מבוא לחוגים ומודולים – שיעורי בית 2

ליאור פולק

1 באפריל 2017

1 תרגיל

יהי p מספר ראשוני.

1. יהי R חוג בלי יחידה מסדר p. הוכיחו כי או ש־$R \cong {}^{\mathbb{Z}}/_{p\mathbb{Z}}$ עם חיבור וכפל מודולו p (של הנציגים), או $R \cong \left({}^{\mathbb{Z}}/_{p\mathbb{Z}}, +, \odot\right)$ עם חיבור מודולו p וכפל האפס שבו תמיד $x \odot y = 0$.
2. תנו דוגמאות לחוגים עם יחידה מסדר p^2 שאינם איזומורפיים. רמז: יש ארבעה כאלו, עד כדי איזומורפיזם. נסו למצוא את כולם.
3. העשרה: קראו את המאמר "מיון חוגים סופיים מסדר p^2" מאת בנג'מין פיין וענו כמה חוגים בלי יחידה יש מסדר p^2q עבור $p \neq q$ ראשוני.

פתרון.

1. יהי R חוג בלי יחידה מסדר p. אזי החבורה החיבורית $(R, +, 0_R)$ היא מסדר p. מכאן נובע שהיא איזומורפית ל־${}^{\mathbb{Z}}/_{p\mathbb{Z}}$. לכן פעולת החיבור היא חיבור מודולו p של הנציגים.
נסמן $\cdot$ את הכפל הרגיל ב־${}^{\mathbb{Z}}/_{\mathbb{Z}}$, וב־$\times$ את הכפל ה"חדש".
לגבי פעולת הכפל, אפשר לצמצם את הבעיה למהו 1×1, שכן

$$a \times b = \underbrace{(1 + 1 + \ldots + 1)}_{a \text{ times}} \times \underbrace{(1 + 1 + \ldots + 1)}_{b \text{ times}} = \underbrace{(1 \times 1 + 1 \times 1 \ldots + 1 \times 1)}_{a \cdot b \text{ times}}$$

לכאורה יש לנו p חוגים שונים.
המקרה הראשון הוא אם החוג איזומורפי לחוג עם חיבור מודולו p וכפל האפס שבו תמיד $x \odot y = 0$ (ז"א, $1 \cdot 1 = 0$), וזה נורא טריוויאלי ומשעמם וסיימנו.
אחרת, נוכיח שכל $p - 1$ החוגים האחרים איזומורפיים לחוג הרגיל ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ עם חיבור וכפל מודולו p (של הנציגים).
נסמן: $1 \times 1 = n$. הכפל הזה עדיין מקיים את תכונות החוגים שאנחנו מכירים, עם יחידה n^{-1} (ההופכי של n ביחס לכפל הרגיל $\cdot$).
למעשה, הכפל הזה הוא: $a \times b = n \cdot a \cdot b$, כאשר $\cdot$ הוא הכפל הרגיל ב־${}^{\mathbb{Z}}/_{p\mathbb{Z}}$.
אזי נבנה איזומורפיזם בין R, החוג ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ עם הכפל המוזר הזה, לבין ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ עם הכפל הרגיל:

$$\psi : \mathbb{Z} \to R, \quad \psi(k) = n^{-1} \cdot k$$

זהו הומומורפיזם של חוגים:

$$\psi(a + b) = n^{-1} \cdot (a + b) = n^{-1} \cdot a + n^{-1} \cdot b = \psi(a) + \psi(b)$$

$$\psi(a \cdot b) = n^{-1} \cdot (a \cdot b) = n \cdot n^{-2} \cdot (a \cdot b) = n \cdot \left(\left[n^{-1} \cdot a\right] \cdot \left[n^{-1} \cdot b\right]\right) = \left[n^{-1} \cdot a\right] \times \left[n^{-1} \cdot b\right] = \psi(a) \cdot \psi(b)$$

$$\psi(1) = n^{-1} = 1_R$$

יש לו הומומורפיזם הופכי:

$$\tilde{\psi} : R \to \mathbb{Z}, \quad \tilde{\psi}(k) = n \cdot k$$

שגם הוא הומומורפיזם, כמו לעיל. נבדוק מהו הגרעין:

$$\psi(x) = 0 \iff \underbrace{1_R + 1_R + \ldots + 1_R}_{x \text{ times}} = 0 \iff p | x$$

ולכן הגרעין הוא $p\mathbb{Z}$. לפי משפט האיזומורפיזם הראשון,

$${}^{\mathbb{Z}}/_{p\mathbb{Z}} \cong R$$

עם הכפל הרגיל ב־${}^{\mathbb{Z}}/_{p\mathbb{Z}}$.

■

2 תרגיל

הוכיחו שתת–הקבוצות הבאות הן אידאלים.

1. יהיו R_1, R_2 חוגים, ויהיו $I_i \triangleleft R_i$ אידאלים. הוכיחו $I_1 \times I_2 \triangleleft R_1 \times R_2$.
2. יהי R חוג. הוכיחו $I = \left\{ f \in R\left[x\right] \middle| f\left(212\right) = 0 \right\} \triangleleft R\left[x\right]$. מה יקרה אם נדרוש $f\left(212\right) = 1$ במקום?
3. נסמן:

$$I = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \quad J = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

$a, b \in \mathbb{Q}$. הוכיחו ש–$I \leq_l M_2\left(\mathbb{Q}\right)$ אידאל שמאלי ו–$J \leq_r M_2\left(\mathbb{Q}\right)$ אידאל ימני. הוכיחו כי $I \bigcap J$ אינו אידאל.

פתרון.

1. יהיו $\left(i_1, i_2\right) \in I_1 \times I_2, \left(r_1, r_2\right) \in R_1 \times R_2$. אזי:

$$\left(r_1, r_2\right) \cdot \left(i_1, i_2\right) = \left(r_1 i_1, r_2 i_2\right) \in I_1 \times I_2$$

לפי כך ש–I_1, I_2 אידאלים ולכן בולעים כפל משמאל. בדומה גם:

$$\left(i_1, i_2\right) \cdot \left(r_1, r_2\right) = \left(i_1 r_1, i_2 r_2\right) \in I_1 \times I_2$$

לפי כך ש–I_1, I_2 אידאלים ולכן בולעים כפל מימין. בסה"כ, $I_1 \times I_2$ אידאל.

2. יהי $r\left(x\right) \in R\left[x\right]$, $i\left(x\right) \in I$. אזי

$$\left(r \cdot i\right)\left(212\right) = r\left(212\right) \cdot i\left(212\right) = i\left(212\right) = 0 = i\left(212\right) = i\left(212\right) \cdot r\left(212\right) = \left(i \cdot r\right)\left(212\right)$$

מותר היה לנו לבצע את המעברים של הכפלה ב–r שכן כל דבר כפול 0 הוא 0.
אם היינו דורשים $f\left(212\right) = 1$ לא היינו מקבלים אידאל.
לדוגמה, בחוג $\mathbb{C}\left[x\right]$, $f\left(x\right) = x - 211 \in I$, אבל $i\left(x\right) \cdot f\left(212\right) = i\left(x\right) \neq 1$, וזהו איננו אידאל.

3. נוכיח:

$$\begin{pmatrix} x & y \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ax + by & 0 \\ ac + bd & 0 \end{pmatrix} \in I$$

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ c & d \end{pmatrix} = \begin{pmatrix} ax + bc & ay + bd \\ 0 & 0 \end{pmatrix} \in J$$

אבל! רק איברים מהצורה $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ נמצאים ב–$I \bigcap J$, ולכן:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ c & d \end{pmatrix} = \begin{pmatrix} ax & ay \\ 0 & 0 \end{pmatrix} \notin I \bigcap J \quad \begin{pmatrix} x & y \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ax & 0 \\ ac & 0 \end{pmatrix} \notin I \bigcap J$$

■

3 תרגיל

הפריכו את הטענות הבאות:

1. איחוד אידאלים הוא אידאל.
2. יהיו $S \subseteq R$ חוגים, ויהי $I \triangleleft S$. אזי $I \triangleleft R$.
3. יהי R חוג. אזי תת–החוג הבא הוא אידאל של $R \times R$:

$$\Delta = \left\{ (r,r) \middle| r \in R \right\} \subset R \times R$$

פתרון.

1. $3\mathbb{Z}, 2\mathbb{Z}$ הם אידאלים של $\mathbb{Z}$. האיחוד הוא $2\mathbb{Z} \bigcup 3\mathbb{Z} = \left\{ z \in \mathbb{Z} \middle| 2|z \vee 3|z \right\}$. אבל $2 + 3 = 5 \notin 2\mathbb{Z} \bigcup 3\mathbb{Z}$, בסתירה לכך שאידאל הוא תת–חבורה חיבורית.
2. ניקח את $\mathbb{R} \triangleleft \mathbb{R}$. אבל $\mathbb{R} \subseteq \mathbb{C}$, $\mathbb{R} \not\triangleleft \mathbb{C}$ שכן $i \cdot r \notin \mathbb{R}$, כאשר i הוא היחידה הקומפלכסית.
3. ניקח את $R = \mathbb{C}$. אזי

$$(1,i) \cdot (1,1) = (1,i) \notin \Delta$$

■

4 תרגיל

נסמן $R = M_2 \left(\mathbb{Z}/2\mathbb{Z}\right)$.

1. מצאו את ההומומורפיזם היחיד של חוגים $\varphi : \mathbb{Z} \to R$.
2. מצאו כמה הומומורפיזמים של חוגים $\psi : \mathbb{Z}\left[\sqrt[3]{2}\right] \to R$ ישנם. רמז: העזרו בסעיף הקודם והראו שהפתרון תלוי רק בתמונה $\psi\left(\sqrt[3]{2}\right)$.

פתרון.

1. יהי הומומורפיזם של חוגים $\varphi : \mathbb{Z} \to R$. אזי

$$\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_R, \varphi(2) = 2\varphi(1) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

כעת:

$$\varphi(2n) = \varphi(2) \cdot \varphi(n) = 0, \varphi(2n+1) = \varphi(2) \cdot \varphi(n) + \varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_R$$

ולכן זהו ההומומורפיזם היחיד. נראה שזהו הומומורפיזם של חוגים:
היחידה נשלחת ליחידה.
החיבור והכפל נשמרים שכן מכפלה וחיבור של מספרים (אי זוגיים וזוגיים) (זוגיים ואי זוגיים) היא (אי זוגית) ומכפלה וחיבור של מספרים (אי זוגיים ואי זוגיים) (זוגיים וזוגיים) היא (זוגית).

2. לפי הסעיף הקודם אנחנו יודעים לאן איברי $\mathbb{Z}$ נשלחים. נבדוק לאן "ההרחבה" נשלחת:

$$\psi\left(\sqrt[3]{2}\right) = A \quad \psi\left(\sqrt[3]{2^2 = 4}\right) = A^2 \quad \psi\left(\sqrt[3]{2^3} = 8\right) = A^3 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

לכן אנו רק צריכים למצוא את המטריצות $A \in M_2\left(\mathbb{Z}/2\mathbb{Z}\right)$ הנילפוטנטיות מסדר 3. אם כן:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = A^3 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^3 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

אלו הן נילפוטנטיות, לפי בדיקה ישירה:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

■

5 תרגיל

הוכיחו שהדרישה לאבליות של החבורה החיבורית של חוג היא מיותרת. כלומר שניתן להסיק אותה משאר האקסיומות של חוג.

פתרון

נוכיח. יהיו $a, b \in R$.

$$0 = 0 \cdot a = (1-1) \cdot a = 1 \cdot a + -1 \cdot a = a + -1 \cdot a$$

ולכן $-a = -1 \cdot a$ (כי ההופכי יחיד בחבורה). ניעזר בכך:

$$a + b - a - b = 1 \cdot (a+b) - 1 \cdot (a+b) = (1-1) \cdot (a+b) = 0 \cdot (a+b) = 0$$

והחבורה החיבורית אבלית.

■

6 תרגיל

הוכיחו שכל תחום שלמות סופי הוא שדה.

פתרון.

יהי R תחום שלמות סופי. נרצה להוכיח שהוא גם בעל חילוק. יהי $a \neq 0 \in R$ ונגדיר:

$$l_a : R \to R,\ l_a(x) = ax$$

נתבונן ב–$l_a(x) = 0$. אזי $ax = 0$ ומכך ש–R תחום שלמות סופי נקבל $x = 0$. לכן זוהי פונקציה חח"ע (לכל $a \neq 0 \in R$), ומכאן שהיא על.

לכן לכל $r \in R$ יש הופכי מימין, אם נסתכל על $l_r(x) = 1$. זהו תחום שלמות (הכפל קומוטטיבי), ולכן כל איבר הפיך. תחום שלמות בו כל איבר הפיך הוא שדה.

■

7 שאלה

תהי X קבוצה. זכרו ש־$\left(P\left(X\right),\triangle,\bigcap\right)$ הוא חוג חילופי. תהי $\phi\neq\tau\subseteq P\left(X\right)$.

1. נאמר ש־τ סגורה לאיחוד אם $A,B\in\tau$ גורר ש־$A\bigcup B\in\tau$. נאמר ש־τ סגורה להכלה אם $A\subseteq B\in\tau$ גורר ש־$A\in\tau$. הוכיחו כי τ אידאל אם ורק אם τ סגורה לאיחוד ולהכלה.
2. נניח ש־X סופית. הוכיחו ש־τ אידאל אם ורק אם קיים $C\subseteq X$ כך ש־$\tau=P\left(C\right)$.
3. מצאו אידאל τ של $\left(P\left(\mathbb{N}\right),\triangle,\bigcap\right)$ שאיננו מן הצורה $P\left(C\right)$.

פתרון.

1. יהי τ אידאל. יהיו $A,B\in\tau$. אזי גם $A\bigcap B\in\tau$ לפי כך ש־τ אידאל ובולע כפל. τ הוא גם תת־חבורה חיבורית של החוג, ולכן גם $A\triangle B\in\tau$. מכאן שגם $\left(A\triangle B\right)\triangle\left(A\bigcap B\right)\in\tau$. אבל:

$$\left(A\triangle B\right)\triangle\left(A\bigcap B\right)=\left(\left(A\bigcup B\right)\setminus\left(A\bigcap B\right)\right)\triangle\left(A\bigcap B\right)=$$

$$=\left[\left(\left(A\bigcup B\right)\setminus\left(A\bigcap B\right)\right)\bigcup\left(A\bigcap B\right)\right]\setminus\underbrace{\left[\left(\left(A\bigcup B\right)\setminus\left(A\bigcap B\right)\right)\bigcap\left(A\bigcap B\right)\right]}_{=\phi}=A\bigcup B$$

ולכן τ סגורה לאיחוד. כעת יהיו $A\subseteq B\in\tau$. אזי גם $A\bigcap B\in\tau$ לפי כך ש־τ אידאל ובולע כפל. אבל $A\bigcap B=A\in\tau$.
לכיוון השני, תהי $\phi\neq\tau\subseteq P\left(X\right)$ סגורה לאיחוד ולהכלה. מכך שהחוג חילופי, מספיק להוכיח אידאל שמאלי, שכן בחוג חילופי כל אידאל הוא דו צדדי. יהי $B\in\tau$, $A\in P\left(X\right)$. ר"ל $A\bigcap B\in\tau$. אבל $A\bigcap B\subseteq B\in\tau$, ולכן $A\bigcap B\in\tau$.

2. אם קיים $C\subseteq X$ כך ש־$\tau=P\left(C\right)$, אזי τ סגורה לאיחוד והכלה. איחוד– כי אם $A,B\in\tau$, אזי $A,B\subseteq C$ (מוכלות ולא שייכות!) ולכן גם $A\bigcup B\subseteq C$ ואזי $A\bigcup B\in\tau$, והכלה– כי אם $A\subseteq B\in\tau$, אזי $A\subseteq B\subseteq C$ ולכן גם $A\subseteq C$ ואזי $A\in\tau$.

לכיוון השני, ניעזר בכך ש־X סופית ו־τ סגורה לאיחוד ולהכלה. מכך ש־X סופית, גם $P\left(X\right)$ סופית ולכן גם τ סופית. בפרט ב־τ יש מספר סופי של קבוצות שכל אחת מהן סופית כתת־קבוצה של X.
נבחר $C=\bigcup\limits_{A\in\tau}A$. זהו איחוד סופי של קבוצות מ־τ, ולכן באינדוקציה על סגירות להכלה גם $C\in\tau$.
נראה ש־$\tau=P\left(C\right)$. יהי $A\in P\left(C\right)$. בפרט $A\subseteq C$. אבל $C\in\tau$, ו־τ סגורה להכלה. לכן גם $A\in\tau$.
יהי $A\in\tau$. אזי בפרט $A\subseteq C$, ולכן $A\in P\left(C\right)$.

3. ניקח את $\tau=\left\{A\in P\left(\mathbb{N}\right)\,\middle|\,\left|A\right|<\aleph_0\right\}$. מכך שאיחוד של קבוצות סופיות הוא סופי וקבוצה שמוכלת בקבוצה סופית היא סופית, נקבל ש־τ אידאל לפי סעיף 1.
נשים לב שניתן לבנות פונקציה על מ־τ ל־$\mathbb{N}$ ע"י התאמת עצמת קבוצה ששייכת ל־τ למספר טבעי ב־$\mathbb{N}$, ולכן $\left|\tau\right|\geq\aleph_0$.
כעת נניח שיש $C\subseteq\mathbb{N}$ כך ש־$\tau=P\left(C\right)$.
נשים לב ש־$\left\{n\right\}\in\tau$ לכל n טבעי לפי הבנייה של τ, ולכן $\left\{n\right\}\in P\left(C\right)$ ולכן $n\in C$ לכל n טבעי, ומכאן $\mathbb{N}\subseteq C$. לכן $C=\mathbb{N}$, ולכן $\left|\tau\right|=\left|P\left(C\right)\right|=2^{\aleph_0}=\aleph$, בסתירה.

■

שתי השאלות הבאות הן בסגנון דומה. נסו לפתור את זו שנראית לכם יותר מעניינת, ואז בדקו האם השאלה האחרת נראית לכם קלה יותר.

8 תרגיל

יהי R חוג בלי יחידה, ויהי $I \leq_l R$ אידאל שמאלי. נסמן $I^+ = \left\{x \in R \middle| xR \subseteq I\right\}$.

1. הוכיחו כי I^+ אידאל דו–צדדי.
2. הוכיחו כי אם $I \triangleleft R$, אזי $I \subseteq I^+$.
3. הוכיחו שאם R חוג עם יחידה, אזי $I^{++} = I^+$.

פתרון

1. יהי $r \in R$, $i^+ \in I^+$. אזי צ"ל $(r \cdot i^+) R \subseteq I$. מתקיים $(r \cdot i^+) R = r \cdot (i^+ R) \underbrace{\subseteq}_{1} r \cdot I \underbrace{\subseteq}_{2} I$, לפי כך ש–$i^+ \in I^+$ (1), ו–I אידאל שמאלי (2).
לכיוון השני, מתקיים $(i^+ \cdot r) R = i^+ \cdot (rR) \underbrace{\subseteq}_{1} i^+ \cdot R \underbrace{\subseteq}_{2} I$, לפי כך ש–$R$ חבורה–למחצה ביחס לכפל (1), ו–$i^+ \in I^+$ (2).
2. נניח $I \triangleleft R$. יהי $i \in I$. אזי $iR \subseteq I$ שכן I אידאל ובפרט בולע כפל מימין. לכן, $i \in I^+$.
3. נניח R חוג עם יחידה. יהי $i^+ \in I^+$. ר"ל $i^+ \cdot R \subseteq I^+$. זה מתקיים שכן I^+ אידאל ובפרט בולע כפל מימין.
יהי $i^{++} \in I^{++}$. אזי $i^{++} \cdot R \subseteq I^+$. בפרט מתקיים $i^{++} \cdot 1 = i^{++} \in I^+$.

■

9 תרגיל

יהי R חוג, ותהי $A \subseteq R$ תת־קבוצה. נגדיר את המאפס השמאלי של A להיות:

$$\mathrm{Ann}_l(A) = \left\{x \in R \middle| \forall a \in A, xa = 0\right\}$$

1. הוכיחו כי $\mathrm{Ann}_l(A) \leq_l R$ אידאל שמאלי.
2. הוכיחו שאם $A \leq_l R$, אזי $\mathrm{Ann}_l(A) \triangleleft R$.
3. נניח $A, B \subseteq R$ תת–קבוצות המכילות את 0. הוכיחו כי $\mathrm{Ann}_l(A+B) = \mathrm{Ann}_l(A) \bigcap \mathrm{Ann}_l(B)$.

פתרון.

1. יהיו $r \in R$, $a \in \mathrm{Ann}_l(A)$. ר"ל $r \cdot a \in \mathrm{Ann}_l(A)$, ז"א לכל $a' \in A$, $(r \cdot a) \cdot a' = 0$.
אבל לפי האסוציאטיביות של הכפל נקבל $(r \cdot a) \cdot a' = r \cdot (a \cdot a') = r \cdot 0 = 0$.
2. נניח $A \leq_l R$. יהיו $r \in R$, $a \in \mathrm{Ann}_l(A)$. מסעיף 1 מ"ל כי $\mathrm{Ann}_l(A)$ אידאל ימני. ז"א מ"ל $a \cdot r \in \mathrm{Ann}_l(A)$. ז"א לכל $a' \in A$, $(a \cdot r) \cdot a' = 0$.
אבל לפי האסוציאטיביות של הכפל נקבל $(a \cdot r) \cdot a' = a \cdot (r \cdot a')$. A אידאל שמאלי, ולכן $(r \cdot a') \in A$. אבל $a \in \mathrm{Ann}_l(A)$, ולכן $a \cdot (r \cdot a') = 0$.
3. נניח $A, B \subseteq R$ תת–קבוצות המכילות את 0.
יהיו $b \in B$, $a \in A$, $c \in \mathrm{Ann}_l(A+B)$. אזי:

$$c \cdot \underbrace{(0+b)}_{\in A+B} = c \cdot b = 0 \quad c \cdot \underbrace{(a+0)}_{\in A+B} = c \cdot a = 0$$

ולכן $c \in \mathrm{Ann}_l(A) \bigcap \mathrm{Ann}_l(B)$.
לכיוון השני, אם $d \in A+B$, $c \in \mathrm{Ann}_l(A) \bigcap \mathrm{Ann}_l(B)$, אזי $d = a + b$ עבור איזשהם $a \in A, b \in B$, ולכן לפי דיסטריבוטיביות הכפל נקבל:

$$c \cdot d = c \cdot (a+b) = c \cdot a + c \cdot b = 0 + 0 = 0$$

■