

חוקים

הצגה: שלשה  $\langle R, +, \cdot \rangle$  תהיה חוג אם:  $\langle R, + \rangle$  תהיה אברהם (חילופית), פעולה הכפל אסוציאטיבית ומתק"מ חוק הפילוג:

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

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

סימונים: האיבר הנייטרלי לחיבור מסומן 0; האיבר הנייטרלי לחיבור קוראים "יחידה", ומסמנים  $-x$ ; אם יש איבר נייטרלי לכפל, מסמנים אותו 1 וקוראים לו "יחידה".

דוגמאות: א.  $F[x_1, \dots, x_n]$  הוא הפולינומים ב-n משתנים מעל שדה  $F$ .

ב. חוג השלמים של גאוס:

$$\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$$

נראה סביר כי לכל לחיבור:

$$(a+bi) + (c+di) = \underbrace{(a+c)}_{\in \mathbb{Z}} + \underbrace{(b+d)}_{\in \mathbb{Z}} i \in \mathbb{Z}[i]$$

ובאופן דומה מראים שאם לכל:

$$0 = 0 + 0i \quad \text{איבר נייטרלי לחיבור:}$$

אסוציאטיביות חוק הפילוג מתקיימים כי הם מתקיימים ב- $\mathbb{C}$ .

$$1 = 1 + 0i \quad \text{יחידה:}$$

חילופיות הכפל מתקיימת כי היא מתקיימת ב- $\mathbb{C}$ .

האם זהו תחום שלמות? כלומר, האם

$$0 = bi \Leftrightarrow a=0 \text{ או } b=0? \quad \text{כן, כי } \mathbb{Z}[i] \subseteq \mathbb{C}.$$

$\mathbb{Z}[i]$  איננו שדה, כי יש בו איברים שלא הופכי, למשל

$1+i$  אין הופכי. נניח בשלילה שהיה לו:

$$(a+bi)(1+i) = 1 \Leftrightarrow (a-b) + (a+b)i = 1$$

$$1 = a-b = -2b$$

$$\Leftrightarrow a = -b \Leftrightarrow$$

אז לא ייתכן, לכן  $b$  הוא מספר שלם.

הוכחה אלגנטית יותר: אנחנו יודעים שההופכי (היחיד) של  $1+i$  ב- $\mathbb{C}$  הוא  $\frac{1-i}{2}$ , וזה לא שלם בגאוס.

## עוד דוגמאות:

ג. קבוצת כל סדרות הממשליות המתכנסות, תחת פעולות לפי רכיבים:

$$a+b = \{a_n+b_n\}_{n=1}^{\infty} \quad a \cdot b = \{a_n \cdot b_n\}_{n=1}^{\infty}$$

סגירות לכפל, למשל, נובעת מהמשפט לפיו

$$\begin{cases} a_n \rightarrow \alpha \\ b_n \rightarrow \beta \end{cases} \Rightarrow a_n b_n \rightarrow \alpha \beta$$

אסוציאטיביות:

$$(a+b)+c = \{a_n+b_n\} + \{c_n\} = \{(a_n+b_n)+c_n\} = \{a_n+(b_n+c_n)\} = \{a_n\} + \{b_n+c_n\} \\ \parallel \\ a+(b+c)$$

זה לא תחום שלמות:

$$(1, 0, 0, 0, \dots) \cdot (0, 1, 0, 0, \dots) = (0, 0, 0, \dots)$$

$$(1, 1, 1, \dots)$$

איבר היחידה:

איבר הקבוצה הוא הפיק אלמנט כל איבר בסדרה שונה מ-0, וההצדקה לא שואפת ל-0.

הוכחה: כיוון תאון: נגדיר  $b_n = a_n^{-1}$  אזי  $a_n \rightarrow \alpha$  כאשר  $b_n \rightarrow \frac{1}{\alpha}$

$$a \cdot b = b \cdot a = \{a_n \cdot b_n\} = \{1\} = 1 \quad b = \{b_n\} \text{ מק"מ"ל}$$

ומאחר שאיבר  $a$  לא שואפים ל-0,  $b$  מתכנסת ולכן היא איבר בתחום.

כיוון שני: אם  $a$  הפיכה, יש איבר שמק"מ  $a \cdot b = b \cdot a = 1$

לכן לכל  $n$ ,  $a_n \cdot b_n = 1$  לכן  $a_n \neq 0$ .

$b$  ש"כ לקבוצה, לכן היא בפרט חסומה, ומכאן אם  $a_n \rightarrow 0$

נובע מכך  $a_n \cdot b_n \rightarrow 0$  בסתירה לכך ש  $a \cdot b = 1$ .  $\square$

## הומומורפיזמים

יהיו  $R, C$  חוגים.  $f: R \rightarrow C$  יוקרא הומומורפיזם אם:

$$f(a+b) = f(a) + f(b) \quad f(ab) = f(a)f(b)$$

## דוגמאות

- העברות הוא הומומורפיזם מחוג הסדרות שפגדורני קודם לממשליות.
- הם פונקציה שווה לאיבר הפאסון הוא הומומורפיזם מחוג זה לממשליות.

$$3. \mathbb{Z}[i] \cong \begin{Bmatrix} a & b \\ -b & a \end{Bmatrix} : a, b \in \mathbb{Z}$$

תרגיל:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  אינן אוטומורפיזם (איטומורפיזם מתקנה  $f(1) = 1$ ) פה  $f(1) = 1$ .

פתרון: תהי:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  איטומורפיזם, נראה שהתקיים  $f(1) = 1$ .  
באופן כללי, אם  $f: R \rightarrow L$  הומומורפיזם של ויש יחידה 1 ב-R, אז  $f(1)$  יחידה ב-L (אלא אם כן L הוא חצי האפס). זה נכון, כי לכל  $\ell \in L$ :

$$\ell \cdot f(1) = f(x) \cdot f(1) = f(x \cdot 1) = f(x) = \ell$$

לכל  $n \geq 1$  נכחי,  $f(n) = f(\underbrace{1+1+\dots+1}_n) = \underbrace{f(1)+\dots+f(1)}_n = n \cdot f(1) = n$

$$f(-n) = -f(n) = -n$$

מאחר ש-L הומומורפיזם חיבורי!

וצה מס'ים את ההוכחה.

הערה:  $x \mapsto -x$  אוטומורפיזם של  $\mathbb{Z}$  כחבורה תחת חיבור.

תרגיל: מצאו את כל האוטומורפיזמים של  $\mathbb{Z}[i]$ .

פתרון: יהי  $\varphi$  אוטומורפיזם. אז  $\varphi(1) = 1$ .

$$\varphi(i) = \pm i \iff \varphi(i)^2 + 1 = 0 \iff \varphi(i^2 + 1) = \varphi(0) \iff i^2 + 1 = 0$$

מתקיים בחירה של  $\varphi(i)$  קובע את  $\varphi$  חד-משמעית, כי:

$$\varphi(a+bi) = \varphi(a) + \varphi(b)\varphi(i) = a + b\varphi(i)$$

לסיכום, יש שני אוטומורפיזמים של  $\mathbb{Z}[i]$ :

$$(z \mapsto z) \text{ ו} (z \mapsto \bar{z}).$$

תרגיל: תהי G חבורה,  $\alpha \in G$  (צדד:  $f_\alpha(g) = \alpha^{-1}g\alpha$ ). הריא כי  $f_\alpha$  אוטו.

$$f_\alpha(g) = \alpha^{-1}g\alpha = \alpha^{-1}g\alpha\alpha^{-1}\alpha = \alpha^{-1}g\alpha = f_\alpha(g) \quad \text{הוכחה: } f_\alpha \circ f_\alpha = \text{id}$$