פתרון תרגיל בית 5 מבוא לחוגים ומודולים
88-212 סמסטר ב' תשפ"א

שאלה 1. עבור האידאלים הבאים קבעו האם הם ראשוניים והאם הם מקסימליים.

א. $I = \langle 4x+1 \rangle \lhd \mathbb{Z}[x]$.

ב. $R = \{ \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a,b \in \mathbb{Q} \}$ $I = \{ \left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \mid b \in \mathbb{Q} \} \lhd R$. רמז: הראו $R \cong \mathbb{Q}[x] / \langle x^2 \rangle$.

ג. $I = \langle \overline{x+1} \rangle \lhd \mathbb{F}_3[x] / \langle x^4 - 16 \rangle$ כאשר בסימון $\overline{x+1}$ הכוונה לתמונה של $x+1$ בהטלה לחוג המנה. רמז: אפשר להשתמש במשפט השאריות הסיני.

פתרון.

א. נסתכל על המנה $\mathbb{Z}[x] / \langle 4x+1 \rangle$, ונטען כי היא איזומורפית ל-$\mathbb{Z}\left[\frac{1}{4}\right]$. אכן, נגדיר $\varphi : \mathbb{Z}[x] \to \mathbb{Z}\left[\frac{1}{4}\right]$ לפי $\varphi(f(x)) = f\left(\frac{1}{4}\right)$. זהו אפימורפיזם. נטען כי הגרעין שלו הוא $I = \langle 4x+1 \rangle$. אכן, אם $f \in \ker\varphi$, אז $f\left(\frac{1}{4}\right) = 0$. אפריורי, אי אפשר לחלק ב-$4x+1$ בשלמים, כי המקדם המוביל אינו הפיך, אז נבצע חילוק פולינומים ב-$\mathbb{Q}[x]$: $f(x) = (4x+1)\, g(x)$ לאיזשהו $g(x) \in \mathbb{Q}[x]$. נכתוב $g(x) = \sum_{i=0}^{n} a_i x^i$, ונטען כי בעצם $g(x) \in \mathbb{Z}[x]$. אכן, $f(x) = g(x) \cdot (4x+1) = a_0 + \sum_{i=1}^{n} (a_i + 4a_{i-1}) x^i + 4a_n x^{n+1} \in \mathbb{Z}[x]$. מהמקדם החופשי נקבל ש-$a_0 \in \mathbb{Z}$; מהמקדם של x נקבל $4a_0 + a_1 \in \mathbb{Z}$, ולכן $a_1 \in \mathbb{Z}$; ובאופן דומה כל $a_i \in \mathbb{Z}$. לכן $f \in I$.
לפי משפט האיזומורפיזם הראשון, $\mathbb{Z}\left[\frac{1}{4}\right] \cong \mathbb{Z}[x]/\langle 4x+1 \rangle$. החוג $\mathbb{Z}\left[\frac{1}{4}\right]$ הוא תחום שלמות שאינו שדה, ולכן I אידאל ראשוני שאינו מקסימלי.

ב. במקרה הזה I אידאל מקסימלי. אפשר להוכיח בשלוש דרכים. בדרך הראשונה – אם J אידאל שמכיל את I, אז J מכיל מטריצה מהצורה $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ לאיזשהו $a \neq 0$. אבל אז גם $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} - \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in J$, וזה איבר הפיך, לכן $J = R$.
בדרך השנייה – אפשר להוכיח ממשפט האיזומורפיזם הראשון ש-$R/I \cong \mathbb{Q}$. זהו שדה, ולכן I מקסימלי.
בדרך השלישית – לפי הרמז, אפשר להוכיח כי $R \cong \mathbb{Q}[x] / \langle x^2 \rangle$, ותחת האיזומורפיזם הזה I מזדהה עם $\langle x \rangle / \langle x^2 \rangle$. ממשפט האיזומורפיזם השלישי אפשר להוכיח שזהו אידאל מקסימלי.

ג. נתחיל ממשפט האיזומורפיזם השלישי:

$$\mathbb{F}_3[x]/\langle x^4-16 \rangle / \langle x+1 \rangle / \langle x^4-16 \rangle \cong \mathbb{F}_3[x] / \langle x+1 \rangle$$

וכמו שראינו בתרגול $\mathbb{F}_3[x] / \langle x+1 \rangle \cong \mathbb{F}_3$. זהו שדה, ולכן האידאל I מקסימלי.

שאלה 2. מצאו $n \in \mathbb{N}$ כך ש-$\mathbb{Z}[i] / \langle 3+i \rangle \cong \mathbb{Z}/n\mathbb{Z}$. הוכיחו את האיזומורפיזם, וקבעו האם האידאל $\langle 3+i \rangle$ הוא אידאל ראשוני, מקסימלי או אף אחד מהם ב-$\mathbb{Z}[i]$.

פתרון. נרצה למצוא את ה-n המתאים. עבור ה-n הנכון יהיה אפימורפיזם $\varphi : \mathbb{Z}[i] \to \mathbb{Z}/n\mathbb{Z}$ כך ש-$\ker\varphi = \langle 3+i \rangle$. כיוון ש-$\varphi$ הומומורפיזם, $\varphi(3) = 3\varphi(1) = 3 + n\mathbb{Z}$; כיוון ש-$3 + i \in \ker\varphi$, $\varphi(3+i) = 3 + \varphi(i) = 0 + n\mathbb{Z}$, ולכן $\varphi(i) = -3 + n\mathbb{Z}$. מצד שני, $-1 + n\mathbb{Z} = \varphi(-1) = \varphi\left(i^2\right) = \varphi(i)^2 = 9 + n\mathbb{Z}$. זה מראה ש-$n \mid 10$.

נראה ש-$n = 10$ הוא בדיוק ה-n הנכון. בחישובים שעשינו ראינו איך להגדיר את $\varphi : \mathbb{Z}[i] \to \mathbb{Z}/10\mathbb{Z}$:

$$\varphi(a+bi) = (a+7b) + 10\mathbb{Z}$$

נראה שזהו הומומורפיזם: החיבוריות ברורה, ולכפליות

$$\varphi((a+bi)(c+di)) = \varphi((ac-bd)+(ad+bc)i) = (ac-bd+7ad+7bc) + 10\mathbb{Z}$$

ומצד שני

$$\begin{aligned}\varphi(a+bi)\varphi(c+di) &= ((a+7b)+10\mathbb{Z})((c+7d)+10\mathbb{Z}) = \\ &= ((a+7b)(c+7d)+10\mathbb{Z}) = \\ &= (ac+49bd+7(ad+bc)) + 10\mathbb{Z} = \\ &= (ac-bd+7ad+7bc) + 10\mathbb{Z}\end{aligned}$$

כנדרש. כמובן $\varphi(1) = 1 + 10\mathbb{Z}$. לכן φ הומומורפיזם. φ על, כי $\varphi(n) = n + 10\mathbb{Z}$.

נחשב את הגרעין של φ. $\varphi(3+i) = 0 + 10\mathbb{Z}$, ולכן $\langle 3+i \rangle \subseteq \ker\varphi$. מצד שני, נניח ש-$a + bi \in \ker\varphi$; אז $a + 7b \in 10\mathbb{Z}$, כלומר $10 \mid (a - 3b)$. אז אפשר לכתוב

$$\frac{a+bi}{3+i} = \frac{a+bi}{3+i} \cdot \frac{3-i}{3-i} = \frac{3a-b}{10} + \frac{3b-a}{10}i.$$

(ודאו ש-$\frac{3a-b}{10}, \frac{3b-a}{10} \in \mathbb{Z}$). לכן $\ker\varphi \subseteq \langle 3+i \rangle$. זה מראה את השוויון, ובסך הכל $\mathbb{Z}[i] / \langle 3+i \rangle \cong \mathbb{Z}/10\mathbb{Z}$.

כיוון ש-$\mathbb{Z}/10\mathbb{Z}$ אינו תחום שלמות, האידאל אינו ראשוני ואינו מקסימלי.

שאלה 3. חוג R נקרא **ראשוני למחצה** אם אין לו אידאלים $0 \neq I \lhd R$ כך ש-$I^2 = 0$. אידאל P בחוג כלשהו R נקרא ראשוני למחצה אם R/P הוא חוג ראשוני למחצה.

א. הוכח כי כל אידאל ראשוני הוא אידאל ראשוני למחצה.

ב. הוכח כי P ראשוני למחצה אם ורק אם (לכל אידאל $I \lhd R$, אם $I^2 \subseteq P$, אז $I \subseteq P$).

ג. אידאל $I \lhd R$ נקרא נילפוטנטי אם קיים $k \in \mathbb{N}$ כך ש-$I^k = 0$. הוכיחו כי חוג הוא ראשוני למחצה אם ורק אם אין בו אידאלים נילפוטנטיים שונים מ-0.

ד. מצאו את כל האידאלים הראשוניים למחצה של $\mathbb{Z}$.

הוכחה.

א. נניח ש-$P \lhd R$ ראשוני. אז R/P הוא חוג ראשוני. אם $I \lhd R/P$ היה אידאל המקיים $I^2 = 0$, אז מהראשוניות נקבל $I = 0$, ולכן P ראשוני למחצה.

ב. נניח ש-P ראשוני למחצה, ויהי $I \lhd R$ אידאל שעבורו $I^2 \subseteq P$. נשים לב כי

$$\left(I+P\right/P)^2 = I^2+P\big/P = P\big/P = 0$$

בחוג המנה, ולכן $I + P) / P = 0$, כלומר $I \subseteq P$.

מהצד השני, נניח שהתנאי מתקיים. כל אידאל של חוג המנה אפשר לכתוב בצורה I/P לאיזשהו $P \subseteq I \lhd R$. אם מתקיים $\left(I\big/P\right)^2 = I^2+P\big/P = 0$ אז $I^2 \subseteq P$, ולכן נקבל $I \subseteq P$, כלומר $I = P$, כנדרש.

ג. $\boxed{\Leftarrow}$ נניח ש-R ראשוני למחצה, ויהי $I \lhd R$ כך ש-$I^k = 0$. נניח שזהו ה-k המינימלי המקיים את זה. אם $k > 1$, אז $I^k = 0 \subseteq I^{2k-2} = \left(I^{k-1}\right)^2$, לכן $I^{k-1} = 0$, בסתירה. לכן $k = 1$, כלומר $I = 0$.
$\boxed{\Rightarrow}$ ישירות מההגדרה.

ד. האידאלים הראשוניים למחצה של $\mathbb{Z}$ הם בדיוק האידאלים מהצורה $p_1 \dots p_k\mathbb{Z}$ עבור ראשוניים שונים $p_1, \dots, p_k$ ואידאל האפס. אכן, כל אידאל לא אפסי של $\mathbb{Z}$ הוא מהצורה $n\mathbb{Z}$ לאיזשהו $n \in \mathbb{N}$. נרשום $n = p_1^{t_1} \dots p_k^{t_k}$. אם יש איזשהו $t_i > 1$, בה"כ $t_k > 1$, אז $\left(p_1^{t_1} \dots p_{k-1}^{t_{k-1}} p_k^{t_k - 1}\mathbb{Z}\right)^2 \subseteq n\mathbb{Z}$, ולכן הוא לא ראשוני למחצה. אם כל $t_i = 1$, אילו היה אידאל $m\mathbb{Z} \lhd \mathbb{Z}$ המקיים $m^2\mathbb{Z} \subseteq n\mathbb{Z}$, אז $n \mid m^2$, אבל כיוון שכל $t_i = 1$ נקבל $n \mid m$, כלומר $m\mathbb{Z} \subseteq n\mathbb{Z}$.

□

שאלה 4. יהי R חוג. ניזכר בהערכה $v : R((x)) \to \mathbb{Z} \cup \{\infty\}$ שהגדרנו בתרגול:

$$v(0) = \infty, \qquad v\left(\sum_{i=-n}^{\infty} a_i x^i\right) = \min\{i \mid a_i \neq 0\}$$

הוכיחו כי מתקיים $v(f+g) \geq \min\{v(f), v(g)\}$ וגם $v(f \cdot g) \geq v(f) + v(g)$. בנוסף, אם R הוא תחום, אז יש שיוויון $v(f \cdot g) = v(f) + v(g)$.

הוכחה. קל לראות כי כל הטענות מתקיימות אם $f = 0$ או $g = 0$, ולכן נניח $f, g \neq 0$. נכתוב $f = \sum_{i=n}^{\infty} a_i x^i$ ו-$g = \sum_{j=m}^{\infty} b_j x^j$ עבור $m, n \in \mathbb{Z}$ (אולי שליליים). אז $v(f) = n$ ו-$v(g) = m$.

עבור הסכום: אם $m \neq n$, בה"כ $n < m$, אז המקדם המוביל של $f+g$ הוא $a_n x^n$, ולכן $v(f+g) = n = \min\{m, n\}$. אם $m = n$, המקדם המוביל של $f+g$ הוא $(a_n + b_n) x^n$, אלא אם $a_n + b_n = 0$ ואז הוא ממעלה יותר גבוהה. לכן $v(f+g) \geq n = \min\{v(f), v(g)\}$.

עבור המכפלה: המקדם המוביל של fg הוא $a_n b_m x^{m+n}$, אלא אם $a_n b_m$ ואז הוא ממעלה יותר גבוהה. לכן $v(fg) \geq m + n = v(f) + v(g)$. אם R הוא תחום, אז $a_n b_m \neq 0$, ונקבל שוויון. □

שאלה 5. יהי R חוג חילופי. הוכיחו שכל אידאל ראשוני $P \lhd R$ הוא מן הצורה $R \cap Q$ עבור אידאל ראשוני $Q \lhd R[[x]]$. (רמז: $R \cong R[[x]] / \langle x \rangle$).

פתרון. עבור P נבנה את $Q = \langle P, x \rangle$. אפשר לראות ש-Q הוא ראשוני לפי המנה

$$R[[x]]/Q \cong R/P$$

שאלה 6. יהי R חוג. איבר $e \in R$ יקרא אידמפוטנט אם $e^2 = e$. אידמפוטנט $e \in R$ הוא לא טריוויאלי אם $e \neq 0_R, 1_R$. בתרגיל הזה נמצא דרך לזהות שחוג R הוא מכפלה ישרה של חוגים.

א. יהיו S, S' חוגים. הוכיחו שאם $R \cong S \times S'$, אז קיים ב-R אידמפוטנט מרכזי לא טריוויאלי.

ב. אידמפוטנטים $e, f \in R$ נקראים אידמפוטנטים אורתוגונליים אם $ef = fe = 0$.
הוכיחו שאם $e \in R$ אידמפוטנט, אז גם $1 - e$ אידמפוטנט. הוכיחו כי e ו-$1 - e$ הם אורתוגונליים.

ג. הוכיחו שאם $e \in R$ הוא אידמפוטנט מרכזי לא טריוויאלי, אז קיים איזומורפיזם של חוגים $\varphi: R \to Re \times R(1-e)$. רמז: זה סעיף קצת ארוך, אבל בעיקר טכני. כתבו במפורש לכל $x \in R$ מהו $\varphi(x)$ ובדקו שאכן מדובר באיזומורפיזם של חוגים.

פתרון.

א. נתבונן באיבר $e = (1,0)$. זהו אידמפוטנט, כי $e^2 = \left(1^2, 0^2\right) = (1,0) = e$; הוא לא טריוויאלי כי $e \neq (1,1)$; והוא מרכזי כי $e(s,s') = (s,0) = (s,s')e$.

ב. מחישוב ישיר, $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$. כמו כן, הם אורתוגונליים כי $e(1-e) = e - e^2 = 0$.

ג. יהי $e \in R$ אידמפוטנט מרכזי לא טריוויאלי. נגדיר העתקה $\varphi : R \to Re \times R(1-e)$ לפי

$$\varphi(x) = (xe, x(1-e)).$$

נטען ש-φ היא האיזומורפיזם הדרוש.
אכן, φ הומומורפיזם כי

$$\varphi(x+y) = ((x+y)e, (x+y)(1-e)) = (xe, x(1-e)) + (ye, y(1-e)) = \varphi(x) + \varphi(y)$$

$$\varphi(xy) = (xye, xy(1-e)) = \left(xye^2, xy(1-e)^2\right) = ((xe)(ye), (x(1-e))(y(1-e))) =$$

$$= (xe, x(1-e))(ye, y(1-e)) = \varphi(x)\varphi(y)$$

(שימו לב שבכפליות השתמשנו בכך ש-$e, 1-e$ אידמפוטנטים מרכזיים. כמו כן, איבר היחידה של $Re \times R(1-e)$ הוא $\varphi(1) = (e, 1-e)$). לכן φ הומומורפיזם.
נראה ש-φ חח"ע. יהי $x \in \ker\varphi$; אזי $\varphi(x) = (xe, x(1-e)) = (0,0)$. אבל אז

$$x = xe + x(1-e) = 0 + 0 = 0$$

ולכן φ חח"ע.
נראה ש-φ על. יהי $(s,s') \in Re \times R(1-e)$. לכן קיימים $y, y' \in R$ שעבורם $s = ye$ ו-$s' = y'(1-e)$. נתבונן ב-$x = ye + y'(1-e)$. אזי

$$\varphi(x) = ((ye + y'(1-e))e, (ye + y'(1-e))(1-e)) =$$

$$= \left(ye^2 + y'(1-e)e, ye(1-e) + y'(1-e)^2\right) =$$

$$= (ye, y'(1-e)) = (s,s')$$

(שימו לב שפה השתמשנו באורתוגונליות של e ו-$1-e$).
בסך הכל הראינו ש-φ איזומורפיזם, כדרוש.

נשתמש בסימון $I \leq_l R$ כדי לומר ש-I הוא אידאל שמאלי של R. כלומר $RI \subseteq I$.

שאלה 7. יהי R חוג בלי יחידה, ויהי $I \leq_l R$ אידאל שמאלי. נסמן $I^+ = \{x \in R \mid xR \subseteq I\}$.

א. הוכיחו $I^+ \lhd R$ אידאל דו־צדדי.

ב. הוכיחו שאם $I \lhd R$, אז $I \subseteq I^+$.

ג. הוכיחו שאם R חוג (עם יחידה), אז $I^+ = I^{++}$.

פתרון. א. $I^+ \neq \varnothing$ כי $0 \in I^+$. היא סגורה לחיסור, כי אם $x, y \in I^+$ אז $r \in R$ ו-$(x-y)r = xr - yr \in I$.
נראה את הבליעה. יהי $x \in I^+$ ו-$r \in R$. אז

$$(rx)R = rxR \subseteq rI \subseteq I \implies rx \in I^+$$

$$(xr)R = xrR \subseteq xR \subseteq I \implies xr \in I^+$$

לכן I^+ אידאל דו-צדדי של R.

ב. אם I מקיים גם בליעה מימין, אז לכל $i \in I$ מתקיים $iR \subseteq I$, ולכן $i \in I^+$. זה מראה ש-$I \subseteq I^+$.

ג. ההכלה $I^+ \subseteq I^{++}$ נובעת משני הסעיפים הקודמים. לכן נותר להוכיח $I^{++} \subseteq I^+$. יהי $x \in I^{++}$; אז לכל $r \in R$ מתקיים $xr \in I^+$. בפרט אפשר לקחת $r = 1$ ולקבל $x \in I^+$. לכן קיבלנו את ההכלה משני הכיוונים.

בהצלחה!