

## אלגברה מופשטת 2 – תרגול 4

### הגדרה

$R$  יקרא חוג פשוט אם אין לו אידיאלים פרט ל  $R$  ול  $\{0\}$ .

### דוגמאות:

- חוג עם חילוק הוא חוג פשוט (כל איבר שונה מ 0 הוא הפיך, ולכן האידיאל היחיד שמכיל אותו הוא  $R$  עצמו).
- חוג קומוטטיבי עם יחידה ופשוט הוא שדה. מכיוון שאם  $x \in R, x \neq 0 \rightarrow Rx = R$  ואז לכל איבר בחוג יש הופכי. ( $Rx$  הוא אידיאל מכיוון שהחוג קומוטטיבי, מכיוון שהחוג פשוט  $Rx = R$  מכיוון שהחוג עם יחידה  $1_R \in Rx$  ז"א קיים  $y \in R$  כך ש  $yx = 1_R$  ומהקומוטטיביות נקבל ש  $xy = 1_R$ ).

### תזכורת

אם  $D$  חוג עם חילוק אז  $Z(D)$  שדה.

### טענה

אם  $R$  חוג פשוט עם יחידה אז  $Z(R)$  שדה.

### הוכחה

ראינו ש  $Z(R)$  תת חוג קומוטטיבי. יהי  $x \in Z(R), x \neq 0$ . מכיוון ש  $R$  חוג פשוט נקבל ש  $\langle x \rangle = Rx = xR = R$ . אם כך קיים  $y \in R$  כך ש  $xy = 1$ , לכן  $x$  הפיך ונשאר להוכיח ש  $x^{-1} \in Z(R)$ . עבור  $r \in R$  מתקיים:  
 $xr = rx \rightarrow x^{-1}xr = x^{-1}rx \rightarrow r = x^{-1}rx \rightarrow rx^{-1} = x^{-1}r \rightarrow x^{-1} \in Z(R)$

### משפט

יהי  $I \triangleleft R$  אז  $M_n(I) \triangleleft M_n(R)$  וכל אידיאל של  $M_n(R)$  הוא מהצורה הזו.

### דוגמא

$$M_n(2\mathbb{Z}) \triangleleft M_n(\mathbb{Z})$$

אם  $R$  הוא חוג עם חילוק, למשל: הממשיים, הרציונלים, הקוטרניונים, אז ל  $R$  אין אידיאלים ולכן  $M_n(R)$  הוא חוג פשוט עם יחידה ולכן  $Z(M_n(R))$  הוא שדה שאיזומורפי ל

$Z(R)$  (לפי משפט המרכז הוא בדיוק המטריצות הסקלריות  $xI$  כאשר  $x \in Z(R)$ , ואז האיזומורפיזם ברור).

### תרגיל:

יהי  $A \subseteq M_n(R)$  תת חוג,  $I \triangleleft A$ . האם בהכרח קיים  $J \triangleleft R$  כך ש  $I = A \cap M_n(J)$ ?

**פתרון:** לא. לדוגמה:

$A$  – מטריצות משולשיות עליונות ב  $M_n(\mathbb{Z})$ .  $I$  מטריצות ב  $A$  עם אלכסון שווה לאפס.

אז לא קיים  $J$  כך ש  $J \triangleleft R$  ו  $I = A \cap M_n(J)$  מכיון ש  $I = \begin{pmatrix} 0 & * & * \\ \cdot & \cdot & * \\ 0 & \cdot & 0 \end{pmatrix}$  ואילו אידיאל של

$M_n(\mathbb{Z})$  (לפי המשפט) הוא מהצורה  $M_n(m\mathbb{Z})$ .

### תרגיל

יהי  $D$  חוג עם חילוק שאינו שדה כך ש  $Z(D) = F \neq D$  (שדה) צ"ל שלכל  $d \in D \setminus F$  מתקיים  $\langle x-d \rangle = D[x]$ .

### פתרון

נוכיח שהאידיאל  $\langle x-d \rangle$  מכיל איבר הפיך. יהי  $e \in D$  כך ש  $ed \neq de$ . אז  
 $f(x) = -e(x-d) + (x-d)e \in \langle x-d \rangle$  בנוסף  $f(x) = ed - de \in D$  (זכרו ש  $x \in Z(D[x])$  לפי הגדרת חוג הפולינומים, ולכן  $ex = xe$ ), חוג עם חילוק ולכן ל  $f(x)$  יש הופכי. ז"א  
 $\langle x-d \rangle = D[x]$

### הערה

שימו לב שאם  $F$  שדה אז לכל  $a \in F$   $\langle x-a \rangle \neq F[x]$  (ניתן להראות שכל האיברים באידיאל הם עם דרגה גדולה שווה ל 1).

**תרגיל:** תנו דוגמה לחוגים  $R, S$ , הומו'  $\varphi: R \rightarrow S$  ואידיאל  $I \triangleleft R$  כך ש  $\varphi(I)$  אינו אידיאל של  $S$  (זכרו שאם  $\varphi$  על אז תמונת אידיאל היא אידיאל).

**פתרון:** ניקח  $R = \mathbb{Z}, S = \mathbb{Q}$  ו-  $\varphi = id$ . אזי תמונת  $\mathbb{Z}$  היא  $\mathbb{Z}$  ואינה אידיאל של  $\mathbb{Q}$  כיוון שהאידיאלים היחידים של  $\mathbb{Q}$  הם  $\{0\}, \mathbb{Q}$ .

## חוג מנה

יהי  $R$  חוג,  $I \triangleleft R$ . אז על  $R/I = \{a+I \mid a \in R\}$  נגדיר חיבור וכפל באופן הבא:

$$(a+I)(b+I) = ab+I \quad \bullet$$

$$(a+I)+(b+I) = (a+b)+I \quad \bullet$$

אז  $(R/I, +, \cdot)$  הוא חוג, איבר האפס הוא  $I$ . אם קיים איבר יחידה בחוג  $R$  אזי קיים איבר יחידה ב  $R/I$  והוא  $1_R + I$ .

## הערה

אם  $I \triangleleft R$  ו  $a \in I$  אז המחלקות  $I$  ו  $\pm a + I$  הן אותו איבר ב  $R/I$ .

## דוגמאות

1.  $R = 3\mathbb{Z}, I = 18\mathbb{Z}$ . אז  $R/I = \{18\mathbb{Z}, 3+18\mathbb{Z}, 6+18\mathbb{Z}, 9+18\mathbb{Z}, 12+18\mathbb{Z}, 15+18\mathbb{Z}\}$ .

בתור חבורה חיבורית  $R/I \cong \mathbb{Z}_6$ . נבנה את לוח הכפל ונראה שבתור חוגים  $R/I$  לא איזומורפי ל  $\mathbb{Z}_6$ , נשים לב שב  $R/I$  אין יחידה וב  $\mathbb{Z}_6$  יש.

$\cdot$	0	3	6	9	12	15
0	0	0	0	0	0	0
3	0	9	0	9	0	9
6	0	0	0	0	0	0
9	0	9	0	9	0	9
12	0	0	0	0	0	0
15	0	9	0	9	0	9

2.  $\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\} \cong \mathbb{Z}_5$ .

3.  $R = \mathbb{R}[x]$  נסמן  $I = \langle x^2 + 1 \rangle = \{f(x)(x^2 + 1) \mid f(x) \in \mathbb{R}[x]\}$ .

נסמן  $\bar{a} = a + I \in R/I$ . מתקיים:  $x^2 + I = x^2 - (x^2 + 1) + I = -1 + I$ , ולכן  $\bar{x}^2 = \bar{-1}$  ב  $R/I$  באותו אופן ניתן לראות ש  $\bar{x}^3 = \bar{-x}, \bar{x}^4 = \bar{1}, \bar{x}^5 = \bar{x}, \dots$

לכן  $R/I = \{\alpha + \beta\bar{x} \mid \alpha, \beta \in \mathbb{R}\}$  כי כל חזקה  $\bar{x}^n$   $n > 1$  היא  $\pm\bar{x}$  או  $\pm\bar{1}$ , כשמתקיים  $\bar{x} \cdot \bar{x} = \bar{-1}$ .

**תרגיל בית:**  $R/I \cong \mathbb{C}$  (מגדירים  $f(\alpha + \beta x) = \alpha + \beta i$  ובודקים שמתקיימות תכונות האיזו). תרגיל

4. יהי  $R = \mathbb{Z}_3[x]$ ,  $I = \langle x^2 + 1 \rangle$ . כמה איברים יש ב  $R/I$ ? כמו בדוגמא הקודמת גם פה  $\overline{x^2} = \overline{-1}$  ב  $R/I$  ולכן  $R/I = \{ \alpha + \beta \overline{x} \mid \alpha, \beta \in \mathbb{Z}_3 \}$  ז"א שב  $R/I$  יש 9 איברים.

## תרגיל

איבר  $x$  בחוג  $R$  הוא נילפוטנט אם קיים  $n \in \mathbb{N}$  כך ש  $x^n = 0$ . יהי  $R$  חוג קומוטטיבי ויהי  $N$  קבוצת האיברים הנילפוטנטים ב  $R$ .

1. הוכיחו כי  $N$  אידיאל ב  $R$ .
2. הוכיחו כי ב  $R/N$  אין איברים נילפוטנטים שונים מאפס.
3. תנו דוגמא לחוג לא קומוטטיבי כך ש  $N$  לא אידיאל.

## פתרון

1.  $N$  שונה מקבוצה ריקה מכיוון ש  $0 \in N$ . יהיו  $a, b \in N$  ז"א קיים  $l$  כך ש  $b^l = 0$  וקיים  $j$  כך ש  $a^j = 0$ . לפי הבינום של ניוטון (נכון בחוגים קומוטטיביים אך לא בלא

$$\text{קומוטטיביים): } (a-b)^{j+l} = \sum_{k=0}^{j+l} (-1)^k \binom{j+l}{k} a^k b^{j+l-k}.$$

• אם  $k \geq j$  אז  $a^k = 0$ .

• אם  $k < j$  אז  $l < l + j - k$  ואז  $b^{j+l-k} = 0$ .

צריך להוכיח גם בליעה כאן, אבל זה קל: אם  $a \in N, b \in R$  אזי קיים  $n > 0$  כך ש  $a^n = 0$  ולכן  $(ab)^n = a^n b^n = 0$ .

2. נניח בשלילה שיש איברים נילפוטנטים שונים מאפס ב  $R/N$ . יהי  $\overline{x} = x + N \in R/N$ ,  $\overline{0} \neq \overline{x}$  כך שקיים  $k \in \mathbb{N}$  כך ש  $\overline{x^k} = \overline{0}$ . אז  $\overline{x^k} = \overline{0} = \overline{x^k} = (x + N)^k = x^k + N$  ולכן  $x^k \in N$ , ולכן  $x^k$  נילפוטנט ז"א קיים  $l \in \mathbb{N}$  כך ש  $(x^k)^l = 0$  ולכן  $x^{kl} = 0$  ז"א  $x \in N$  (מכיוון ש  $x$  נילפוטנט) ז"א  $\overline{x} = \overline{0}$  בסתירה להנחה ש  $\overline{x} \neq \overline{0}$ .

3. יהי  $R = M_2(\mathbb{Q})$ ,  $e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ,  $e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ , ולכן הם איברים נילפוטנטים,  $e_{12}^2 = e_{21}^2 = 0$ .

$$\text{אבל } (e_{12} + e_{21})^n = \begin{cases} I \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{cases} \text{ כאשר } n \text{ זוגי, ל } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ כאשר } n \text{ אי זוגי}$$

סה"כ קיבלנו ש  $(e_{12} + e_{21})^n \neq 0$  לכל  $n \in \mathbb{N}$ .

ולכן  $N$  אינו סגור לחיבור ו  $N$  אינו אידיאל.

**הגדרה:** יהי  $R$  חוג,  $R_0 \subseteq R$  תת-חוג ו-  $X \subseteq R$  תת-קבוצה. **התת-חוג הנוצר מעל  $R_0$**

**ע"י  $X$**  הוא חיתוך כל התת-חוגים של  $R$  המכילים את  $R_0, X$ . מסמנים ב-  $R_0[X]$ . אם

$R_0[X] = R$  אזי אומרים ש  $R$  **נוצר ע"י  $X$**  (מעל  $R_0$ ). אם  $X$  סופית ו  $R$  נוצר ע"י  $X$  אז

אומרים ש  $R$  **נוצר סופית** (מעל  $R_0$ ), ומסמנים  $R = R_0[a_0, \dots, a_n]$  כאשר  $X = \{a_0, \dots, a_n\}$ .

הערה: בחוג קומוטטיבי דרך אחרת לאפיין חוג הנוצר סופית היא כאוסף כל הביטויים

הפולינומיאליים ב  $a_0, \dots, a_n$  עם מקדמים ב  $R_0$ , כלומר  $\sum_{i_1, \dots, i_n=0}^d r_{i_1, \dots, i_n} a_1^{i_1} \cdots a_n^{i_n}$ .

### דוגמאות:

1. יהי  $S = R[x_1, \dots, x_n]$  חוג פולינומים מעל חוג  $R$  אזי  $S$  נוצר סופית ע"י  $\{x_1, \dots, x_n\}$  (כי

אם  $\hat{R} \subseteq S$  הוא תת-חוג המכיל את  $x_1, \dots, x_n$  ואת  $R$  אזי הוא מכיל את כל

הפולינומים, לפי סגירות לחיבור וכפל בחוג).

2.  $S = \mathbb{Z}$  נוצר סופית מעל כל תת-חוג שלו  $R = n\mathbb{Z}$  כי  $R[1] = \mathbb{Z}$ .

### משפט האיזומורפיזם הראשון

יהי  $f: R \rightarrow S$  הומומורפיזם, אז  $R/\ker f \cong \text{Im } f$ .

**תרגיל:** כל חוג קומוטטיבי נוצר סופית מעל  $R_0$  הוא מנה (יותר מדויק לומר שהוא

איזומורפי למנה, אבל אנחנו נזהה בין שני המושגים) של חוג פולינומים  $R_0[x_1, \dots, x_n]$ .

### פתרון:

יהי  $S$  חוג נוצר סופית מעל  $R_0$ , אזי קיימים  $a_1, \dots, a_n \in S$  היוצרים את  $S$  מעל  $R_0$ . נגדיר

$\pi: R_0[x_1, \dots, x_n] \rightarrow S$  ע"י  $\pi(x_i) = a_i$  לכל  $1 \leq i \leq n$  ו-  $\pi(r) = r$  לכל  $r \in R_0$ ; נרחיב את

הגדרת  $\pi$  לכל  $R_0[x_1, \dots, x_n]$  ע"י  $\pi(f(x_1, \dots, x_n)) = f(a_1, \dots, a_n)$  (יש לבדוק שזהו הומו, עשו

זאת). כעת ניתן לראות ש  $\pi$  היא על כיוון שכל איבר ב  $S$  ניתן להצגה כביטוי פולינומיאלי

ב-  $a_1, \dots, a_n$ :  $f(a_1, \dots, a_n) = \sum_{i_1, \dots, i_n=0}^d r_{i_1, \dots, i_n} a_1^{i_1} \cdots a_n^{i_n}$  ואז המקור שלו הוא  $f(x_1, \dots, x_n)$ . לפי משפט

האיזומורפיזם הראשון, נקבל ש  $S \cong R / \text{Ker } \pi$ .

**הערה:** הכיוון השני של המשפט אינו נכון בניסוח זה. לדוגמא אם ניקח  $\mathbb{Z}[x]$  אזי  $2\mathbb{Z}[x]$  הוא אידאל, והמנה איזומורפית ל  $\mathbb{Z}_2[x]$  (נגדיר  $\varphi: \mathbb{Z}[x] \rightarrow \mathbb{Z}_2[x]$  פונק' שמבצעת מודולו 2 לכל המקדמים, זהו הומו' על שהגרעין שלו הוא בדיוק  $2\mathbb{Z}[x]$  ואז לפי איזו' 1). זהו אינו חוג נוצר סופית מעל  $\mathbb{Z}$ , כיוון שאינו מכיל את  $\mathbb{Z}$  (וגם לא עותק איזומורפי של  $\mathbb{Z}$ , כי לכל איבר  $a \in \mathbb{Z}_2[x]$  מתקיים  $2a = 0$ ).