbb{Z}_2 דומה לפעולת XOR בין הפולינומים. סעיף ב הרבה יותר קל לחישוב מאשר סעיף א...]

פיתרון

סעיף א: נבצע את אלגוריתם אוקלידס (לא נפרט כאן את החילוק הארוך הנדרש בחלק מהשלבים).

$$\begin{aligned} x^4 - x^3 - x^2 + 2 &= (x-1) * (x^3 - x) + (-x+2) \\ x^3 - x &= (-x^2 - 2x - 3) * (-x+2) + 6 \\ -x+2 &= (-1/6 * x + 2/6) * 6 + 0 \end{aligned}$$

$$-x+2 = (x^4 - x^3 - x^2 + 2) - (x-1) * (x^3 - x)$$

$$\begin{aligned} 6 &= (x^3 - x) - (-x^2 - 2x - 3) * (-x+2) = \\ &= (x^3 - x) - (-x^2 - 2x - 3) * [(x^4 - x^3 - x^2 + 2) - (x-1) * (x^3 - x)] = \\ &= (x^2 + 2x + 3) * (x^4 - x^3 - x^2 + 2) + (1 + (-x^2 - 2x - 3) * (x-1)) * (x^3 - x) = \\ &= (x^2 + 2x + 3) * (x^4 - x^3 - x^2 + 2) + (-x^3 - x^2 - x + 4) * (x^3 - x) \end{aligned}$$

נחלק את המשוואה האחרונה ב-6 ונקבל:

$$\begin{aligned} 1 &= \left(\frac{1}{6}x^2 + \frac{2}{6}x + \frac{3}{6}\right)(x^4 - x^3 - x^2 + 2) + \left(-\frac{1}{6}x^3 - \frac{1}{6}x^2 - \frac{1}{6}x + \frac{4}{6}\right)(x^3 - x) \\ \text{לכן, } a(x) &= \left(-\frac{1}{6}x^3 - \frac{1}{6}x^2 - \frac{1}{6}x + \frac{2}{3}\right) \text{ ו- } b(x) = \left(\frac{1}{6}x^2 + \frac{1}{3}x + \frac{1}{2}\right) \end{aligned}$$

סעיף ב: נבצע את אלגוריתם אוקלידס (לא נפרט כאן את החילוק הארוך הנדרש בחלק מהשלבים).

$$\begin{aligned} x^4 + x + 1 &= 1 * (x^4 + x^3) + (x^3 + x + 1) \\ x^4 + x^3 &= (x+1) * (x^3 + x + 1) + (x^2 + 1) \\ x^3 + x + 1 &= x * (x^2 + 1) + 1 \\ x^2 + 1 &= (x^2 + 1) * 1 + 0 \end{aligned}$$

$$x^3 + x + 1 = (x^4 + x + 1) + (x^4 + x^3)$$

$$\begin{aligned} x^2 + 1 &= (x^4 + x^3) + (x+1) * (x^3 + x + 1) = \\ &= (x^4 + x^3) + (x+1) * ((x^4 + x + 1) + (x^4 + x^3)) = \\ &= (x+1) * (x^4 + x + 1) + x * (x^4 + x^3) \end{aligned}$$

$$\begin{aligned} 1 &= (x^3 + x + 1) + x * (x^2 + 1) = \\ &= [(x^4 + x + 1) + (x^4 + x^3)] + x * [(x+1) * (x^4 + x + 1) + x * (x^4 + x^3)] = \\ &= (1 + x * (x+1)) * (x^4 + x + 1) + (1 + x * x) * (x^4 + x^3) = \\ &= (x^2 + x + 1) * (x^4 + x + 1) + (x^2 + 1) * (x^4 + x^3) \end{aligned}$$

לכן, $a(x) = x^2 + x + 1$ ו- $b(x) = x^2 + 1$ (ה- \gcd הוא 1, כמובן).

שאלה 4

מצאו את ההופכי של $(x^2 + x + 2)$ בחוג $\mathbb{R}[x]/\langle x^3 + 1 \rangle$.

פיתרון

נחפש פולינומים $a(x), b(x) \in \mathbb{R}[x]$ כך ש- $1 = a(x)(x^2 + x + 2) + b(x)(x^3 + 1)$

$$x^3+1 = (x-1) * (x^2+x+2) + (-x+3)$$

$$x^2+x+2 = (-x-4) * (-x+3) + 14$$

$$-x+3 = (-1/14 * x + 3/14 * x) * 14 + 0$$

$$-x+3 = (x^3+1) - (x-1) * (x^2+x+2)$$

$$14 = (x^2+x+2) - (-x-4) * (-x+3) = (x^2+x+2) + (x+4) * (-x+3) =$$

$$= (x^2+x+2) + (x+4) * [(x^3+1) - (x-1) * (x^2+x+2)] =$$

$$= (- (x-1) * (x+4) + 1) * (x^2+x+2) + (x+4) * (x^3+1) =$$

$$= (-x^2-3x+5) * (x^2+x+2) + (x+4) * (x^3+1)$$

נחלק את המשוואה האחרונה ב-14 ונקבל

$$\left(-\frac{1}{14}x^2 - \frac{3}{14}x + \frac{5}{14}\right)(x^2 + x + 1) + \left(\frac{1}{14}x + \frac{4}{14}\right)(x^3 + 1) = 1$$

לכן, ההופכי של $(x^2 + x + 2)$ בחוג $\mathbb{R}[x]/\langle x^3 + 1 \rangle$ הוא

$$\left(-\frac{1}{14}x^2 - \frac{3}{14}x + \frac{5}{14}\right) \bmod (x^3 + 1) = \left(-\frac{1}{14}x^2 - \frac{3}{14}x + \frac{5}{14}\right)$$