מבוא לחוגים ומודולים – תרגיל 2

אילאי לוינגט וירין כהן.

מתרגל: תומר באואר.

שאלה 1

א. ראינו בתורת החבורות שהחבורה היחידה מסדר p היא $\mathbb{Z}_p$, ולכן החוג שלנו הוא $\mathbb{Z}_p$ עם חיבור מודולו p.
אפשרות אחת: הכפל הוא כפל האפס, שמהווה חוג (ברור).
כעת נניח שהכפל הוא לא כפל האפס. נסמן אותו ב-×, ואת הכפל הרגיל ב-·.
לכל $a, b \in R$ מתקיים:

$$a \times b = \underbrace{(1+1+\cdots+1)}_{\text{a } times} \times \underbrace{(1+1+\cdots+1)}_{\text{b } times} = \underbrace{(1\times 1+1\times 1+\cdots+1\times 1)}_{\text{a·b } times}$$

כאשר 1 הוא האיבר המתאים ל-$1 \in \mathbb{Z}_p$. לכן זה מוגדר באופן יחיד על ידי 1×1.
אם $1 \times 1 = 0$ זה כפל האפס. אחרת, $1 \times 1 = n$. אזי מתקיים: $a \times b = n \cdot a \cdot b$. נשים לב שהכפל קומוטטיבי.
הכפל אכן אסוציאטיבי, סגור ומקיים את חוק הפילוג. לכן זה אכן משרה חוג בלי יחידה.
כמו כן, איבר היחידה של הכפל הוא n^{-1} (ההופכי ביחס לכפל הרגיל, שקיים מכיוון ש-$\mathbb{Z}_p$ הוא שדה): $a \times n^{-1} = n \cdot a \cdot n^{-1} = a$.
כעת נבנה איזומורפיזם בין החוג R לבין $\mathbb{Z}_p$: נגדיר: $\psi: \mathbb{Z}_p \to R$ על ידי: $\psi(k) = n^{-1} \cdot k$.
זה הומומורפיזם של חוגים:

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

נוכיח שהוא על: יהי $a \in R$. אזי $\psi(n \cdot a) = n^{-1} \cdot n \cdot a = a$.
מכיוון שהקבוצות סופיות ובעלות אותו מספר איברים, הוא גם חח"ע.
לכן זה איזומורפיזם: $\mathbb{Z}_p \cong R$.

ב. דוגמאות לחוגים מסדר p^2:

- $\mathbb{Z}_p \times \mathbb{Z}_p$ עם החיבור והכפל הרגילים.
- $\mathbb{Z}_{p^2}$ עם החיבור והכפל הרגילים.

לא מצאנו את השניים הנוספים. אם תוכלו, תרשמו באתר.

שאלה 2

א. הוכחנו בחבורות שמכפלה קרטזית היא תת-חבורה.
יהיו $(y_1, y_2) \in R_1 \times R_2$, $(x_1, x_2) \in I_1 \times I_2$. אזי, מכיוון ש-$I_1, I_2$ אידיאלים:
$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2) \in I_1 \times I_2$$
בליעה משמאל – באופן דומה.

ב. $I = \{f \in R[x] | f(212) = 0\}$

- נראה שזה תת-חבורה חיבורית:
ברור: $0_{R[x]} = 0 \in I$.
סגירות לחיבור: יהיו $f, g \in I$. אזי:
$$(f+g)(212) = f(212) + g(212) = 0 + 0 = 0$$
ולכן $f + g \in I$.
- נראה בליעה מימין: יהי $f \in I, g \in R[x]$. אזי:
$$(f \cdot g)(212) = f(212) \cdot g(212) = 0 \cdot g(212) = 0$$
ולכן $f \cdot g \in I$.
בליעה משמאל – באופן דומה.

לכן I הוא אידיאל.

- אם נדרוש $f(212) = 1$ במקום, I לא תהיה סגורה לחיבור, כי אם $f, g \in I$, אזי $(f+g)(212) = f(212) + g(212) = 1 + 1 = 2 \neq 1$.

ג. ברור שאלה תת-חבורות חיבוריות, שכן הן מכילות את מטריצת האפס והן סגורות לחיבור.

- נוכיח ש-I אידיאל שמאלי.
יהיו $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in I$, $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(\mathbb{Q})$. אזי:
$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} xa + yb & 0 \\ za + wb & 0 \end{pmatrix} \in I$$
- נוכיח ש-J אידיאל ימני.
יהיו $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in J$, $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(\mathbb{Q})$. אזי:
$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + bz & az + bw \\ 0 & 0 \end{pmatrix} \in J$$
- $I \cap J = \{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} | a \in \mathbb{Q}\}$. נוכיח שזה לא אידיאל.
$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Q})$, $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I \cap J$, אבל: $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \notin \mathrm{I} \cap \mathrm{J}$.
לכן אין בליעה מימין, ולכן הוא לא אידיאל.

שאלה 3

א. הוכחנו ש-$2\mathbb{Z}, 3\mathbb{Z}$ אידיאלים של $\mathbb{Z}$, אבל האיחוד אינו סגור לחיבור, ולכן אינו אידיאל:
$2 \in 2\mathbb{Z}, 3 \in 3\mathbb{Z}$, אבל $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

ב. ניקח $\mathrm{R} = \mathbb{R}, S = \mathbb{Z}, I = 2\mathbb{Z}$. ראינו ש-$I$ אידיאל של S. הוכחנו שמכיוון ש-$\mathbb{R}$ שדה, כל האידיאלים שלו טריוויאליים, לכן I אינו אידיאל של R.

ג. ניקח $R = \mathbb{Z}$. אזי $(1,1) \in \Delta, (1,2) \in \mathbb{Z}$ אבל $(1,2) \cdot (1,1) = (1,2) \notin \Delta$. לכן Δ אינו אידיאל של $\mathbb{Z}$.

שאלה 4

א. אם קיים הומומורפיזם, הוא חייב לקיים: $\varphi(1_{\mathbb{Z}}) = 1_R$, כלומר $\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. מסגירות לחיבור ולהופכי, הוא חייב לקיים, לכל $k \in \mathbb{Z}$: $\varphi(k) = \begin{pmatrix} k(mod\ 2) & 0 \\ 0 & k(mod\ 2) \end{pmatrix}$. לכן זה מגדיר הומומורפיזם יחיד. נותר להוכיח שהוא אכן הומומורפיזם:

- מעביר יחידה ליחידה – מההגדרה.
- סגור לחיבור – מההגדרה.
- סגור לכפל:

$$\varphi(a)\varphi(b) = \begin{pmatrix} a(mod\ 2) & 0 \\ 0 & a(mod\ 2) \end{pmatrix}\begin{pmatrix} b(mod\ 2) & 0 \\ 0 & b(mod\ 2) \end{pmatrix}$$

$$= \begin{pmatrix} ab(mod\ 2) & 0 \\ 0 & ab(mod\ 2) \end{pmatrix} = \varphi(ab)$$

ב. ראשית, נשים לב שכל פולינום ב-$\mathbb{Z}[\sqrt[3]{2}]$ הוא מהצורה: $a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2$, מכיוון שחזקות יותר גבוהות ניתן להכניס באחד המקדמים האלה.
בדומה לסעיף א', מכיוון שהומומורפיזם כזה שולח יחידה ליחידה, הוא חייב לקיים:
$\psi(k) = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$
מסגירות לחיבור וכפל, הומומורפיזם כזה חייב לקיים:

$$\psi\left(a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2\right) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\psi(\sqrt[3]{2}) + \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}\left(\psi(\sqrt[3]{2})\right)^2$$

ולכן הפתרון תלוי רק בתמונה $\psi(\sqrt[3]{2})$.

נשים לב ש-$2 = \left(\sqrt[3]{2}\right)^3$, ולכן:

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

מבדיקה ידנית, נובע שהמטריצות היחידות שמקיימות $M^3 = 0$ הן:

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

נותר לבדוק האם הם הומומורפיזמים. הם שומרים על יחידה מהבנייה.

1. $\psi\left(a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2\right) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$
   - סגירות לחיבור:

$$\psi\left(a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2\right) + \psi\left(x + y\sqrt[3]{2} + z\left(\sqrt[3]{2}\right)^2\right) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

$$= \begin{pmatrix} a + x & 0 \\ 0 & a + x \end{pmatrix} = \psi\left(a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 + x + y\sqrt[3]{2} + z\left(\sqrt[3]{2}\right)^2\right)$$

- סגירות לכפל:

$$\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)\cdot\psi\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)=\begin{pmatrix}a&0\\0&a\end{pmatrix}\begin{pmatrix}x&0\\0&x\end{pmatrix}=\begin{pmatrix}ax&0\\0&ax\end{pmatrix}$$

$$\psi\left(\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)\right)$$

$$=\psi\left(ax+2bz+2cy+(ay+bx+2cz)\sqrt[3]{2}+(az+cx+by)\left(\sqrt[3]{2}\right)^2\right)$$

$$=\begin{pmatrix}(ax+2bz+2cy)(mod\ 2)&0\\0&(ax+2bz+2cy)(mod\ 2)\end{pmatrix}=\begin{pmatrix}ax&0\\0&ax\end{pmatrix}$$

$$=\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)\cdot\psi\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)$$

ולכן זה הומומורפיזם.

2. $\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)=\begin{pmatrix}a&b\\0&a\end{pmatrix}$

- סגירות לחיבור:

$$\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)+\psi\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)=\begin{pmatrix}a&b\\0&a\end{pmatrix}+\begin{pmatrix}x&y\\0&x\end{pmatrix}$$

$$=\begin{pmatrix}a+x&b+y\\0&a+x\end{pmatrix}=\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2+x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)$$

- סגירות לכפל:

$$\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)\cdot\psi\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)=\begin{pmatrix}a&b\\0&a\end{pmatrix}\begin{pmatrix}x&y\\0&x\end{pmatrix}=\begin{pmatrix}ax&ay+bx\\0&ax\end{pmatrix}$$

$$\psi\left(\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)\right)$$

$$=\psi\left(ax+2bz+2cy+(ay+bx+2cz)\sqrt[3]{2}+(az+cx+by)\left(\sqrt[3]{2}\right)^2\right)$$

$$=\begin{pmatrix}(ax+2bz+2cy)(mod\ 2)&(ay+bx+2cz)(mod\ 2)\\0&(ax+2bz+2cy)(mod\ 2)\end{pmatrix}$$

$$=\begin{pmatrix}ax&ay+bx\\0&ax\end{pmatrix}=\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)\cdot\psi\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)$$

ולכן זה הומומורפיזם.

3. זה דומה מאוד לסעיף 2. הוא גם הומומורפיזם.

4. $\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)=\begin{pmatrix}a+b & b\\ b & a+b\end{pmatrix}$

- סגירות לחיבור:

$$\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)+\psi\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)=\begin{pmatrix}a+b & b\\ b & a+b\end{pmatrix}+\begin{pmatrix}x+y & y\\ y & x+y\end{pmatrix}$$
$$=\begin{pmatrix}a+x+b+y & b+y\\ b+y & a+x+b+y\end{pmatrix}$$
$$=\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2+x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)$$

- סגירות לכפל:

$$\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)\cdot\psi\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)=\begin{pmatrix}a+b & b\\ b & a+b\end{pmatrix}\begin{pmatrix}x+y & y\\ y & x+y\end{pmatrix}$$
$$=\begin{pmatrix}ax+ay+bx & ay+bx\\ ay+bx & ax+ay+bx\end{pmatrix}$$

$$\psi\left(\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)\right)$$

$$=\psi\left(ax+2bz+2cy+(ay+bx+2cz)\sqrt[3]{2}+(az+cx+by)\left(\sqrt[3]{2}\right)^2\right)$$

$$=\begin{pmatrix}(ax+2bz+2cy+ay+bx+2cz)(mod\ 2) & (ay+bx+2cz)(mod\ 2)\\ (ay+bx+2cz)(mod\ 2) & (ax+2bz+2cy+ay+bx+2cz)(mod\ 2)\end{pmatrix}$$

$$=\begin{pmatrix}ax+ay+bx & ay+bx\\ ay+bx & ax+ay+bx\end{pmatrix}=\psi\left(a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\right)\cdot\psi\left(x+y\sqrt[3]{2}+z\left(\sqrt[3]{2}\right)^2\right)$$

ולכן זה הומומורפיזם.

ג. מבין ההומומורפיזמים מהסעיפים הקודמים אין אפימורפיזם, מכיוון שלא ניתן להציג את המטריצה $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$ כתמונה של אף אחד מההומומורפיזמים. (בכולם צריכים להיות אותם איברים על האלכסון).

שאלה 5

יהי חוג R. נוכיח את האבליות של החבורה החיבורית מתוך התכונות האחרות:

יהיו $a, b \in \mathrm{R}$. אזי מתקיים: $0 = 0 \cdot a = (1-1) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a$

ולכן: $-a = (-1) \cdot a$. לכן מתקיים:

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

ולכן: $a + b = b + a$, ולכן היא אבלית. מש"ל.

שאלה 6

יהי R תחום שלמות סופי. צריך להוכיח שהוא שדה.

יהי $a \in R$. נגדיר: $\ell_a: R \to R$ על ידי: $\ell_a(x) = a \cdot x$. נתבונן בגרעין. מכיוון ש-R תחום שלמות:

$$x \in Ker(\ell_a) \Leftrightarrow ax = 0 \Leftrightarrow x = 0$$

לכן ℓ_a חח"ע, ומכיוון ש-R סופי היא גם על.

לכן קיים $y \in R$ כך ש-$ay = 1$, כלומר a הפיך מימין.

באופן דומה, בעזרת $r_a = xa$ נקבל ש-a הפיך משמאל.

לכן a הפיך. מש"ל

שאלה 7

א. $\Leftarrow$ נניח ש-τ אידיאל.

- יהיו $A, B \in \tau$. מתקיים:
$$(A \triangle B) \triangle (A \cap B) = \big((A \cup B) \backslash (A \cap B)\big) \triangle (A \cap B)$$
$$= \Big(\big((A \cup B) \backslash (A \cap B)\big) \cup (A \cap B)\Big) \backslash \Big(\big((A \cup B) \backslash (A \cap B)\big) \cap (A \cap B)\Big)$$
האיבר מימין להפרש הוא קבוצה ריקה, והאיבר משמאל הוא $A \cup B$.
מכיוון ש-τ סגורה להפרשים סימטריים וחיתוכים: $A \cup B \in \tau$.
- יהיו $A \subseteq B \in \tau$. מכיוון ש-τ אידיאל, הוא סגור לחיתוכים ולכן: $A = A \cap B \in \tau$.

$\Rightarrow$ נניח ש-τ סגורה לאיחודים והכלות.

- נוכיח ש-$(\tau, \triangle)$ היא תת-חבורה אבלית. ברור שהיא אבלית.
איבר היחידה: יהי $A \in \tau$ (נתון שהיא לא ריקה). $\emptyset \subseteq A$ ולכן $\emptyset \in \tau$ בגלל שהיא סגורה להכלות.
סגירות ל"חיבור": יהיו $A, B \in \tau$. מכיוון שהיא סגורה לאיחודים: $A \cup B \in \tau$. מכיוון שהיא סגורה להכלות: $A \triangle B \in \tau$, שכן $A \triangle B \subseteq A \cup B$.
סגורה להופכי: ההופכי של כל $A \in \tau$ הוא A, שכן $A \triangle A = \emptyset$.

- בליעה: בגלל שהחוג חילופי, מספיק להוכיח בליעה מימין. יהיו $A \in \tau, B \in P(X)$.
החיתוך $A \cap B \subseteq A$. מכיוון שהיא סגורה להכלות, $A \cap B \in \tau$.

ב. $\Leftarrow$ נניח ש-τ אידיאל. נסמן: $C=\bigcup_{A\in\tau}A$. נוכיח: $\tau=P(C)$:

- $\subseteq$ תהי $A\in\tau$. מההגדרה $A\subseteq C$ ולכן $A\in P(C)$.
- $\supseteq$ תהי $A\in P(C)$, כלומר $A\subseteq C$. מכיוון ש-X סופית, גם $P(X)$ סופית, ולכן גם τ סופית. מכיוון ש-C איחוד סופי ו-τ סגורה לאיחודים, $C\in\tau$. מכיוון ש-τ סגורה להכלות, גם $A\in\tau$.

$\Rightarrow$ נניח שקיים $C\subseteq X$ כך ש-$\tau=P(C)$. נשתמש בסעיף א' ונוכיח סגירות לאיחוד והכלה.

- יהיו $A,B\in\tau$, בפרט הן תתי-קבוצות של C. לכן גם $A\cup B\subseteq C$, כלומר $A\cup B\in\tau$.
- יהיו $A\subseteq B\in\tau$. בפרט $B\subseteq C$, ולכן גם $A\subseteq C$, כלומר $A\in P(C)=\tau$.

ג. נבחר: $\tau=\{A\in P(\mathbb{N})\,||A|<\aleph_0\}$.
הוא סגור לאיחוד, מפני שאיחוד קבוצות סופיות הוא סופי.
סגור להכלה כי קבוצה שמוכלת בקבוצה סופית היא סופית.
לכן, לפי סעיף א' היא אידיאל.
נניח בשלילה שיש $C\subseteq\mathbb{N}$ כך ש-$\tau=P(C)$.
מהגדרת τ, לכל $n\in\mathbb{N}$: $\{n\}\in\tau$, ולכן $n\in C$. מכאן, $\mathbb{N}\subseteq C$, ולכן $C=\mathbb{N}$, בפרט $\mathbb{N}\in\tau$,
אך $|\mathbb{N}|=\aleph_0$, בסתירה להגדרת τ.