פתרון תרגיל בית 2 מבוא לחוגים ומודולים
88-212 סמסטר ב' תשפ"א

שאלה 1. נסתכל על החוג $R = M_3(\mathbb{C})$, ובתוכו על ארבע תת-הקבוצות הבאות:

$$\left\{\begin{pmatrix} * & * & * \\ * & * & 0 \\ * & 0 & * \end{pmatrix}\right\}, \quad \left\{\begin{pmatrix} * & * & * \\ 0 & * & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\}, \quad \left\{\begin{pmatrix} * & 0 & * \\ 0 & * & 0 \\ * & 0 & * \end{pmatrix}\right\}, \quad \left\{\begin{pmatrix} * & 0 & * \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix}\right\}.$$

לכל אחת מתת-הקבוצות, קבעו והוכיחו:

- האם היא תת-חוג?
- האם היא תת-חוג בלי יחידה? אם כן, האם יש בה יחידה?
- הראו שאף אחת מתת-הקבוצות האלו אינן אידאל של R מבלי להיעזר בשאלה 8.

(תזכורת: בכל מקום שמופיעה כוכבית אמור להופיע איבר של שדה הבסיס $\mathbb{C}$, והכוכביות לא בהכרח שוות זו לזו. למשל, $\left\{\begin{pmatrix} a & 0 & b \\ 0 & c & 0 \\ 0 & 0 & d \end{pmatrix} \mid a,b,c,d \in \mathbb{C}\right\} = \left\{\begin{pmatrix} * & 0 & * \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix}\right\}$.)

פתרון. ראשית, לפי הגדרתן כל הקבוצות האלו סגורות לחיסור. לכן, על מנת לבדוק האם הן תת-חוג בלי יחידה (או תת-חוג), מספיק לבדוק סגירות לכפל. לאורך הפתרון נסמן על ידי I_3 את מטריצת היחידה מסדר 3×3 מעל $\mathbb{C}$.

$S_1 = \left\{\begin{pmatrix} * & 0 & * \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix}\right\}$: סגורה לכפל, כי

$$\begin{pmatrix} a & 0 & b \\ 0 & c & 0 \\ 0 & 0 & d \end{pmatrix}\begin{pmatrix} e & 0 & f \\ 0 & g & 0 \\ 0 & 0 & h \end{pmatrix} = \begin{pmatrix} ae & 0 & af+bh \\ 0 & cg & 0 \\ 0 & 0 & dh \end{pmatrix}.$$

כמו כן, $I_3 \in S_1$, ולכן זהו תת-חוג. כיוון שהוא מכיל את היחידה, הוא לא יכול להיות אידאל.

$S_2 = \left\{\begin{pmatrix} * & 0 & * \\ 0 & * & 0 \\ * & 0 & * \end{pmatrix}\right\}$: בעצם, אם היינו מחליפים את האינדקסים 2 ו-3, היינו מקבלים שזהו החוג $M_2(\mathbb{C}) \times \mathbb{C}$. עם זאת, ניתן גם לבדוק ישירות שיש סגירות לכפל:

$$\begin{pmatrix} a & 0 & b \\ 0 & c & 0 \\ d & 0 & e \end{pmatrix}\begin{pmatrix} f & 0 & g \\ 0 & h & 0 \\ i & 0 & j \end{pmatrix} = \begin{pmatrix} af+bi & 0 & ag+bj \\ 0 & ch & 0 \\ df+ei & 0 & dg+ej \end{pmatrix}.$$

גם פה $I_3 \in S_2$ ולכן זהו תת-חוג, ומאותו הנימוק כמו S_1 הוא לא יכול להיות אידאל.

$S_3 = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\}$: נראה שזהו תת-חוג בלי יחידה:

$$\begin{pmatrix} a & b & c \\ 0 & d & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} e & f & g \\ 0 & h & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} ae & af+bh & ag \\ 0 & dh & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

הפעם $I_3 \notin S_3$, ולכן זהו תת-חוג בלי יחידה שאינו תת-חוג. נשים לב שגם אין בו יחידה; אכן,

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} e & f & g \\ 0 & h & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

ולכן לא נוכל למצוא מטריצה $\begin{pmatrix} e & f & g \\ 0 & h & 0 \\ 0 & 0 & 0 \end{pmatrix}$ שתהיה יחידה בו. נראה במפורש שזהו אינו אידאל: $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in S_3$ אבל

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \notin S_3.$$

$S_4 = \left\{ \begin{pmatrix} * & * & * \\ * & * & 0 \\ * & 0 & * \end{pmatrix} \right\}$: הוא אינו סגור לכפל, כי

$$\underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}}_{\in S_4} \underbrace{\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{\in S_4} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \notin S_4.$$

לכן הוא לא תת-חוג בלי יחידה, לא תת-חוג, ולא אידאל.

שאלה 2. יהי R חוג, ותהי $S \subseteq R$ תת-קבוצה. הוכיחו כי $C_R(C_R(C_R(S))) = C_R(S)$.
(הדרכה: הראו כי אם $S \subseteq S'$, אז $C_R(S) \supseteq C_R(S')$.)

פתרון. בשלב הראשון, נוכיח את הטענה שבהדרכה: אם $S \subseteq S'$ אז $C_R(S) \supseteq C_R(S')$. אכן, יהי $x \in C_R(S')$. מהגדרת המרכז, $xs = sx$ לכל $s \in S'$. בפרט, זה נכון לכל $s \in S$, ולכן $x \in C_R(S)$.

כעת נעבור להוכחת הטענה. כיוון ש-$S \subseteq C_R(C_R(S))$, לפי טענת העזר שהוכחנו מתקיים $C_R(S) \supseteq C_R(C_R(C_R(S)))$ (פה S משחק בתפקיד עצמו ו-$C_R(C_R(S))$ משחק בתפקיד S').

בכיוון השני, אנחנו יודעים ש-$T \subseteq C_R(C_R(T))$ לכל $T \subseteq R$. ניקח $T = C_R(S)$, ונקבל $C_R(S) \subseteq C_R(C_R(C_R(S)))$.

הראינו הכלה משני הכיוונים, ולכן $C_R(C_R(C_R(S))) = C_R(S)$, כנדרש.

שאלה 3 (רענון הגדרות)**.** יהיו R ו-S חוגים, ויהי $\varphi : R \to S$ הומומורפיזם. הוכיחו את הטענות הבאות:

א. $\varphi(-x) = -\varphi(x)$.

ב. אם x הפיך ב-R, אז $\varphi(x)$ הפיך ב-S.

ג. אם x נילפוטנטי ב-R (כלומר, קיים $n > 0$ כך ש-$x^n = 0$), אז $\varphi(x)$ נילפוטנטי ב-S.

ד. אם φ אפימורפיזם, אז $\varphi(Z(R)) \subseteq Z(S)$.

הוכחה.

א. כיוון ש-φ הומומורפיזם,

$$\varphi(x) + \varphi(-x) = \varphi(x + (-x)) = \varphi(0_R) = 0_S.$$

אך הנגדי לחיבור של כל איבר הוא יחיד, ולכן $\varphi(-x) = -\varphi(x)$.

ב. מכך ש-φ הומומורפיזם של חוגים, אנחנו יודעים ש-$\varphi(1_R) = 1_S$. לכן

$$\varphi(x)\varphi\left(x^{-1}\right) = \varphi\left(xx^{-1}\right) = \varphi(1_R) = 1_S$$

וגם

$$\varphi\left(x^{-1}\right)\varphi(x) = \varphi\left(x^{-1}x\right) = \varphi(1_R) = 1_S$$

ולכן $\varphi(x)$ הפיך, וההופכי שלו הוא $\varphi\left(x^{-1}\right)$.

ג. נניח ש-x נילפוטנטי ב-R. לכן קיים $n > 0$ כך ש-$x^n = 0_R$. כיוון ש-φ מכבד כפל,

$$\varphi(x)^n = \varphi(x^n) = \varphi(0_R) = 0_S$$

ומכאן ש-$\varphi(x)$ נילפוטנטי.

ד. נניח ש-φ אפימורפיזם, ויהי $x \in Z(R)$. צ"ל: $\varphi(x) \in Z(S)$.
יהי $s \in S$. כיוון ש-φ אפימורפיזם, קיים $y \in R$ כך ש-$\varphi(y) = s$. אך $x \in Z(R)$, לכן $xy = yx$, ומכאן

$$\varphi(x)s = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x) = s\varphi(x).$$

הראינו ש-$\varphi(x)$ מתחלף עם כל איבר של S, ולכן $\varphi(x) \in Z(S)$.

□

שאלה 4. נסמן $R = M_2(\mathbb{Z}/2\mathbb{Z})$.

א. מצאו את ההומומורפיזם היחיד של חוגים $\varphi : \mathbb{Z} \to R$.

ב. מצאו את כל ההומומורפיזמים של חוגים $\psi : \mathbb{Z}\left[\sqrt[3]{2}\right] \to R$ (הדרכה: הסבירו מדוע כל הומומורפיזם כזה נקבע על ידי התמונה של $\sqrt[3]{2}$).

ג. ענו במהירות: האם בין ההומומורפיזמים מהסעיף הקודם יש אפימורפיזם?

פתרון. נסמן $\mathbb{Z}/2\mathbb{Z} = \left\{\bar{0}, \bar{1}\right\}$.

א. אנחנו יודעים שבכל הומומורפיזם, $\varphi\left(1_{\mathbb{Z}}\right)=1_{R}$. במקרה שלנו,

$$\varphi\left(1\right)=\begin{pmatrix}\overline{1} & \overline{0}\\ \overline{0} & \overline{1}\end{pmatrix}.$$

מהחיבוריות של φ, לכל $n\in\mathbb{Z}$ יתקיים

$$\varphi\left(n\right)=\begin{pmatrix}\overline{n} & \overline{0}\\ \overline{0} & \overline{n}\end{pmatrix}.$$

במילים אחרות, אם n זוגי אז נקבל את מטריצת האפס, ואם n אי-זוגי נקבל את מטריצת היחידה.

ב. ראשית נזכור כי

$$\mathbb{Z}\left[\sqrt[3]{2}\right]=\left\{a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^{2}\mid a,b,c\in\mathbb{Z}\right\}=\left\{a+b\sqrt[3]{2}+c\sqrt[3]{4}\mid a,b,c\in\mathbb{Z}\right\}.$$

נניח כי $\varphi\left(\sqrt[3]{2}\right)=A$ ידוע לנו. אז לכל $a+b\sqrt[3]{2}+c\sqrt[3]{4}=x\in\mathbb{Z}\left[\sqrt[3]{2}\right]$,

$$\begin{aligned}\varphi\left(x\right)=\varphi\left(a+b\sqrt[3]{2}+c\sqrt[3]{4}\right)=\varphi\left(a\right)+\varphi\left(b\right)\varphi\left(\sqrt[3]{2}\right)+\varphi\left(c\right)\varphi\left(\sqrt[3]{2}\right)^{2}=\\ =\varphi\left(a\right)+\varphi\left(b\right)\cdot A+\varphi\left(c\right)\cdot A^{2}.\end{aligned}$$

לכן ברגע שקבענו מי זה $\varphi\left(\sqrt[3]{2}\right)$ כל φ יוגדר באופן יחיד.
מי יכול להיות $\varphi\left(\sqrt[3]{2}\right)$? כיוון ש-$\varphi$ הומומורפיזם, חייב להתקיים

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

כלומר צריך למצוא את כל המטריצות $A\in M_{2}\left(\mathbb{Z}/2\mathbb{Z}\right)$ המקיימות $A^{3}=0$, וכל מטריצה כזו תגדיר לנו הומומורפיזם (זו לא טענה טריוויאלית, כי צריך לוודא שאין עוד "יחסים" ש-$\sqrt[3]{2}$ מקיים. אבל זה נכון). בחוג הזה אין הרבה מטריצות, אפשר לבדוק ישירות ולמצוא את כל האפשרויות.
למי שזוכר קצת אלגברה לינארית, אפשר להקל עלינו בחיפוש מעט. A היא מטריצה 2×2, לכן אם $A^{3}=0$ בהכרח $A^{2}=0$. הפולינום האופייני שלה הוא $p_{A}\left(x\right)=x^{2}$, אז מתקיים $\operatorname{tr}\left(A\right)=\overline{0}$ (כי זה המקדם של x), והיא צריכה להיות לא הפיכה. אז המטריצות האפשריות הן $\begin{pmatrix}\overline{0} & \overline{0}\\ \overline{0} & \overline{0}\end{pmatrix},\begin{pmatrix}\overline{0} & \overline{1}\\ \overline{0} & \overline{0}\end{pmatrix},\begin{pmatrix}\overline{0} & \overline{0}\\ \overline{1} & \overline{0}\end{pmatrix},\begin{pmatrix}\overline{1} & \overline{1}\\ \overline{1} & \overline{1}\end{pmatrix}$, ולכן יש ארבעה הומומורפיזמים כאלו.

ג. לא. כיוון ש-$\mathbb{Z}\left[\sqrt[3]{2}\right]$ חילופי, אילו היה אפימורפיזם $\psi:\mathbb{Z}\left[\sqrt[3]{2}\right]\to M_{2}\left(\mathbb{Z}/2\mathbb{Z}\right)$, גם $M_{2}\left(\mathbb{Z}/2\mathbb{Z}\right)$ היה חילופי, בסתירה.

שאלה 5. יהי p מספר ראשוני.

א. 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 $x\odot y=0$.

ב. תנו דוגמאות לחוגים עם יחידה מסדר p^{2} שאינם איזומורפיים.
רשות: יש ארבעה כאלו, עד כדי איזומורפיזם. נסו למצוא את כולם.

ג. 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.

א. החבורה החיבורית של R היא מסדר p, ולכן חייבת להיות ציקלית ואיזומורפית ל-$\mathbb{Z}/p\mathbb{Z}$. כעת נותר לקבוע מהו הכפל.
נבחר a יוצר של החבורה החיבורית של R. אם $a^2 = 0$, אז $r_1r_2 = 0$ לכל $r_1, r_2 \in R$.
אכן, אפשר לכתוב $r_1 = m_1a$ ו-$r_2 = m_2a$ לאילושהן $m_1, m_2 \in \mathbb{N}$, ואז

$$r_1r_2 = m_1m_2 \cdot a^2 = m_1m_2 \cdot 0 = 0.$$

נניח $a^2 \neq 0$. אזי $a^2 = ma$ לאיזשהו $1 \leq m \leq p-1$. אם $n = m^{-1} \pmod p$, אז ההעתקה $\varphi : \mathbb{Z}/p\mathbb{Z} \to R$ המוגדרת לפי $\varphi(k + p\mathbb{Z}) = kna$ היא איזומורפיזם.
אכן, היא הומומורפיזם כי

$$\varphi(k + p\mathbb{Z}) + \varphi(k' + p\mathbb{Z}) = (kna) + (k'na) = (k + k')\,na = \varphi((k + k') + p\mathbb{Z})$$
$$\varphi(k + p\mathbb{Z}) \cdot \varphi(k' + p\mathbb{Z}) = (kna) \cdot (k'na) = kk'n^2a^2 = kk'n\,(nm)\,a = kk'na = \varphi(kk' + p\mathbb{Z})$$

(המעבר האחרון נכון מאחר ש-$nm \equiv 1 \pmod p$ וכן $pa = 0$ ב-R). כמו כן, הגרעין שלה הוא בפרט תת-חבורה חיבורית של $\mathbb{Z}/p\mathbb{Z}$; אך הוא לא שווה לכולה, כי $\varphi(1 + p\mathbb{Z}) = na \neq 0$, ולכן φ חח"ע. כיוון ש-φ פונקציה חח"ע בין שתי קבוצות מאותו הגודל, היא גם על. בסך הכל φ איזומורפיזם.

ב. ארבעת החוגים היחידים עד כדי איזומורפיזם מסדר p^2 הם $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})[x] / \langle x^2 \rangle$ ו-$\mathbb{F}_{p^2}$ (השדה עם p^2 איברים).
כיצד לוודא שהם לא איזומורפיים? בכל אחד משלושת החוגים הראשונים יש מחלקי אפס, ולכן אף אחד מהם אינו שדה. זה מראה ש-$\mathbb{F}_{p^2}$ אינו איזומורפי לאף אחד מהם. $\mathbb{Z}/p^2\mathbb{Z}$ אינו איזומורפי ל-$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ול-$(\mathbb{Z}/p\mathbb{Z})[x] / \langle x^2 \rangle$ כי החבורות החיבוריות שלהם לא איזומורפיות; והחוגים $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ו-$(\mathbb{Z}/p\mathbb{Z})[x] / \langle x^2 \rangle$ אינם איזומורפיים כי ב-$(\mathbb{Z}/p\mathbb{Z})[x] / \langle x^2 \rangle$ יש אידאל נילפוטנטי מסדר 2 (אם I הוא האידאל הנוצר על ידי $x + \langle x^2 \rangle$, אז $I^2 = 0$), ואילו ב-$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ אין אידאל כזה (האידאלים היחידים הלא-טריוויאליים הם $\mathbb{Z}/p\mathbb{Z} \times \{0\}$ ו-$\{0\} \times \mathbb{Z}/p\mathbb{Z}$).

שאלה 6. הוכיחו שתת־הקבוצות הבאות הן אידאלים.

א. עבור חוג R, $I = \left\{ \begin{pmatrix} 0 & a_1 & a_2 \\ 0 & 0 & a_3 \\ 0 & 0 & 0 \end{pmatrix} \mid a_i \in R \right\} \lhd \left\{ \begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_4 & a_5 \\ 0 & 0 & a_6 \end{pmatrix} \mid a_i \in R \right\}$.

ב. יהי R חוג. הוכיחו $I = \{f \in R[x] \mid f(212) = 0\} \lhd R[x]$. מה יקרה אם נדרוש $f(212) = 1$ במקום?

ג. נסמן

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}, \qquad J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$$

הוכיחו ש-$I \leq_l M_2(\mathbb{Q})$ אידאל שמאלי ו-$J \leq_r M_2(\mathbb{Q})$ אידאל ימני. הוכיחו כי $I \cap J$ אינו אידאל.

פתרון. א. I היא תת-חבורה חיבורית של חוג המטריצות המשולשיות העליונות S. כדי להוכיח שהיא אידאל, נבדוק בליעה משני הצדדים:

$$\begin{pmatrix}0 & a_1 & a_2\\ 0 & 0 & a_3\\ 0 & 0 & 0\end{pmatrix}\begin{pmatrix}b_1 & b_2 & b_3\\ 0 & b_4 & b_5\\ 0 & 0 & b_6\end{pmatrix}=\begin{pmatrix}0 & a_1b_4 & a_1b_5+a_2b_6\\ 0 & 0 & a_3b_6\\ 0 & 0 & 0\end{pmatrix}$$
$$\begin{pmatrix}b_1 & b_2 & b_3\\ 0 & b_4 & b_5\\ 0 & 0 & b_6\end{pmatrix}\begin{pmatrix}0 & a_1 & a_2\\ 0 & 0 & a_3\\ 0 & 0 & 0\end{pmatrix}=\begin{pmatrix}0 & b_1a_1 & b_1a_2+b_2a_3\\ 0 & 0 & b_4a_3\\ 0 & 0 & 0\end{pmatrix}$$

לכן זהו אידאל.

ב. I הוא תת-חבורה חיבורית של $R\left[x\right]$ כי היא לא ריקה, ואם $f,g\in I$, אז

$$\left(f-g\right)\left(212\right)=f\left(212\right)-g\left(212\right)=0-0=0\ .$$

נראה בליעה משני הצדדים: אם $f\in I$ ו-$g\in R\left[x\right]$,

$$\left(f\cdot g\right)\left(212\right)=f\left(212\right)\cdot g\left(212\right)=0\cdot g\left(212\right)=0$$
$$\left(g\cdot f\right)\left(212\right)=g\left(212\right)\cdot f\left(212\right)=g\left(212\right)\cdot 0=0\ .$$

לכן $f\cdot g,g\cdot f\in I$, ומכאן ש-I אידאל של $R\left[x\right]$.
אם היינו דורשים $f\left(212\right)=1$, זה לא היה אידאל, ואפילו לא תת-חבורה חיבורית (למשל, פולינום האפס לא היה בתוך I).

ג. I ו-J הם תת-חבורות חיבוריות של $M_2\left(\mathbb{Q}\right)$, כי

$$\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}-\begin{pmatrix}a' & b'\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a-a' & b-b'\\ 0 & 0\end{pmatrix}\in I$$

וכן

$$\begin{pmatrix}a & 0\\ b & 0\end{pmatrix}-\begin{pmatrix}a' & 0\\ b' & 0\end{pmatrix}=\begin{pmatrix}a-a' & 0\\ b-b' & 0\end{pmatrix}\in J\ .$$

נראה ש-I אידאל ימני:

$$\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\begin{pmatrix}c & d\\ e & f\end{pmatrix}=\begin{pmatrix}ac+be & ad+bf\\ 0 & 0\end{pmatrix}\in I\ .$$

בדומה, J אידאל שמאלי:

$$\begin{pmatrix}c & d\\ e & f\end{pmatrix}\begin{pmatrix}a & 0\\ b & 0\end{pmatrix}=\begin{pmatrix}ca+db & 0\\ ea+fb & 0\end{pmatrix}\in J\ .$$

החיתוך שלהם הוא $I\cap J=\left\{\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}\mid a\in\mathbb{Q}\right\}$. זו גם תת-חבורה חיבורית, אבל היא לא אידאל, כי אין בליעה מאף צד. למשל,

$$\underbrace{\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}}_{\in I\cap J}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\notin I\cap J\ .$$

שאלה 7. הפריכו את הטענות השגויות הבאות:

א. איחוד אידאלים הוא אידאל.

ב. יהיו $S \subseteq R$ חוגים, ויהי $I \lhd S$. אז $I \lhd R$.

ג. יהי R חוג. אז תת־החוג הבא הוא אידאל של $R \times R$:

$$\Delta = \{(r,r) \mid r \in R\} \subseteq R \times R$$

פתרון. א. ניקח $R = \mathbb{Z}$, $I = 2\mathbb{Z}$, $J = 3\mathbb{Z}$. אז $I, J \lhd R$, אבל $I \cup J \ntriangleleft R$, כי זו אפילו לא תת-חבורה חיבורית. למעשה, $I \cup J$ הוא אידאל של R אם ורק אם $I \subseteq J$ או $J \subseteq I$ (מדוע?).

ב. ניקח $R = \mathbb{Q}$, $S = \mathbb{Z}$, $I = 2\mathbb{Z}$. אנחנו יודעים ש-I הוא אידאל של $\mathbb{Z}$, אבל I אינו אידאל של $\mathbb{Q}$ (כי האידאלים היחידים של $\mathbb{Q}$ הם $\{0\}$ ו-$\mathbb{Q}$).

ג. ניקח $R = \mathbb{Z}$. אז $(1,1) \in \Delta$, אבל $(1,1) \cdot (1,0) = (1,0) \notin \Delta$, ולכן אין בליעה.

שאלה 8. יהי R חוג. בשאלה זו נחקור את המרכז ואת האידאלים של חוג המטריצות מעל R.

א. הראו כי $Z\left(M_n\left(R\right)\right) = Z\left(R\right) I_n$. כלומר, המרכז של $M_n\left(R\right)$ מכיל רק מטריצות סקלריות, שהאיבר באלכסון שלהן הוא מהמרכז של R.

ב. הראו כי אם $I \lhd R$, אז $M_n\left(I\right) \lhd M_n\left(R\right)$.

ג. הראו כי כל אידאל של $M_n\left(R\right)$ הוא מהצורה הנ"ל. כלומר, הראו שאם $J \lhd M_n\left(R\right)$, אז קיים $I \lhd R$ שעבורו $J = M_n\left(I\right)$.

(הדרכה לסעיפים א' ו-ג': היעזרו במטריצות e_{ij} שבהן יש 1 במקום ה-(i,j) ו-0 בכל מקום אחר.)

הוכחה. לאורך הפתרון, e_{ij} יסמן את המטריצה שיש בה 1 במקום ה-(i,j) ו-0 בשאר המקומות. ניתן לבדוק ישירות מהגדרת הכפל שמתקיים $e_{ij}e_{kl} = \delta_{jk}e_{il}$. כמו כן, הקבוצה $\{e_{ij}\}_{i,j=1}^{n}$ מהווה בסיס של $M_n\left(R\right)$, בדיוק במובן של מרחבים וקטוריים – כל מטריצה ניתנת לכתיבה בצורה יחידה באופן $\sum_{i,j=1}^{n} a_{ij}e_{ij}$.

א. תהי $A \in Z\left(M_n\left(R\right)\right)$. נכתוב $A = \sum_{i,j=1}^{n} a_{ij}e_{ij}$. לכן לכל $X \in M_n\left(R\right)$ מתקיים $AX = XA$. נבחר $X = e_{kl}$, ונקבל:

$$Ae_{kl} = \left(\sum_{i,j=1}^{n} a_{ij}e_{ij}\right) e_{kl} = \sum_{i,j=1}^{n} \left(a_{ij}e_{ij}e_{kl}\right) = \sum_{i=1}^{n} a_{ik}e_{il}$$

$$e_{kl}A = e_{kl}\left(\sum_{i,j=1}^{n} a_{ij}e_{ij}\right) = \sum_{i,j=1}^{n} \left(a_{ij}e_{kl}e_{ij}\right) = \sum_{j=1}^{n} a_{lj}e_{kj}$$

כדי שיתקיים שוויון בהכרח $a_{ik} = 0$ לכל $i \neq k$ (כי במקום ה-(i,l) במטריצה הראשונה כתוב a_{ik} ובמטריצה השנייה כתוב 0) ו-$a_{lj} = 0$ לכל $l \neq j$ (בדומה). אם ניקח $(i,j) = (k,l)$ נקבל שבמקום ה-(k,l) במטריצה הראשונה כתוב a_{kk} ובמטריצה השנייה כתוב a_{ll}, ולכן $a_{kk} = a_{ll}$. כיוון שזה נכון לכל k,l, זה מראה שהמטריצה A סקלרית, כנדרש.

ב. נניח $I \lhd R$. נראה ש-$M_n(I)$ תת-חבורה חיבורית: יהיו $A, B \in M_n(I)$, ונכתוב $A = \sum_{i,j=1}^{n} a_{ij} e_{ij}$ ו-$B = \sum_{i,j=1}^{n} b_{ij} e_{ij}$ עבור $a_{ij}, b_{ij} \in I$. אז

$$A - B = \sum_{i,j=1}^{n} (a_{ij} - b_{ij}) e_{ij}$$

היא מטריצה שכל איבריה ב-I, ולכן $A - B \in M_n(I)$.
נראה את תכונת הבליעה. תהי $A = \sum_{i,j=1}^{n} a_{ij} e_{ij} \in M_n(I)$, ותהי $C = \sum_{k,l=1}^{n} c_{kl} e_{kl} \in M_n(R)$ (לכן $a_{ij} \in I$ ו-$c_{kl} \in R$). מכאן

$$A \cdot C = \left(\sum_{i,j=1}^{n} a_{ij} e_{ij}\right) \cdot \left(\sum_{k,l=1}^{n} c_{kl} e_{kl}\right) = \sum_{i,j,k,l=1}^{n} (a_{ij} c_{kl} e_{ij} e_{kl}) = \sum_{i,l=1}^{n} \left(\sum_{j=1}^{n} a_{ij} c_{jl}\right) e_{il}.$$

כל $\sum_{j=1}^{n} a_{ij} c_{jl} \in I$, כי כל $a_{ij} \in I$ והאידאל I מקיים את תכונת הבליעה מימין. בכך הראינו ש-I בולע מימין. ההוכחה לכיוון השני זהה.

ג. יהי $J \lhd M_n(R)$. נגדיר $I = \{a \in R \mid a \cdot e_{11} \in J\}$.

טענה 1. $I \neq \varnothing$. אכן, $0 \in I$.

טענה 2. $I \lhd R$. זו תת-חבורה חיבורית: אם $a, b \in I$, אז $a \cdot e_{11}, b \cdot e_{11} \in J$. לכן גם $(a - b) \cdot e_{11} \in J$, ומכאן $a - b \in I$. נראה את תכונת הבליעה: יהי $a \in I$ ויהי $r \in R$. לכן $a \cdot e_{11} \in J$ ו-$r \cdot e_{11} \in M_n(R)$. כיוון ש-$J$ אידאל,

$$(a \cdot r) e_{11} = (a \cdot e_{11})(r \cdot e_{11}), (r \cdot a) e_{11} = (r \cdot e_{11})(a \cdot e_{11}) \in J$$

ולכן $a \cdot r, r \cdot a \in I$. זה מראה ש-$I$ אידאל.

טענה 3. $M_n(I) \subseteq J$. תהי $\sum_{i,j=1}^{n} a_{ij} e_{ij} \in M_n(I)$; לכן $a_{ij} \in I$ לכל i, j. לפי הגדרת I, $a_{ij} \cdot e_{11} \in J$. כיוון ש-$J$ אידאל, גם

$$e_{i1} \cdot (a_{ij} e_{11}) \cdot e_{1j} = a_{ij} e_{ij} \in J.$$

כיוון ש-J סגור לחיבור, $\sum_{i,j=1}^{n} a_{ij} e_{ij} \in J$.

טענה 4. $J \subseteq M_n(I)$. תהי $A = \sum_{i,j=1}^{n} a_{ij} e_{ij} \in J$. לכן לכל $1 \leq k, l \leq n$, מהבליעה של J נקבל

$$e_{1k} \left(\sum_{i,j=1}^{n} a_{ij} e_{ij}\right) e_{l1} = a_{kl} \cdot e_{11} \in J.$$

לפי הגדרת I, $a_{kl} \in I$ לכל $1 \leq k, l \leq n$. לכן $A \in M_n(I)$, כנדרש. זה מוכיח את הדרוש.

$\square$

שאלה 9.

א. הראו כי אם $R_1, \ldots, R_n$ חוגים ו-$I_j \lhd R_j$ אידאלים, אז $\prod_{j=1}^{n} I_j \lhd \prod_{j=1}^{n} R_j$.

ב. הראו כי אם $R_1, \ldots, R_n$ חוגים, אז כל אידאל של $\prod_{j=1}^{n} R_j$ הוא מהצורה $\prod_{j=1}^{n} I_j$ לאידאלים $I_j \lhd R_j$.

ג. הראו כי טענת הסעיף הקודם אינה נכונה אם מדובר על מכפלה אינסופית.

הוכחה.

א. ראשית, נשים לב ש-$\prod_{j=1}^{n} I_j$ היא תת-חבורה חיבורית: אם $(a_1,\ldots,a_n),(b_1,\ldots,b_n)\in\prod_{j=1}^{n} I_j$, אז

$$(a_1,\ldots,a_n)-(b_1,\ldots,b_n)=(a_1-b_1,\ldots,a_n-b_n)\in\prod_{j=1}^{n} I_j$$

כשהשתמשנו בכך שכל I_j הוא תת-חבורה חיבורית.
נראה את תכונת הבליעה: יהי $(a_1,\ldots,a_n)\in\prod_{j=1}^{n} I_j$ ויהי $(r_1,\ldots,r_n)\in\prod_{j=1}^{n} R_j$. כיוון שכל I_j אידאל, $a_jr_j, r_ja_j\in I_j$ לכל $1\le j\le n$, ולכן

$$(a_1,\ldots,a_n)\cdot(r_1,\ldots,r_n)=(a_1r_1,\ldots,a_nr_n)\in\prod_{j=1}^{n} I_j$$

$$(r_1,\ldots,r_n)\cdot(a_1,\ldots,a_n)=(r_1a_1,\ldots,r_na_n)\in\prod_{j=1}^{n} I_j$$

כנדרש.

ב. יהי $J\lhd\prod_{j=1}^{n} R_j$. לכל $1\le j\le n$ נסמן על ידי e_j את הווקטור שבו 1 במקום ה-j ו-0 בשאר המקומות, ונגדיר $I_j=\{a\in R_j\mid ae_j\in J\}$.
$I_j\lhd R_j$: אכן, זו תת-חבורה חיבורית כי אם $ae_j,be_j\in J$, אז $(a-b)\,e_j\in J$; ומתקיימת תכונת הבליעה כי אם $ae_j\in J$ ו-$r\in R$, אז גם $(ar)\,e_j=(ae_j)\,(re_j)\in J$ ובדומה ל-ra.
מהסגירות לחיבור של J נובע $\prod_{j=1}^{n} I_j\subseteq J$. מצד שני, לכל $(a_1,\ldots,a_n)\in J$ מתקיים $(a_1,\ldots,a_n)\,e_j=a_je_j\in J$, ולכן $a_j\in I_j$. זה מראה את ההכלה בכיוון ההפוך.

ג. נראה שעבור מכפלות אינסופיות הטענה אינה נכונה. בתוך $\prod_{i\in I} R_i$ נסתכל על הסכום הישר $\bigoplus_{i\in I} R_i$ שהוגדר בתרגיל הבית הראשון (תזכורת: בסכום הישר רק מספר סופי של קואורדינטות הוא שונה מ-0). זהו אידאל של המכפלה הישרה (בדקו!), אך הוא לא מכפלה ישרה של אידאלים של R_i.

$\square$

הערה. שימו לב שבשתי השאלות האחרונות השתמשנו במובן חזק בכך שבחוגים שלנו יש יחידה. אילו היינו עובדים עם חוגים ללא יחידה, הטענות היו שגויות. למשל, היה ניתן למצוא חוג בלי יחידה R ואידאל $J\lhd M_n(R)$ שאינו מן הצורה $M_n(I)$ לאף $I\lhd R$.

שאלה 10. תהי X קבוצה. הזכרו ש-$(P(X),\triangle,\cap)$ הוא חוג חילופי. תהי $\varnothing\neq\tau\subseteq P(X)$ תת־קבוצה לא ריקה.

א. נאמר ש-τ סגורה לאיחוד אם $A,B\in\tau$ גורר $A\cup B\in\tau$. נאמר ש-τ סגורה להכלה אם $A\subseteq B\in\tau$ גורר $A\in\tau$. הוכיחו כי τ אידאל אם ורק אם τ סגורה לאיחוד והכלה.

ב. נניח ש-X סופית. הוכיחו ש-τ אידאל אם ורק אם קיים $C\subseteq X$ כך ש-$\tau=P(C)$.

ג. מצאו אידאל τ של $(P(\mathbb{N}),\triangle,\cap)$ שאינו מן הצורה $P(C)$.

פתרון. א. $\boxed{\Leftarrow}$ נניח ש-τ אידאל של $P(X)$. לכל $A,B\in\tau$ מתקיים

$$A\cup B=(A\vartriangle B)\vartriangle(A\cap B)$$

וכיוון ש-τ סגורה לחיבור ולכפל של החוג, $A\cup B\in\tau$. לכן τ סגורה לאיחוד. כדי להראות ש-τ סגורה להכלה, תהי $B\in\tau$ ותהי $A\subseteq B$. לכן $A=A\cap B$, ומהבליעה של τ ביחס לכפל נקבל $A\in\tau$. לכן τ סגורה להכלה.

$\boxed{\Rightarrow}$ נניח ש-τ סגורה לאיחוד ולהכלה. כדי לראות ש-τ תת-חבורה חיבורית, כלומר סגורה לחיסור, יהיו $A,B\in\tau$. החיסור שלהם הוא $A\vartriangle B\subseteq A\cup B$. כיוון ש-$\tau$ סגורה לאיחוד, $A\cup B\in\tau$, ומהסגירות להכלה $A\vartriangle B\in\tau$. כדי לראות בליעה, תהי $A\in\tau$ ותהי $B\in P(X)$. כיוון שהחוג חילופי, מספיק לבדוק בליעה מצד שמאל. אכן, $B\cap A\subseteq A$, ומהסגירות להכלה $B\cap A\in\tau$.

ב. $\boxed{\Leftarrow}$ נניח ש-τ אידאל. ניקח $C=\cup\tau=\bigcup_{A\in\tau}A$. כיוון ש-$X$ סופית, גם $P(X)$ סופית, ולכן τ סופית; זה מראה ש-C היא איחוד של מספר סופי של איברים מ-τ, ולפי הסעיף הקודם – $C\in\tau$. לפי הסגירות להכלה נקבל $P(C)\subseteq\tau$. מצד שני, אם $A\in\tau$ אז $A\subseteq C$ לפי הגדרת C, ולכן $A\in P(C)$. זה מראה ש-$\tau\supseteq P(C)$, ולכן נקבל שוויון.

$\boxed{\Rightarrow}$ הקבוצה $P(C)$ סגורה לאיחוד ולהכלה, ולכן היא אידאל (לפי הסעיף הקודם).

ג. נסתכל בתוך $P(\mathbb{N})$ על אוסף תת-הקבוצות הסופיות $\tau=\{A\subseteq\mathbb{N}\mid|A|<\infty\}$. זהו אוסף שסגור לאיחוד ולהכלה, ולכן לפי סעיף א' זהו אידאל. אך הוא לא מהצורה $P(C)$, (אחרת C הייתה צריכה להכיל כל תת-קבוצה סופית של $\mathbb{N}$, כלומר להיות כל $\mathbb{N}$, אבל $\mathbb{N}\notin\tau$.

בהצלחה!