

פתרון תרגיל בית 4 מבוא לחוגים ומודולים 88-212 סמסטר ב' תשע"ח

אייר מזור ודניאל יעקובי

26 במאי 2018

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

א. נרצה להוכיח את השוויון $I \cap J = IJ + JI$ בעזרת הכלה זו כיוונית. יהי $a \in I \cap J$ וקו מקסימליים ולכן קיימים $i \in I, j \in J$ כך ש $i + j = 1$. נכתוב

$$a = a \cdot 1 = a \cdot (i + j) = a \cdot i + a \cdot j \in JI + IJ$$

ומכאן שמתקיים $I \cap J \subseteq IJ + JI$.

כעת יהי $a + b \in IJ + JI$. ראינו בהרצאה שמתקיים $IJ, JI \subseteq I \cap J$ ולכן $a, b \in I \cap J$ הוא אידיאל ולכן סגור לחיבור, מכאן, $a + b \in I \cap J$ ולכן $I \cap J \subseteq IJ + JI$.

□ סך הכל, $I \cap J = IJ + JI$, כדרוש.

ב. יהי $n \in \mathbb{N}$. תחילה נוכיח ש I^n, J קו מקסימליים, נעשה זאת באינדוקציה על n . בסיס האינדוקציה, $n = 1$, נתון. נניח ש I^{n-1}, J קו מקסימליים, כלומר, קיימים $i' \in I^{n-1}, j' \in J$ כך ש $1 = i' + j'$. מכיוון ש I, J קו מקסימליים קיימים $i \in I, j \in J$ כך ש $1 = i + j$. נכפול את שני אגפיה של משוואה זו ב- i' לקבלת

$$i' = i \cdot i' + j \cdot i' \in I^n + J$$

וכעת נכתוב

$$1 = i' + j' \in I^n + J + J = I^n + J$$

ומכאן נסיק כי I^n, J קו מקסימליים.

בעצם הוכחנו, אם I, J קו מקסימליים אז גם I^n, J קו מקסימליים לכל $n \in \mathbb{N}$. נפעיל טענה זו על I^n, J , הם קו מקסימליים ולכן גם I^n, J^m קו מקסימליים לכל $m \in \mathbb{N}$. זה בדיוק מה שנדרש להוכיח. □

שאלה 2. 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. נרצה להוכיח שכל שניים מבין האידיאלים הם קו מקסימליים. לכל זוג אידיאלים נראה שאיבר היחידה נמצא בחיבור שלהם.

$$1 = x - (x - 1) \in I_0 + I_1$$

$$1 = 3x - y + (-3(x - 2) + (y - 5)) \in I_0 + I_2$$

$$1 = (x - 1) - (x - 2) \in I_1 + I_2$$

ומכאן נסיק שכל שניים מבין האידיאלים הנ"ל הם קו מקסימליים.

ב. כעת עלינו להוכיח $R/I_1 \cong \mathbb{Z}$. נוכיח טענה חזקה יותר: נסמן

$$I = \langle x - \alpha, y - \beta \rangle, \alpha, \beta \in \mathbb{Z}$$

ונוכיח $R/I \cong \mathbb{Z}$. נוכיח תחילה כי כל פולינום $f(x, y) \in \mathbb{Z}[x, y]$ ניתן להציג גם כ:

$$f(x, y) = p(x, y)(x - \alpha) + q(x, y)(y - \beta) + g(x, y)$$

כאשר החזקות הכי גבוהות של x, y, xy ב $g(x, y)$ קטנות משל $f(x, y)$. נרשום

$$f(x, y) = a_0 + a_1x + \dots + a_nx^n + b_0 + b_1y + \dots + b_my^m + c_{00} + c_{11}xy + c_{12}xy^2 + \dots + c_{rs}x^r y^s$$

ונגדיר

$$p(x, y) = a_nx^{n-1} + c_{rs}x^{r-1}y^s, \quad q(x, y) = b_my^{m-1}$$

$$a(x, y) = p(x, y)(x - \alpha) + q(x, y)(y - \beta), \quad g(x, y) = f(x, y) - a(x, y)$$

נשים לב כי

$$a(x, y) = a_nx^n + c_{rs}x^r y^s - \alpha a_nx^{n-1} - \alpha c_{rs}x^{r-1}y^s + b_my^m - \beta b_my^{m-1}$$

מכאן ניתן לראות כי המקדמים של $x^n, y^m, x^r y^s$ של $g(x, y)$ מתאפסים. כלומר הצגנו את $f(x, y)$ כמתואר למעלה. כעת נפעיל את אותו התהליך על $g(x, y)$ וכך הלאה. נשים לב כי החזקות של x^n, y^m ושל $x^r y^s$ יורדות ולכן לבסוף נישאר עם "שארית" מהצורה

$$r(y) = d_0 + d_1y + \dots + d_sy^s$$

אך באותו האופן, ניתן לכתוב אותה כך

$$r(y) = h(y)(y - \beta) + u(y)$$

כאשר $\deg u < \deg r$. שוב, נמשיך עם תהליך זה עד שנגיע ל- $\rho \in \mathbb{Z}$.
כאשר $\rho \in \mathbb{Z}$.

סך הכל קיבלנו ש $f(x, y) \in \mathbb{Z}[x, y]$ כלשהו ניתן לכתוב גם כך:

$$f(x, y) = p(x, y)(x - \alpha) + q(x, y)(y - \beta) + \rho$$

כאשר $\rho \in \mathbb{Z}, p(x, y), q(x, y) \in \mathbb{Z}[x, y]$ נראה כך

$$I = \{p(x, y)(x - \alpha) + q(x, y)(y - \beta) : p(x, y), q(x, y) \in \mathbb{Z}[x, y]\}$$

לכן כל $f(x, y) \in \mathbb{Z}[x, y]$ מקיים $f(x, y) \in \rho + I$. מכאן כי חוג המנה נראה כך

$$R/I = \{[\rho] : \rho \in \mathbb{Z}\}, \quad ([\rho] = \rho + I)$$

עבור $\rho \neq 0$ נקבל $\rho \notin I$ מכיוון שכל פולינום ב I מתאפס בנקודה (α, β) ו- ρ אינו מתאפס בה (כפולינום). לכן $[0] \neq [\rho]$. מכאן שעבור $\rho_1 \neq \rho_2$ נקבל $[\rho_1] \neq [\rho_2]$. לכן ההעתקה הבאה תהיה מוגדרת היטב

$$\begin{aligned} \varphi: R/I &\rightarrow \mathbb{Z} \\ [\rho] &\mapsto \rho \end{aligned}$$

□ קל לוודא שזהו איזומורפיזם, כלומר, $R/I \cong \mathbb{Z}$.

שאלה 3.

א. נסמן

$$R = \mathbb{F}_2[x]/\langle x^2 \rangle, \quad S = \mathbb{F}_2[x]/\langle x^2 - 1 \rangle$$

ונוכיח $R \cong S$. תחילה נסתכל על איברים ב- R . מתקיים $[x]^2 = [x^2] = [0]_R = 0_R$ מכאן כי לכל $k \geq 2$, $[x]^k = 0_R$ ולכן עבור איבר כלשהו $r \in R$ נקבל

$$r = [a_0 + a_1x + \dots + a_nx^n] = [a_0] + [a_1][x] + \dots + [a_n][x]^n = [a_0] + [a_1][x]$$

כעת נסתכל על איברים ב- S . מתקיים $[x]^2 = [1]$ $\Rightarrow [x^2] = [1]$ $\Rightarrow [x^2 - 1] = [0]_S = 0_S$. לכן, נוכל לקבץ את כל המקדמים של החזקות הזוגיות אל האיבר החופשי ואת כל המקדמים של החזקות האי זוגיות אל המקדם של x . עבור $s \in S$ כלשהו

$$s = [a_0 + a_1x + \dots + a_nx^n] = [b_0] + [b_1][x]$$

כאשר $b_0 = \sum a_i$ זוגי, $b_1 = \sum a_i$ אי זוגי.

מהנ"ל אנו יכולים לכתוב את כל איבריהם של החוגים R, S

$$R = \{[0]_R, [1]_R, [x]_R, [x+1]_R\}, \quad S = \{[0]_S, [1]_S, [x]_S, [x+1]_S\}$$

נגדיר את ההעתקה $\varphi: R \rightarrow S$ על ידי $\varphi([a_0]_R + [a_1]_R[x]_R) = [a_0]_S + [a_1]_S[x]_S$ זהו העתקה חח"ע ועל לפי ההצגה הנ"ל והיא משמרת צורה (משמרת כפל, חיבור ושולחת את 1 ל-1) לפי ההגדרה של פעולות על קוסטים. כלומר, φ איזומורפיזם של חוגים ($R \cong S$).

ב. נסמן

$$R = \mathbb{Q}[x]/\langle x^2 \rangle, \quad S = \mathbb{Q}[x]/\langle x^2 - 1 \rangle$$

ונוכיח $R \not\cong S$. נניח בשלילה שקיים איזומורפיזם $\varphi: R \rightarrow S$. לכן לפי תכונות של איזומורפיזם

$$\varphi([0]_R) = \varphi([x^2]_R) = \varphi^2([x]_R), \quad \varphi([0]_R) = [0]_S$$

ומכאן כי $\varphi^2([x]_R) = [0]_S$. קיים $p(x) \in \mathbb{Q}[x]$ כך ש- $\varphi([x]_R) = [p(x)]_S$, לכן, $[p^2(x)]_S = [0]_S$ כלומר, $p^2(x) \in \langle x^2 - 1 \rangle$. מכאן כי קיים $q(x) \in \mathbb{Q}[x]$ כך ש- $p^2(x) = q(x)(x^2 - 1) = q(x)(x-1)(x+1)$

נניח $p(x) \notin \langle x^2 - 1 \rangle$, כלומר, $x-1, x+1$ או שניהם אינם מחלקים את $p(x)$ מכאן כי הם גם אינם מחלקים את $p^2(x)$ בסתירה. לכן, $p(x) \in \langle x^2 - 1 \rangle$, כלומר, $[p(x)]_S = [0]_S$ ואז

$$\varphi([x]_R) = [p(x)]_S = [0]_S = \varphi([0]_R)$$

כלומר, $x \in \langle x^2 \rangle$. מכאן כי קיים $f(x) \in \mathbb{Q}[x]$ כך ש- $x = f(x)x^2$ אך זה לא הגיוני משיקולי דרגות, סתירה. לכן לא קיים איזומורפיזם $\varphi: R \rightarrow S$, כלומר, $R \not\cong S$.

שאלה 4. יהי חוג חילופי, יהי $a \in R$ איבר נילפוטנטי (כלומר קיים $k \in \mathbb{N}$ כך ש $a^k = 0$) ויהי פולינום $f(x) = r_n x^n + \dots + r_1 x + r_0 \in R[x]$.

א. עלינו להוכיח ש- $a = 0$ או ש- a מחלק אפס. מכיוון ש- a נילפוטנטי קיים $k \in \mathbb{N}$ מינימלי כך ש $a^k = 0$. אם $k = 1$ אז $a = 0$ וסיימנו. אחרת, $k \geq 2$, $a \neq 0$. נוכל לכתוב $a \cdot a^{k-1} = 0$. ממינימליות $k, a^{k-1} \neq 0$ ולכן לפי ההגדרה קיבלנו ש- a מחלק אפס. \square

ב. כעת צריך להוכיח כי $1 + a \in R^\times$. נתבונן במכפלה $(1 + a)(1 - a + a^2 - \dots + a^{k-1})$

$$\begin{aligned} (1 + a) \sum_{i=0}^{k-1} (-1)^i a^i &= \sum_{i=0}^{k-1} (-1)^i a^i + \sum_{i=0}^{k-1} (-1)^i a^{i+1} \\ &= 1 + \sum_{i=1}^{k-1} (-1)^i a^i - \sum_{i=0}^{k-1} (-1)^{i+1} a^{i+1} \\ &= 1 + \sum_{i=1}^{k-1} (-1)^i a^i - \sum_{i=1}^{k-1} (-1)^i a^i + (-1)^k a^k \\ &= 1 \end{aligned}$$

\square מצאנו את ההפכי של $1 + a$ ולכן $1 + a \in R^\times$.

ג. יהי $u \in R^\times$. נראה כי $u + a \in R^\times$. נשים לב כי $u + a = u(1 + u^{-1}a)$. מתקיים $(u^{-1}a)^k = (u^{-1})^k a^k = 0$ (המעבר הראשון מחילופיות R). כלומר, $u^{-1}a$ נילפוטנטי. לכן, מהסעיף הקודם $1 + u^{-1}a \in R^\times$. $u \in R^\times$ ו- R^\times היא חבורה ביחס לכפל ולכן

$$u + a = u(1 + u^{-1}a) \in R^\times$$

\square כדרוש.

ד. (\Rightarrow) : נניח $f(x)$ הפיך. כלומר, קיים פולינום $g(x) \in R[x]$ כך ש $f(x)g(x) = 1$. נסמן $g(x) = a_0 + a_1 x + \dots + a_m x^m$. מתקיים $f(0)g(0) = a_0 r_0 = 1$ כלומר r_0 הפיך (וגם a_0). כעת נכתוב

$$f(x)g(x) = c_0 + c_1 x + \dots + c_{n+m} x^{n+m} = 1$$

כאשר $c_i = \sum_{k=0}^i r_k a_{i-k}$ (נוסחה לכפל פולינומים). לכן עבור $i \geq 1$ מתקיים $c_i = 0$. בפרט, $c_{n+m} = r_n a_m = 0$. נמשיך, $r_n a_m = 0$, נקבל, $r_n^2 a_{m-1} = 0$. נמשיך כך עד שנקבל $r_n^m a_0 = 0$. $r_n^m a_0 = 0$ ונזכור ש $r_n a_m = 0$ (ראינו למעלה) ולכן $r_n^m = 0$. כלומר, r_n נילפוטנטי. מכאן כי האיבר $r_n x^n \in R[x]$ נילפוטנטי, אז מסעיף קודם, $f(x) - r_n x^n = r_{n-1} x^{n-1} + \dots + r_1 x + r_0$ הפיך (כי $f(x)$ הפיך, נתון). כעת נוכל להראות באותו האופן שגם $r_{n-1} x^{n-1}$ נילפוטנטי וכך הלאה. לכן r_1, \dots, r_n נילפוטנטיים וראינו כבר ש r_0 הפיך.

(\Leftarrow) : נניח כעת כי r_1, \dots, r_n נילפוטנטיים, r_0 הפיך. מכאן כי $r_1 x, \dots, r_n x^n \in R[x]$ נילפוטנטיים. נוכיח את טענת העזר הבאה:

יהי R חוג חילופי ויהיו $a, b \in R$ איברים נילפוטנטיים, אזי, $a + b$ נילפוטנטי.

קיימים $n, m \in \mathbb{N}$ מינימליים כך ש $a^n = 0, b^m = 0$. נוסחת הבינום של ניוטון מתקיימת בחוג קומוטטיבי ולכן

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

לכן $a+b$ נילפוטנטי. זה מסיים את טענת העזר, נחזור לתרגיל.

כעת מטענת העזר אנו יכולים לומר שהסכום $r_1x + \dots + r_nx^n$ נילפוטנטי. נתון לנו שהאיבר r_0 הפיך ולכן מסעיף ג' נקבל ש- $f(x) = r_0 + r_1x + \dots + r_nx^n$ הפיך. \square

ה. (\Rightarrow) : נניח r_0, \dots, r_n נילפוטנטיים. אזי גם $r_i x^i$ נילפוטנטיים. ראינו בסעיף הקודם שסכום נילפוטנטיים הוא נילפוטנטי ולכן גם $f(x) = r_0 + r_1x + \dots + r_nx^n$ נילפוטנטי. \square

(\Leftarrow) : נניח $f(x)$ נילפוטנטי. כלומר, קיים $m \in \mathbb{N}$ כך ש $f^m(x) = 0$ (כפולינום האפס). כלומר, כל המקדמים מתאפסים בפולינום $f^m(x)$. r_n^m הוא המקדם של $(x^n)^m$ בפולינום $f^m(x)$ ולכן $r_n^m = 0$, כלומר, r_n נילפוטנטי ומכאן גם כי $r_n x^n$ נילפוטנטי. סכום נילפוטנטיים הוא נילפוטנטי ולכן גם $f(x) - r_n x^n = r_0 + r_1x + \dots + r_{n-1}x^{n-1}$ נילפוטנטי. כעת הפולינום $r_0 + r_1x + \dots + r_{n-1}x^{n-1}$ נילפוטנטי ובאותו האופן נראה ש- r_{n-1} נילפוטנטי וכך הלאה. לבסוף נקבל r_0, \dots, r_n נילפוטנטיים. \square

שאלה 5. יהי A חוג בוליאני.

א. A הוא חוג בוליאני, כלומר, לכל $a \in A$ מתקיים $a^2 = a$. יהי $a \in A$.

$$-a = (-a)^2 = a^2 = a$$

כלומר, $a + a = 0$. \square

ב. יהי F שדה המקיים $x^2 = x$ לכל $x \in F$. יהי $x \neq 0$ אזי הוא הפיך. אם נכפול את שני אגפיה של המשוואה $x^2 = x$ ב x^{-1} נקבל $x = 1$. כלומר, האיבר היחיד ב F ששונה מ 0 הוא 1 וזה בדיוק \mathbb{F}_2 . \square

ג. יהי $M \triangleleft A$ אידיאל מקסימלי. אזי A/M הוא שדה. יהי $a + M \in A/M$.

$$a + M = a^2 + M = (a + M)(a + M) = (a + M)^2$$

מכאן כי A/M הוא חוג בוליאני ומהסעיף הקודם $A/M \cong \mathbb{F}_2$. \square

ד. יהי $M \triangleleft A$ אידיאל מקסימלי ויהי $a \in A$. אם $a \notin M$ אז מתקיים $[a] \neq [0]$ בחוג המנה. אך בחוג המנה יש שני איברים בלבד $[0]$ או $[1]$ (מהסעיף הקודם). לכן, $[a] = [1]$. כלומר, $[a] = [1]$ ומכאן כי $1 - a \in M$. באופן דומה אם $1 - a \notin M$ אז $1 - a \in M$ או $a, 1 - a \in M$ ואז $[a] = [1 - a] = [1]$ ואז $[a] = [1] = [2a] = [0]$, סתירה. סך הכל $a \in M$ או $1 - a \in M$ אך לא שניהם יחד. \square

ה. יהי $a \in A, a \neq 0$. לפי הלמה של צורן קיים $M \triangleleft A$ אידיאל מקסימלי המכיל את $\langle 1 - a \rangle$ (כמקסימום בקבוצה $\{M \subset A \mid M \triangleleft A, \langle 1 - a \rangle \subseteq M\}$ הקבוצה לא ריקה כי האידיאל $\langle 1 - a \rangle \neq A$ בה) לכן, לפי סעיף קודם, מתקיים כי $a \notin M$ וסיימנו. \square

