

אלגברה ב' 2 - הרצאה 1

21.02.11

חוגים, שדות

הגדרה. חוג הוא קבוצה R עם שתי פעולות בינאריות אסוציאטיביות $+$, $\cdot$ כך ש- $(R, +)$ היא חבורה חילופית ויש חוקי פילוג:

$$(a + b)c = ac + bc$$

$$c(a + b) = ca + cb$$

הערה. לא תמיד נכתוב את ה- $\cdot$. אבל הוא אמור להיות שם.

הגדרה. R חוג חילופי אם הכפל חילופי.

הגדרה. R חוג עם יחידה אם יש $1 \in R$ כך ש- $1 \cdot a = a \cdot 1 = a$ לכל $a \in R$.

הערה. יש רק יחידה אחת. אם $1, 1' \in R$ יחידות אז

$$1 = 1 \cdot 1' = 1'$$

מעתה נדבר רק על חוגים עם יחידות.

דוגמאות.

1. $\mathbb{Z}$

2. $\mathbb{Z}/n\mathbb{Z} \quad n \geq 1$

3. $\mathbb{C}$

4. $\mathbb{Q}$

5. $\mathbb{R}$

6. $M_n(F)$ כאשר F שדה.

7. $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$

8. $\{0\}$ כאן $0 = 1$. יתר על כן, אם בחוג מסויים R מתקיים $1 = 0$ אז $R = \{0\}$ כי כל $a \in R$ הוא למעשה $a \cdot 1 = a$.

תרגיל: בחוג R לכל $a \in R$ מתקיים $0 = a \cdot 0 = 0 \cdot a$.
תרגיל: בחוג R : $-1 \cdot a = -a$ לכל $a \in R$. $a + (-1)a = 1 \cdot a(-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0$.
תרגיל: חוג R ההפיכים:

$$R^* = \{a \in R : \exists s \in R, as = 1 = sa\}$$

הגדרה. חוג עם יחידה R נקרא תחום שלמות (או תחום) אם אין בו מחלקי 0. כלומר, בו מתקיים:

$$a, b \neq 0 \Rightarrow ab \neq 0$$

שדה F הוא חוג בו $F \setminus \{0\}$ חבורה חילופית ביחס לכפל. שדה הוא תחום שלמות.

הגדרה. העתקה $\varphi : R \rightarrow S$ נקראת הומומורפיזם אם היא שומרת חיבור וכפל. כלומר מעבירה סכום לסכום וכפל לכפל. כמו כן, מתקיים:

$$\varphi(1_R) = 1_S$$

הגדרה. איזומורפיזם הוא הומומורפיזם חח"ע ועל.

הגדרה. תת קבוצה R_0 של חוג R נקראת תת חוג של R אם היא סגורה תחת החיבור והכפל ומכילה את איבר היחידה.

דוגמא. $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ ע"י $k \mapsto [k] = k + n\mathbb{Z}$. זהו למעשה הפימורפיזם (הומומורפיזם על).

הערה. יהי $V_0 : R_0 \rightarrow S$ הומומורפיזם. אז

$$1. S_0 = \varphi_0(R_0) \subseteq S \text{ הוא תת חוג של } S.$$

2. אם במקרה φ_0 חח"ע אז $\varphi_0 : R_0 \rightarrow S_0$ הוא איזומורפיזם. אפשר למצוא חוג R שמכיל את R_0 , כלומר R_0 הוא תת חוג שלו ולהרחיב את φ_0 לאיזומורפיזם $\varphi : R \rightarrow S$. נשלים ע"י "עותקים" של איברי $S \setminus S_0$ ופעולות מוגדרות לפי S .

חוג הפולינומים

יהי R חוג עם יחידה. נגדיר

$$R[x] = \left\{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in R, \text{ מסויים } 0 \right\}$$

$$\left(\sum_{i=0}^{\infty} a_i x^i \right) + \left(\sum_{i=0}^{\infty} b_i x^i \right) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{\infty} a_i x^i \right) \cdot \left(\sum_{j=0}^{\infty} b_j x^j \right) = \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

זה מוגדר היטב כי גם התוצאות מאותה הצורה וכן יתאפסו החל ממקום מסויים.
 באופן מקוצר נכתוב $\sum_{i=0}^n a_i x^i$ כאשר $a_{n+1} = a_{n+2} = \dots = 0$ כמו כן נכתוב a_0
 במקום $a_0 x^0$ וכן $a_1 x$ במקום $a_1 x^1$.

הגדרה. המעלה של פולינום

$$\deg(\underbrace{\sum_{i=0}^{\infty} a_i x^i}_{\neq 0}) = \max\{i : a_i \neq 0\}$$

וכן נגדיר: $\deg(0) = -\infty$.

נשים לב:

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$$

$$\deg(fg) \leq \deg(f) + \deg(g)$$

באי שוויון השני יש שוויון כאשר R הוא תחום.

זאת דוגמא נוספת לחוג.

נראה דוגמא של הומומורפיזם:

דוגמא. R חוג עם יחידה חילופי. $\alpha \in R$. ההצבה: $f \mapsto f(\alpha)$ היא הומומורפיזם
 $R[x] \rightarrow R$.

הערה. יחידה צריך כדי להגדיר α^0 .

הגדרה. יהי R חוג. תת קבוצה I ב- R נקראת אידאל אם איננה ריקה, סגורה תחת חיבור,
 מקיימת:

$$\forall x \in I \quad \forall a \in R \quad a \cdot x, x \cdot a \in I$$

בפרט לדוגמא הנגדיים תמיד גם באידאל.

דוגמאות. 1. $\{0\}$.

2. R עצמו.

3. גרעין של הומומורפיזם $\varphi: R \rightarrow S$.

4. $I = 2\mathbb{Z} \subseteq \mathbb{Z} = R$.

5. אם R חילופי $x \in \mathbb{R}$ אז $(x) := \{ax | a \in R\}$ הוא אידאל. אידאל מהצורה הזאת
 נקרא אידאל ראשי. זהו האידאל הקטן ביותר של R שמכיל את האיבר x .

הערה. אם $I_1, I_2 \subseteq R$ אידאלים אז גם $I_1 \cap I_2$, $I_1 + I_2 = \{x_1 + x_2 | x_1 \in I_1, x_2 \in I_2\}$,
 $I_1 \cdot I_2 = \{\sum_{i=1}^n (x_i \cdot y_i) | x_i \in I_1, y_i \in I_2\}$ הם אידאלים. סתם קבוצת מכפלות כנראה
 לא תהיה סגורה תחת חיבור.

הגדרה. אידאל I של R נקרא נאות (proper) אם $I \neq R$. זה שקול לכך ש- $1 \notin I$. כמו כן זה שקול לכך ש- $u \notin I$ כאשר $u \in R^*$.

תרגיל: יהי R חוג חילופי. אז R הוא שדה אם ורק אם R אינו חוג האפס וכן $0, R$ הם האידאלים היחידים ב- R .

הוכחה. יהי $x \in R, x \neq 0$. אז (x) הוא אידאל שונה מ- 0 . לכן $(x) = R$. בפרט $1 \in (x)$. כלומר, יש $a \in R$ כך ש- $ax = 1$ ולכן $x \in R^*$. כיוון שני באמת תרגיל.

□

יהי R חוג, $I \subseteq R$ אידאל. בפרט R חבורה חילופית ביחס לחיבור. I תת חבורה (תת קבוצה לא ריקה סגורה לחיבור). אז R/I חבורת המנה ביחס לחיבור. במקרה שלנו זה לא סתם חבורה אלא חוג. איברי R/I :

$$a \in R \quad [a] = a + I = \{a + x \mid x \in I\}$$

הפעולות:

$$[a] + [b] = [a + b]$$

$$[a][b] = [ab]$$

את זה שהחיבור מוגדר היטב זוכרים מאלגברה ב'1. נוכיח לגבי הכפל. אם $[a] = [a'], [b] = [b']$. כלומר, $a - a' \in I, b - b' \in I$.

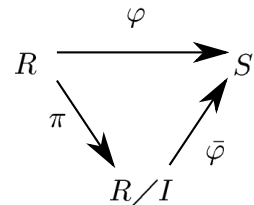
$$ab - a'b' = a \underbrace{(b - b')}_{\in I} + \underbrace{(a - a')}_{\in I} b'$$

לכן כל ההפרש ב- I . מכאן, $[ab] = [a'b']$.

משפט. בסימונים הנ"ל R/I הוא חוג והעתקה $\pi : R \rightarrow R/I$ הנתונה ע"י $a \mapsto [a]$ היא אפימורפיזם.

משפט. משפט האיזומורפיזם הראשון:

יהי $\varphi : R \rightarrow S$ הומומורפיזם של חוגים. ניקח I אידאל כך ש- $I \leq \ker \varphi$. אז קיים הומומורפיזם יחיד $\bar{\varphi} : R/I \rightarrow S$ כך ש- $\bar{\varphi} = \varphi \circ \pi$.



אם $I = \ker \varphi$ אז $\bar{\varphi}$ חח"ע. אם φ על אז $\bar{\varphi}$ על.

הוכחה. נסתמך על משפט האיזומורפיזם הראשון לחבורות. אם $\bar{\varphi}$ נתון ע"י $\bar{\varphi}([a]) = \varphi(a)$ צריך לבדוק ש- $\bar{\varphi}$ שומר על כפל.

$$\bar{\varphi}([a][b]) = \bar{\varphi}([ab]) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}([a])\bar{\varphi}([b])$$

□

תרגיל:

אם $\pi: R \rightarrow R/I$ אז $J \subseteq R/I$ אידאל אם $\pi^{-1}(J) \subseteq R$ אידאל. ההעתקה $J \mapsto \pi^{-1}(J)$ היא התאמה חח"ע מאוסף כל האידאלים של R/I על אוסף כל האידאלים של R שמכילים את I .
רמז: מזכיר את משפט האיזומורפיזם השני.

הגדרה. אידאל I נקרא מרבי אם $I \neq R$ ואין אידאל J בין I ל- R פרט ל- I ו- R . כלומר אם $J \subseteq R$ אידאל, $I \subseteq J$ אז $I = J$ או $J = R$.

הגדרה. $I \neq R$ נקרא אידאל ראשוני אם לכל $a, b \in R$ מתקיים: אם $ab \in I$ אז $a \in I$ או $b \in I$.

דוגמא. $R = \mathbb{Z}$: $(3) = 3\mathbb{Z}$ אידאל מרבי וגם ראשוני. אבל אנחנו לא יודעים עדיין שכאן כל אידאל הוא ראשי או אנחנו לא יודעים להוכיח את זה. בינתיים.

למה.

1. אידאל I הוא פרבי $\Leftrightarrow R/I$ הוא שדה.

2. אידאל I הוא ראשוני $\Leftrightarrow R/I$ הוא תחום שלמות.

הוכחה.

1. R/I שדה $\Leftrightarrow R/I \neq 0$ ו- $0, R/I$ האידאלים היחידים ב- R/I (תרגיל) $\Leftrightarrow I \neq R$ ו- I, R האידאלים היחידים ב- R (תרגיל) $\Leftrightarrow I$ מרבי.

2. R/I תחום שלמות $\Leftrightarrow$ לכל $[a], [b] \in R/I$ אם $[a][b] = [0]$ אז $[a] = 0$ או $[b] = 0$ וגם $[1] \neq [0] \Leftrightarrow$ לכל $a, b \in R$ אם $a, b \in I$ אז $a \in I$ או $b \in I$ וגם $1 \notin I$.
 $\underbrace{1 \notin I}_{I \neq R}$

מסקנה. אידאל פרבי הוא ראשוני.

מדוע? כי אם הוא מרבי אז R/I שדה ובפרט תחום שלמות.

□