

מבנים דיסקרטיים – תרגיל 7 – פתרון

שאלה 1

יהי $(R, +, \cdot)$ חוג עם יחידה. נסמן ב- R^* את קבוצת האיברים ההופכיים ב- R .

- הוכיחו כי (R^*, \cdot) חבורה.
- מצאו את \mathbb{Z}^* , \mathbb{R}^* ואת \mathbb{Z}_{12}^* .

פיתרון

נסמן את היחידה של R ב- 1_R .

סעיף א: נוכיח סגירות: יהיו $a, b \in R^*$. אזי $a, b \in R$ הפיכים ולכן קיימים להם הופכיים a^{-1}, b^{-1} .

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1_R a^{-1} = aa^{-1} = 1_R$$

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1_R b = b^{-1}b = 1_R$$

ולכן $b^{-1}a^{-1}$ הוא הופכי של ab ב- R , כלומר $ab \in R^*$.

אסוציאטיביות הכפל ב- R^* נובעת מאסוציאטיביות הכפל ב- R .

נוכח קיום יחידה: 1_R היא יחידה ביחס לכפל ב- R ולכן מספיק להוכיח $1_R \in R^*$.

באמת, $1_R \cdot 1_R = 1_R$ (כי יחידה) ולכן $1_R^{-1} = 1_R$ ונובע ש- $1_R \in R^*$.

נוכח קיום הופכי: יהי $a \in R^*$. אזי a הפיך ב- R עם הופכי שנסמן ב- a^{-1} . מתקיים $a^{-1}a = aa^{-1} = 1_R$

ולכן a^{-1} הפיך עם הופכי a ב- R (כלומר $(a^{-1})^{-1} = a$). בפרט, נובע ש- $a^{-1} \in R^*$ ולכן a הפיך

ב- R^* . **מש"ל.**

הערה: בחלק של הסגירות הוכחנו שבכל מונויד M , אם $a, b \in M$ הפיכים, אז ab הפיך ומתקיים

$$(ab)^{-1} = b^{-1}a^{-1}$$

סעיף ב: \mathbb{R} שדה ולכן כל איבר חוץ מ-0 הפיך, כלומר $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ (זה גם מסתדר עם המשמעות

שנתנו ל- \mathbb{R}^* כשלמדנו על חבורות).

לפי משפט שהוכחנו בשיעור, $a \in \mathbb{Z}_n$ הפיך אם $\gcd(a, n) = 1$. לכן, $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$.

[דרך ישירה יותר: קל לבדוק ש- $11^{-1} = 11$, $7^{-1} = 7$, $5^{-1} = 5$, $1^{-1} = 1$ ב- \mathbb{Z}_{12} . שאר אברי \mathbb{Z}_{12} הם מחלקי 0

(בדקו! לדוגמא: $9 \cdot 4 \equiv 0 \pmod{12}$ ולכן $9, 4 \in \mathbb{Z}_{12}$ מחלקי 0) ולכן לא יכולים להיות הפיכים (מדוע?).]

לסיום, נראה ש- $\mathbb{Z}^* = \{\pm 1\}$: באמת, $1 \cdot 1 = (-1) \cdot (-1) = 1$ ולכן $1^{-1} = 1$ ו- $(-1)^{-1} = -1$

ונובע $\{\pm 1\} \subseteq \mathbb{Z}^*$. מצד שני, יהי $n \in \mathbb{Z}^*$. אזי קיים $m \in \mathbb{Z}$ כך ש- $mn = 1$.

זה אומר ש- $|m| \cdot |n| = |1| = 1$. לא ייתכן $n = 0$ או $m = 0$ כי אז נקבל $nm = 0 \neq 1$ (בסתירה ל-

$mn = 1$). לכן $|n|, |m| \geq 1$ (כי n, m שלמים), אבל $|m| \cdot |n| = 1$ ולכן בהכרח $|m| = |n| = 1$.

לכן, $n = 1$ או $n = -1$. כלומר, $\mathbb{Z}^* \subseteq \{\pm 1\}$.

שאלה 2

יהי F שדה ויהי $f \in F[x]$, $f \neq 0$. הראו כי הפיך ב- $F[x]$ אם ורק אם $\deg f = 0$. [רמז: העזרו

בעובדה שעבור $f, g \in F[x]$ מתקיים $\deg(fg) = \deg f + \deg g$]

הוכחה

כוון א: נניח כי f הפיך. אזי קיים $g \in F[x]$ כך ש- $gf = 1$. לכן, $\deg g + \deg f = \deg gf = \deg 1 = 0$.
היות ו- $\deg f \geq 0$ ו- $\deg g \geq 0$ בהכרח מתקיים $\deg f = 0$ (אחרת נקבל $\deg g + \deg f > 0$, בסתירה למה שהראינו) וזה מה שרצינו להוכיח.

כוון ב: נניח כי $\deg f = 0$. אזי $f(x) = c \cdot x^0 = c$ עבור $0 \neq c \in F$ כלשהו. היות ו- F שדה, c הפיך. יהי $g(x) := c^{-1} \cdot x^0 = c^{-1}$. אזי $g(x)f(x) = c^{-1}c = 1$. לכן $g(x)$ הופכי של $f(x)$ ב- $F[x]$, כדרוש. (אין צורך לבדוק ש- $f(x)g(x) = 1$ כי $F[x]$ חוג חילופי). **מש"ל.**

שאלה 3

יהי R חוג חילופי עם יחידה. יהי u איבר הפיך ב- R ויהיו $a, b \in R$. הוכיחו כי $a|b$ אם ורק אם $ua|b$.
[תזכורת: $a|b$ אומר שקיים $c \in R$ כך ש- $b = ac$]

הוכחה

נסמן את היחידה של R ב- 1_R .

כוון א: נניח כי $a|b$. אזי קיים $c \in R$ כך ש- $ac = b$. לכן, $(ua)(cu^{-1}) = acuu^{-1} = ac1_R = ac = b$.
קיבלנו ש- $(ua)(cu^{-1}) = b$ ולכן $ua|b$.

כוון ב: נניח כי $ua|b$. היות ו- u הפיך אז גם u^{-1} הפיך (ההופכי שלו הוא u . בדקו!). לכן, לפי כוון א, נובע ש- $b | (ua)u^{-1}$. אבל $u^{-1}(ua) = (u^{-1}u)a = 1_R a = a$ ולכן $a|b$. **מש"ל.**

שאלה 4

יהי R חוג חילופי עם יחידה וללא מחלקי 0 (כלומר, $ab = 0$ גורר $a = 0$ או $b = 0$).

א. יהיו $a, b, c \in R$. הראו כי אם $ab = ac$ ו- $a \neq 0$ אז $b = c$.
ב. יהיו $a, b \in R$. הראו כי $a|b$ וגם $b|a$ אם ורק אם קיים $u \in R$ הפיך כך ש- $a = ub$.

הוכחה

נסמן את היחידה של R ב- 1_R .

סעיף א: נתון כי $ab = ac$. אזי $a(b - c) = ab - ac = 0$. היות ו- R אין מחלקי 0 זה אומר ש- $a = 0$ או $b - c = 0$. אבל נתון ש- $a \neq 0$ ולכן בהכרח $b - c = 0$, כלומר $b = c$. **מש"ל.**

סעיף ב: היות ו- $a|b$ קיים $v \in R$ כך ש- $av = b$. היות ו- $b|a$ קיים $u \in R$ כך ש- $bu = a$. לכן:
 $a1_R = a(vu) = (av)u = buu = a1_R$, כלומר קיבלנו $a1_R = a(vu)$.
אם $a \neq 0$ אז לפי סעיף א נובע ש- $uv = 1_R$ ולכן u הפיך (אין צורך לבדוק ש- $vu = 1_R$ כי R חילופי).
היות ו- $a = bu = ub$ אז גמרנו.
אם $a = 0$, אז $b = au = 0u = 0$ ולכן $b = 0 = 1_R a = 1_R 0$. היות ו- 1_R הפיך, גמרנו.
מש"ל.

שאלה 5

- א. חשבו את $\gcd(54,33)$ ומצאו מספרים שלמים $\alpha, \beta \in \mathbb{Z}$ כך ש- $54\alpha + 33\beta = \gcd(54,33)$.
ב. חשבו את $\gcd(68,57)$ ומצאו מספרים שלמים $\alpha, \beta \in \mathbb{Z}$ כך ש- $68\alpha + 57\beta = \gcd(68,57)$.

פיתרון

בעזרת אלגוריתם אוקלידס:

סעיף א:

$$\begin{aligned} 54 &= 1 * 33 + 21 \rightarrow 21 = 54 - 33 \\ 33 &= 1 * 21 + 12 \rightarrow 12 = 33 - 21 = 33 - (54 - 33) = -54 + 2 * 33 \\ 21 &= 1 * 12 + 9 \rightarrow 9 = 21 - 12 = (54 - 33) - (-54 + 2 * 33) = 2 * 54 - 3 * 33 \\ 12 &= 1 * 9 + 3 \rightarrow 3 = 12 - 9 = (-54 + 2 * 33) - (2 * 54 - 3 * 33) = -3 * 54 + 5 * 33 \\ 9 &= 3 * 3 + 0 \end{aligned}$$

לכן, $\gcd(54,33) = 3$ ו- $3 = (-3) \cdot 54 + 5 \cdot 33$

סעיף ב:

$$\begin{aligned} 68 &= 1 * 57 + 11 \rightarrow 11 = 68 - 57 \\ 57 &= 5 * 11 + 2 \rightarrow 2 = 57 - 5 * 11 = 57 - 5 * (68 - 57) = -5 * 68 + 6 * 57 \\ 11 &= 5 * 2 + 1 \rightarrow 1 = 11 - 5 * 2 = (68 - 57) - 5 * (-5 * 68 + 6 * 57) = \\ 2 &= 2 * 1 + 0 \quad \quad \quad = 26 * 68 - 31 * 57 \end{aligned}$$

לכן, $\gcd(68,57) = 1$ ו- $1 = 26 \cdot 68 - 31 \cdot 57$

שאלה 6

מצאו פולינומים $q(x), r(x) \in \mathbb{R}[x]$ כך ש- $x^4 + x = q(x)(x^2 + 2x - 2) + r(x)$ ו- $\deg r(x) < 2$.

פיתרון

נבצע חילוק ארוך של פולינומים:

$$\begin{array}{r} x^2 - 2x + 6 \\ \hline x^4 + 2x^3 - 2x^2 \quad | \quad x^2 + 2x - 2 \\ \hline -2x^3 + 2x^2 + x \\ -2x^3 - 4x^2 + 4x \\ \hline 6x^2 - 3x \\ 6x^2 + 12x - 12 \\ \hline -15x + 12 \end{array}$$

לכן, $x^4 + x = (x^2 - 2x + 6)(x^2 + 2x - 2) + (-15x + 12)$, כלומר, $[r(x) = -15x + 12$ ו- $q(x) = x^2 - 2x + 6$]