

פתרון תרגיל בית 3 מבוא לחוגים ומודולים 88-212 סמסטר ב' תשפ"א

שאלה 1. יהי R חוג, ויהיו $I, J, K \triangleleft R$ אידיאלים.

א. הוכיחו $(I \cap J)(I \cap J) \subseteq IJ \subseteq (I \cap J)$.

ב. הוכיחו $I(J + K) = IJ + IK$.

ג. הוכיחו את המודולריות של סריג האידיאלים שהזכרנו בתרגול: אם $I \subseteq K$, אזי
 $I + (J \cap K) = (I + J) \cap K$

פתרון.

א. את ההכלה $IJ \subseteq I \cap J$ ראיתם בהרצאה. עבור ההכלה השנייה, אם $x, y \in I \cap J$ בפרט $x \in J$ ו- $y \in I$, ולכן $xy \in IJ$. כיוון ש- IJ הוא אידיאל, הוא סגור לסכומים סופיים, והטענה נובעת.

ב. \supseteq $IJ, IK \subseteq I(J + K)$ כי $J, K \subseteq J + K$. כיוון שסכום אידיאלים הוא האידיאל המינימלי המכיל את שניהם, נקבל את ההכלה $IJ + IK \subseteq I(J + K)$.
 \subseteq יהי $a \in I(J + K)$. אז אפשר לכתוב $a = \sum_{i=1}^n x_i y_i$ עבור $x_i \in I$ ו- $y_i \in J + K$. לפי הגדרת סכום, לכל $1 \leq i \leq n$ אפשר לכתוב $y_i = j_i + k_i$ עבור $j_i \in J$ ו- $k_i \in K$. בסך הכל $a = \sum_{i=1}^n x_i y_i = \sum_{i=1}^n x_i j_i + \sum_{i=1}^n x_i k_i \in IJ + IK$.

ג. \subseteq נשים לב כי $I \subseteq I + J, K \subseteq I + J$, ולכן $I \subseteq (I + J) \cap K$. בנוסף, $J \cap K \subseteq J \subseteq I + J$ וגם $J \cap K \subseteq K$, ולכן $J \cap K \subseteq (I + J) \cap K$. מהמינימליות של סכום אידיאלים, נקבל את ההכלה.

\supseteq יהי $k \in (I + J) \cap K$. אז אפשר לכתוב $k = i + j$ עבור $i \in I$ ו- $j \in J$. לכן $j = k - i \in K$ כלומר $j \in J \cap K$, ולכן $x \in I + (J \cap K)$.

שאלה 2. יהי $R = \mathbb{Z}[x]$, $I = \langle 2, x \rangle$ ו- $J = \langle 3, x \rangle$. הוכיחו כי $\{ij \mid i \in I, j \in J\}$ אינו אידיאל של R .

הוכחה. נסמן

$$S = \{f \cdot g \mid f \in I, g \in J\}$$

האיברים באידיאלים I ו- J הם מהצורה $f = 2f_1 + xf_2 \in I$, $g = 3g_1 + xg_2 \in J$. אם נבחר $f = 2$, $g = 3$, אז $6 \in S$. אם נבחר $f = g = x$, אז $x^2 \in S$. נוכיח כי $6 + x^2 \notin S$ ולכן S אינה תת-חבורה חיבורית של החוג, ובפרט לא אידיאל. נניח בשלילה כי קיימים $f_1, f_2, g_1, g_2 \in \mathbb{Z}[x]$ ממעלה לכל היותר 2, ובלי הגבלת הכלליות הם קבועים, כך ש-

$$\begin{aligned} (2f_1 + xf_2)(3g_1 + xg_2) &= 6 + x^2 \\ 6f_1g_1 + (2f_1g_2 + 3f_2g_1)x + f_2g_2x^2 &= 6 + x^2 \end{aligned}$$

אז $f_1 g_1 = 1$ (כי הם קבועים) וגם $f_2 g_2 = 1$ (מדוע המעלה שלהם צריכה להיות אפס?). לכן
 אבל אז לא יתכן כי $f_2 = g_2 = \pm 1, f_1 = g_1 = \pm 1$

$$2f_1 g_2 + 3f_2 g_1 = 0$$

במקרה שלנו מכפלת האידיאלים היא $IJ = \langle 6, x \rangle$. נסו להראות כי x אינו יכול להכתב בצורה $x = f \cdot g$ כאשר $f \in I$ ו- $g \in J$.
 □

שאלה 3. יהי R חוג, ויהי $I \triangleleft R$ אידיאל. ראינו כי $M_n(I) \triangleleft M_n(R)$. הוכיחו

$$M_n(R)/M_n(I) \cong M_n(R/I)$$

הוכחה. נגדיר $\varphi : M_n(R) \rightarrow M_n(R/I)$ לפי $\varphi((a_{ij} + I)) = (a_{ij} + I)$ (כלומר מבצעים מודולו I בכל מרכיב בנפרד). נראה כי φ הומומורפיזם:

$$\begin{aligned} \varphi((a_{ij}) + (b_{ij})) &= \varphi((a_{ij} + b_{ij})) = (a_{ij} + b_{ij} + I) = (a_{ij} + I) + (b_{ij} + I) = \\ &= \varphi((a_{ij})) + \varphi((b_{ij})) \\ \varphi((a_{ij}) \cdot (b_{ij})) &= \varphi\left(\left(\sum_{k=1}^n a_{ik} b_{kj}\right)\right) = \left(\sum_{k=1}^n a_{ij} b_{kj} + I\right) = \\ &= \left(\sum_{k=1}^n (a_{ij} + I)(b_{kj} + I)\right) = \left(\sum_{k=1}^n (a_{ij} + I)\right) \left(\sum_{k=1}^n (b_{kj} + I)\right) = \\ &= \varphi((a_{ij})) \cdot \varphi((b_{ij})) \end{aligned}$$

וכן $\varphi(I_n) = I_n$ (כאשר I_n מטריצת היחידה).
 φ על: לכל מטריצה $(a_{ij} + I) \in M_n(R/I)$ מתקיים $(a_{ij} + I) \in \ker \varphi = M_n(I)$

$$A \in \ker \varphi \iff \forall 1 \leq i, j \leq n : \varphi(A)_{ij} = 0 + I \iff \forall 1 \leq i, j \leq n : a_{ij} \in I$$

□ מפה הטענה נובעת לפי משפט האיזומורפיזם הראשון.

שאלה 4. בחוג $R = \mathbb{Z}[x, y]$ נסמן שלושה אידיאלים:

$$I_0 = \langle x, y \rangle, \quad I_1 = \langle x - 1, y - 3 \rangle, \quad I_2 = \langle x - 2, y - 5 \rangle$$

א. הוכיחו שכל שניים מבין האידיאלים הם קו-מקסימליים.

ב. הוכיחו ש- $R/I_1 \cong \mathbb{Z}$ (טענה זו נכונה גם ל- I_0 ול- I_2).

פתרון.

א. I_0 ו- I_1 הם קו-מקסימליים, כי $x - (x - 1) = 1$.
 I_1 ו- I_2 הם קו-מקסימליים, כי $(x - 1) - (x - 2) = 1$.
 לגבי I_0 ו- I_2 : $2 \in I_0 + I_2$, כי $2 = x - (x - 2)$. $5 \in I_0 + I_2$, כי $5 = y - (y - 5)$.
 כעת, $1 \in I_0 + I_2$, כי $1 = 5 - 2 \cdot 2 \in I_0 + I_2$.

ב. נגדיר הומומורפיזם $\varphi : \mathbb{Z}[x, y] \rightarrow \mathbb{Z}$ לפי $\varphi(f(x, y)) = f(1, 3)$.

- φ הומומורפיזם: ישירות מכך שהחיבור והכפל בחוג הפולינומים מתאימים לחיבור וכפל בכל נקודה בנפרד.
- φ על: לכל $a \in \mathbb{Z}$, $\varphi(a) = a$ (כלומר אם לוקחים את הפולינום הקבוע a , הצבת $(1, 3)$ בו תיתן a). לכן φ על.
- $\ker \varphi = I_1$: בכיוון אחד, מחישוב ישיר רואים $\varphi(x-1) = \varphi(y-3) = 0$. לכן $x-1, y-3 \in \ker \varphi$, כלומר $I_1 = \langle x-1, y-3 \rangle \subseteq \ker \varphi$. בכיוון השני, יהי $f(x, y) \in \ker \varphi$. אם נחשוב על $f(x, y)$ כעל פולינום במשתנה y עם מקדמים ב- $\mathbb{Z}[x]$ (כלומר מזהים את $\mathbb{Z}[x, y] = (\mathbb{Z}[x])[y]$), הפולינום $y-3$ הוא פולינום מתוקן ולכן ניתן לבצע בו חילוק עם שארית. זה מסביר למה אפשר לכתוב $f(x, y) = p(x, y)(y-3) + q(x)$. כעת $q(x)$ הוא פולינום רק במשתנה x , וכיוון ש- $x-1$ מתוקן אפשר לבצע בו חילוק עם שארית ולכתוב $q(x) = g(x)(x-1) + r$ כאשר r קבוע. בסך הכל $f(x, y) = p(x, y)(y-3) + g(x)(x-1) + r$. אבל $f(x, y) \in \ker \varphi$, לכן $\varphi(f) = r = 0$. כלומר $f \in I_1$.

לפי משפט האיזומורפיזם הראשון, $\mathbb{Z}[x, y]/I_1 \cong \mathbb{Z}$.

שאלה 5. הוכיחו את האיזומורפיזמים הבאים על ידי משפט האיזומורפיזם הראשון (הסבירו כל צעד, כולל בניית ההומומורפיזם וחשוב הגרעין):

א. $\mathbb{Z}[x]/\langle p, x \rangle \cong \mathbb{Z}/p\mathbb{Z}$.

ב. $\mathbb{Z}[\frac{1}{3}]/5\mathbb{Z}[\frac{1}{3}] \cong \mathbb{Z}/5\mathbb{Z}$.

פתרון.

א. נגדיר $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}$ לפי $\varphi(f) = f(0) + p\mathbb{Z}$.

• הומומורפיזם, כי:

$$\begin{aligned} \varphi(f+g) &= (f(0) + g(0)) + p\mathbb{Z} = (f(0) + p\mathbb{Z}) + (g(0) + p\mathbb{Z}) = \varphi(f) + \varphi(g) \\ \varphi(f \cdot g) &= (f(0) \cdot g(0)) + p\mathbb{Z} = (f(0) + p\mathbb{Z}) \cdot (g(0) + p\mathbb{Z}) = \varphi(f) \cdot \varphi(g) \\ \varphi(1) &= 1 + p\mathbb{Z} \end{aligned}$$

כמו כן על כי $\varphi(n) = n + p\mathbb{Z}$.

נטען כי $\ker \varphi = \langle p, x \rangle$. כיוון אחד הוא ברור ($\langle p, x \rangle \subseteq \ker \varphi$ כי $x \in \ker \varphi$ ונכתוב $f(x) = a_0 + a_1x + \dots + a_nx^n$ מאחר ש- $f \in \ker \varphi$, $a_0 \equiv 0 \pmod{p}$, כלומר $a_0 = pm$, $f = mp + (a_1 + \dots + a_nx^{n-1})x \in \langle p, x \rangle$ אבל אז $x \in \langle p, x \rangle$ כנדרש.

ממשפט האיזומורפיזם הראשון נקבל את המסקנה.

ב. נרצה להגדיר הומומורפיזם $\varphi : \mathbb{Z}[\frac{1}{3}] \rightarrow \mathbb{Z}/5\mathbb{Z}$. מה הוא יכול להיות? אנחנו יודעים ש- $\varphi(1) = 1$, לכן $\varphi(n) = n$ לכל $n \in \mathbb{Z}$. אם נקבע מהו $\varphi(\frac{1}{3})$ נסיים. האיבר הזה צריך לקיים

$$1 = \varphi(1) = \varphi\left(3 \cdot \frac{1}{3}\right) = 3 \cdot \varphi\left(\frac{1}{3}\right) \pmod{5}$$

לכן אין ברירה אלא לבחור $\varphi(\frac{1}{3}) = 2$. כלומר אם קיים הומומורפיזם φ כזה הוא חייב להיות הפונקציה

$$\varphi\left(\frac{m}{3^n}\right) = \varphi(m) \cdot \varphi\left(\frac{1}{3}\right)^n = m \cdot 2^n + 5\mathbb{Z}$$

נוודא ש- φ מוגדרת היטב: נניח ש- $\frac{m}{3^n} = \frac{m'}{3^{n'}}$, ובה"כ $n \leq n'$. לכן $3^{n'-n}m = m'$. מכאן שמתקיים

$$\begin{aligned}\varphi\left(\frac{m'}{3^{n'}}\right) &= m' \cdot 2^{n'} + 5\mathbb{Z} = 3^{n'-n} \cdot 2^{n'} \cdot m + 5\mathbb{Z} = 3^{n'-n} \cdot 2^{n'-n} \cdot 2^n \cdot m + 5\mathbb{Z} = \\ &= 6^{n'-n} \cdot 2^n \cdot m + 5\mathbb{Z} = 2^n \cdot m + 5\mathbb{Z} = \varphi\left(\frac{m}{3^n}\right)\end{aligned}$$

נוודא שזה אכן הומומורפיזם:

$$\begin{aligned}\varphi\left(\frac{m}{3^n} + \frac{m'}{3^{n'}}\right) &= \varphi\left(\frac{3^{n'}m + 3^n m'}{3^{n+n'}}\right) = (3^{n'}m + 3^n m') 2^{n+n'} + 5\mathbb{Z} = \\ &= 6^{n'} \cdot 2^n \cdot m + 6^n \cdot 2^{n'} \cdot m + 5\mathbb{Z} = 2^n \cdot m + 2^{n'} \cdot m + 5\mathbb{Z} = \varphi\left(\frac{m}{3^n}\right) + \varphi\left(\frac{m'}{3^{n'}}\right) \\ \varphi\left(\frac{m}{3^n} \cdot \frac{m'}{3^{n'}}\right) &= (mm') 2^{n+n'} + 5\mathbb{Z} = (m \cdot 2^n + 5\mathbb{Z})(m' \cdot 2^{n'} + 5\mathbb{Z}) = \varphi\left(\frac{m}{3^n}\right) \cdot \varphi\left(\frac{m'}{3^{n'}}\right) \\ \varphi(1) &= \varphi\left(\frac{1}{3^0}\right) = 1 \cdot 2^0 + 5\mathbb{Z} = 1 + 5\mathbb{Z}\end{aligned}$$

קל לוודא ש- φ על (כי $\varphi(n) = n + 5\mathbb{Z}$). כמו כן,

$$\ker \varphi = \left\{ \frac{m}{3^n} \mid m \cdot 2^n \in 5\mathbb{Z} \right\} = \left\{ \frac{m}{3^n} \mid m \in 5\mathbb{Z} \right\} = 5\mathbb{Z} \left[\frac{1}{3} \right]$$

המסקנה נובעת ממשפט האיזומורפיזם הראשון.

שאלה 6. יהי R חוג.

- א. יהיו $I, J \triangleleft R$ קורמקסימליים. הוכיחו כי $I \cap J = IJ + JI$.
- ב. יהיו $I, J, K \triangleleft R$ כך ש- I, K קורמקסימליים וגם J, K קורמקסימליים. הראו כי גם IJ, K קורמקסימליים.
- ג. הוכיחו באמצעות אינדוקציה על n את משפט השאריות הסיני ל- n אידאלים: יהי R חוג, ויהיו $I_1, \dots, I_n \triangleleft R$ אידאלים קורמקסימליים בזוגות. אזי

$$R/I_1 \cap \dots \cap I_n \cong R/I_1 \times \dots \times R/I_n$$

הסיקו שעבור חוג חילופי R ואידאלים כנ"ל מתקיים

$$R/I_1 \dots I_n \cong R/I_1 \times \dots \times R/I_n$$

הוכחה.

- א. $IJ + JI \subseteq I \cap J$ ולכן $IJ, JI \subseteq I \cap J$ $\boxed{\supseteq}$.
לפי הנתון קיימים $x \in I$ ו- $y \in J$ כך ש- $x + y = 1$. יהי $z \in I \cap J$ לכן $\boxed{\subseteq}$

$$z = z \cdot 1 = z(x + y) = zx + zy$$

קעת $z \in I \cap J \subseteq I$, לכן $zy \in IJ$, ומצד שני $z \in I \cap J \subseteq J$ ולכן $zx \in JI$. זה מראה $z \in IJ + JI$.

ב. לפי הנתון $I + K = J + K = R$. לכן קיימים $x \in I, y \in J, z, z' \in K$ כך ש- $x + z = 1 = y + z'$. לכן $1 = (x + z)(y + z') = xy + (xz' + zy + zz')$. לפי ההגדרה $xy \in IJ$, וכיוון ש- K הוא אידיאל מתקיים $xz' + zy + zz' \in K$. לכן IJ, K הם קו-מקסימליים.

ג. עבור $n = 2$ זהו משפט השאריות הסיני שהוכחתם בהרצאה. נניח כי הטענה נכונה עבור n כלשהו, ונוכיח עבור $n + 1$. יהיו I_1, \dots, I_{n+1} אידיאלים קו-מקסימליים בזוגות. אם נשתמש בסעיף הקודם על I_1, \dots, I_n ביחס ל- I_{n+1} , נקבל ש- $I_1 \dots I_n$ ו- I_{n+1} הם קו-מקסימליים, ובפרט $I_1 \cap \dots \cap I_n$ ו- I_{n+1} הם קו-מקסימליים. לפי משפט השאריות הסיני עבור $n = 2$,

$$R/I_1 \cap \dots \cap I_{n+1} = R/(I_1 \cap \dots \cap I_n) \cap I_{n+1} \cong R/I_1 \cap \dots \cap I_n \times R/I_{n+1}$$

ולפי הנחת האינדוקציה נקבל את הדרוש.

□

שאלה 7. מצאו $x \in \mathbb{Z}$ המקיים $x \equiv 2 \pmod{5}, x \equiv 4 \pmod{7}, x \equiv 8 \pmod{11}$.

פתרון. נתחיל מלמצוא $y \in \mathbb{Z}$ המקיים $y \equiv 3 \pmod{5}$ ו- $y \equiv 4 \pmod{7}$. נשים לב כי $3 \cdot 5 - 2 \cdot 7 = 1$, ולכן ה- y המתאים הוא $3 \cdot 5 - 2 \cdot 7 = 1$ (הוא יחיד מודולו 35).

כעת נמצא $x \in \mathbb{Z}$ המקיים $x \equiv 32 \pmod{35}$ ו- $x \equiv 8 \pmod{11}$. נמצא את המקדמים של 1 כצירוף לינארי של 11 ו-35:

$$(35, 11) = \{35 = 3 \cdot 11 + 2\} = (11, 2) = \{11 = 5 \cdot 2 - 1\} = (2, 1) = 1$$

ולכן

$$1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (35 - 3 \cdot 11) = 16 \cdot 11 - 5 \cdot 35$$

כלומר ה- x הדרוש הוא

$$x = 16 \cdot 11 \cdot 32 - 5 \cdot 35 \cdot 8 = 4232 \equiv 382 \pmod{385}$$

שאלה 8. יהיו $a_1, \dots, a_n \in \mathbb{R}$ מספרים שונים, ויהיו $b_1, \dots, b_n \in \mathbb{R}$ הוכיחו, באמצעות משפט השאריות הסיני, כי קיימת פונקציה רציפה $f: \mathbb{R} \rightarrow \mathbb{R}$ כך ש- $f(a_i) = b_i$ לכל $1 \leq i \leq n$.

(הדרכה: בחוג הפונקציות הרציפות $C(\mathbb{R})$, שהפעולות בו הן חיבור נקודתי ומכפלה נקודתית, הסתכלו על אידיאלים מהצורה $I_a = \{f \in C(\mathbb{R}) \mid f(a) = 0\}$ עבור $a \in \mathbb{R}$.)

הוכחה. בחוג הפונקציות הרציפות $C(\mathbb{R})$ נגדיר לכל $a \in \mathbb{R}$ את הקבוצה

$$I_a = \{f \in C(\mathbb{R}) \mid f(a) = 0\}$$

נטען כי כל I_a הוא אידיאל. אכן, הוא תת-חוג כי אם $f, g \in I_a$ אז

$$(f - g)(a) = f(a) - g(a) = 0$$

ואם $f \in I_a$ ו- $g \in C(\mathbb{R})$ אז

$$(f \cdot g)(a) = f(a) \cdot g(a) = 0 \cdot g(a) = 0$$

(מספיק לבדוק בליעה מצד אחד כי $C(\mathbb{R})$ חוג חילופי).
 כעת נטען שעבור $a \neq b$, האידיאלים I_a ו- I_b הם קו-מקסימליים. לשם כך מספיק להראות
 $f \in I_a + I_b$. ניקח את הפונקציות $f(x) = \frac{x-a}{b-a}$ ו- $g(x) = \frac{x-b}{b-a}$. קל לראות כי $f \in I_a$
 ו- $g \in I_b$, ולכן

$$f(x) - g(x) = \frac{x-a}{b-a} - \frac{x-b}{b-a} = 1 \in I_a + I_b$$

מה שמראה שהאידיאלים קו-מקסימליים.
 כעת נוכל להוכיח את הטענה. יהיו $a_1, \dots, a_n \in \mathbb{R}$ מספרים שונים, ויהיו $b_1, \dots, b_n \in \mathbb{R}$
 $f \in C(\mathbb{R})$ נשים לב כי $g_i(x) = b_i$ לכל $1 \leq i \leq n$ נגדיר $f(a_i) = b_i$. כיוון שהאידיאלים
 I_{a_1}, \dots, I_{a_n} קו-מקסימליים באוגות, ממשפט השאריות הסיני נקבל כי קיימת פונקציה רציפה
 f המקיימת $f \equiv g_i \pmod{I_{a_i}}$ לכל $1 \leq i \leq n$, כנדרש. \square

שאלה 9. יהי R חוג חילופי. נסמן על ידי N את אוסף האיברים הנילפוטנטיים ב- R (תזכורת:
 איבר $a \in R$ הוא נילפוטנטי, אם קיים $n \in \mathbb{N}$ שעבורו $a^n = 0$).

- א. הוכיחו ש- N הוא אידיאל של R .
- ב. הוכיחו שב- R/N אין איברים נילפוטנטיים לא טריוויאליים (כלומר שונים מ-0).
- ג. תנו דוגמה לחוג לא חילופי שבו N אינו אידיאל.

פתרון.

א. N אינו ריק כי $0 \in N$. יהיו $a, b \in N$. אז קיימים $n, m \in \mathbb{N}$ כך ש- $a^n = b^m = 0$.
 נוסחת הבינום של ניוטון נכונה גם בחוגים חילופיים. לכן

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} (-1)^k \binom{n+m}{k} a^k b^{n+m-k}$$

אם $k \geq n$, אז $a^k = 0$. אחרת, $k < n$ ולכן $m < n+m-k$, כלומר $b^{n+m-k} = 0$.
 לכן $a-b \in N$. ברור שאם $r \in R$, אז $ra \in N$ כי $(ra)^n = r^n a^n = 0$.

ב. נניח בשלילה כי $\bar{x} = x + N \in R/N$ הוא נילפוטנטי. אז קיים $n \in \mathbb{N}$ כך
 ש- $\bar{x}^n = \bar{0}$. כלומר

$$N = \bar{0} = \bar{x}^n = (x+N)^n = x^n + N$$

ולכן $x^n \in N$. כלומר x^n הוא נילפוטנטי, ולכן קיים $k \in \mathbb{N}$ כך ש- $(x^n)^k = 0$. לכן
 $x^{nk} = 0$, ונקבל $x \in N$. אך זו סתירה כי הנחנו כי $\bar{x} \neq \bar{0} = N$.

ג. נבחר $R = M_2(\mathbb{Q})$, $e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, אז $e_{12}^2 = e_{21}^2 = 0$, ולכן הם
 נילפוטנטיים. אבל לכל $n \in \mathbb{N}$

$$(e_{12} + e_{21})^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

ולכן $e_{12} + e_{21} \notin N$. כלומר N אינו סגור לחיבור, ובפרט אינו אידיאל.

בהצלחה!