

תרגיל מספר 9 מבנים אלגבריים

1. יהא R חוג חילופי עם יחידה. איבר $a \in R$ יקרא מחלק אפס אם קיים $b \in R, b \neq 0$ כך ש $ab = 0$.

(א) הוכיחו/הפירוכו: אם $a \in R$ הפיך אז אינו מחלק אפס.
פתרון: הוכחה: נניח בשלילה כי a מחלק אפס אזי קיים $b \neq 0$ כך ש $ab = 0$. נכפול את השוואה ב a^{-1} ונקבל

$$b = 1 \cdot b = a^{-1}ab = a^{-1}0 = 0$$

סתירה.

(ב) הוכיחו/הפירוכו: אם $a \in R$ אינו מחלק אפס אז a הפיך.
פתרון: הפרכה: למשל $3 \in \mathbb{Z}$ אינו מחלק אפס כי לכל $b \neq 0$ מתקיים $3b \neq 0$. אבל 3 אינו הפיך.

2. יהא $a \in \mathbb{Z}$. הוכיחו: אם $\gcd(a, n) \neq 1$ אז $[a] \notin U_n$. (רמז: האם a מחלק אפס?).
פתרון: נניח $\gcd(a, n) \neq 1$ צ"ל $a \notin U_n$. נגדיר $b = \frac{n}{\gcd(a, n)}$ מהנתון $0 < b < n$ בנוסף .

$$ab = a \frac{n}{\gcd(a, n)} = \frac{a}{\gcd(a, n)} \cdot n \equiv 0 \pmod{n}$$

לכן $[a][b] = [0]$ ב \mathbb{Z}_n ו $[b] \neq [0]$ (כי $0 < b < n$ ולכן בפרט n לא מחלק את b).
 קיבלנו כי $[a]$ מחלק אפס ב \mathbb{Z}_n ולכן לא הפיך. כלומר $[a] \notin U_n$

3. יהא $p \in \mathbb{N}$. הוכיחו כי ראשוני אמ"מ $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ הינו שדה.
פתרון: ידוע כי \mathbb{Z}_p הוא חוג חילופי עם יחידה ($1 \in \mathbb{Z}_p$) הוא היחידה ומתקיים כי $ab = ba \pmod{p}$ ולכן הוא חילופי).

(\Leftarrow) נתון p ראשוני. מספיק להראות כי הוא חוג עם חילוק. כלומר לכל $a \in \mathbb{Z}_p, a \neq 0$ קיים הופכי בחוג. אכן אם $a \neq 0$ אזי $\gcd(a, p) = 1$ כי ראשוני (המחלקים היחידים של p הן $1, p$ אם p מחלק את a אזי $a = 0$ בבחוג שלנו). לכן $a \in U_p$ כלומר קיים c כך ש $ac = 1 \pmod{p}$ ולכן c הוא ההופכי של a .

(\Rightarrow) נניח $n = p$ לא ראשוני ונוכיח כי \mathbb{Z}_n אינו שדה. כיוון ש n אינו ראשוני קיימים $1 < a, b < n$ כך ש $n = ab \pmod{n}$ לכן $ab = 0 \pmod{n}$ כיוון ש $1 < b < n$ ב \mathbb{Z}_p ולכן הוא מחלק אפס ובפרט לא הפיך לפי אחד מתרגילים קודמים. ולכן \mathbb{Z}_n לא שדה

4. יהא R חוג. יהיו I, J שני אידיאלים של R . הוכיחו כי $I \cap J$ גם אידיאל של R .
פתרון: ידוע כי חיתוך של תתי חבורות היא תת חבורה. לכן $(I \cap J, +)$ היא

תת חבורה. נראה בליעה מצד שמאל (מצד שני הרעיון דומה): לכל $r \in R$ ולכל $x \in I \cap J$ מתקיים כי $x \in I$ וגם $x \in J$ ולכן $rx \in I$ וגם $rx \in J$ (כי הם אידיאלים ולכן $rx \in I \cap J$).

5. יהא R חוג קומטטיבי עם יחידה.

(א) הוכיחו כי $Ra = \{ra : r \in R\}$ הוא אידיאל של R .
פתרון: נתחיל להראות כי $(Ra, +)$ תת חבורה. מוגדרות: לכל $r_1a, r_2a \in Ra$ מתקיים כי

$$r_1a + r_2a = (r_1 + r_2)a \in Ra$$

כי $r_1 + r_2 \in R$. קיבוציות: נובעת מקיבוציות של איברים ב R . האיבר הנטרלי לחיבור 0 שייך ל R כי $0a \in Ra$. נגדי: לכל $ra \in Ra$ גם $(-r)a \in Ra$ והוא מקיים

$$ra + (-r)a = [r + (-r)]a = 0a = 0$$

כנדרש.

נראה בליעה משמאל (כיוון שהחוג חילופי זה מוכיח גם בליעה מימין). יהא $r \in R$ ו $x \in Ra$ אזי $x = r'a$ עבור $r' \in R$ ואז $rx = rr'a \in R$ כי $rx = rr'a \in R$.

(ב) יהא $a \in R$. הוכיחו כי $Ra = R$ אמ"מ a הפיך.
פתרון: בכיוון (\Rightarrow) נתון כי a הפיך. לכן קיים a^{-1} ואז כל $r \in R$ ניתן להצגה $r = ra^{-1} \cdot a \in Ra$ (כי $ra^{-1} \in R$) לכן $R \subseteq Ra$ ההכפלה $Ra \subseteq R$ תמיד מתקיימת.

בכיוון (\Leftarrow) נתון $Ra = R$ בפרט $1 \in R = Ra$ לכן קיים $r \in R$ כך ש $1 = ra$ כיוון שהחוג חילופי מתקיים גם $ar = ra = 1$ ולכן $r = a^{-1}$ כנדרש.

(ג) יהא $a \in R$. הוכיחו כי $Ra = \{0\}$ אמ"מ $a = 0$.
פתרון: בכיוון (\Rightarrow) נתון כי $a = 0$ לכן $Ra = \{ra : r \in R\} = \{r0 : r \in R\} = \{0\}$.

בכיוון (\Leftarrow) נתון $Ra = \{0\}$ בפרט $a = 1 \cdot a \in Ra = \{0\}$ לכן $a = 0$ כנדרש.

(ד) הסיקו מי הם כל האידיאלים של $R = \mathbb{F}$ שדה.
פתרון: יהא I אידיאל. אפשרות 1: $I = \{0\}$.
 אפשרות 2: $I \neq \{0\}$ לכן קיים $a \in I$ ו $a \neq 0$ ואז $\mathbb{F}a \subseteq I$ (כי לכל $r \in \mathbb{F}$ מתקיים $ra \in I$ מתכונת הבליעה). כיוון שמדובר בשדה אז a הפיך ולכן $\mathbb{F} = \mathbb{F}a \subseteq I$ ההכלה $I \subseteq \mathbb{F}$ תמיד מתקיימת ולכן $I = \mathbb{F}$.
 לסיכום: האידיאלים היחידים של שדה הם האידיאלים הטריוואלים.