

פתרון תרגיל בית 7 מבוא לחוגים ומודולים 88-212 סמסטר ב' תשפ"א

שאלה 1. הסבירו מדוע המשוואה $(-1 + \sqrt{7})(1 + \sqrt{7}) = 2 \cdot 3 = 6$ לא סותרת את העובדה ש- $\mathbb{Z}[\sqrt{7}]$ הוא תחום פריקות יחידה.

פתרון. נשים לב שאלו לא גורמים אי פריקים! למשל $2 = (3 + \sqrt{7})(3 - \sqrt{7})$. אם נמשיך לפרק כל אחד מהגורמים, נקבל בסוף גורמים זהים (עד כדי חברות). חשבו את הגורמים האלו... זה אימון טוב בלפרק דברים. התשובה מופיעה בסוף הקובץ.
רמז: אם תמצאו איבר מנורמה 2 למשל, אז תקבלו פירוק $(a + b\sqrt{7})(a - b\sqrt{7}) = 2$.

שאלה 2. הראו שבפירוקים $\sqrt{-6} \cdot \sqrt{-6} = -2 \cdot 3$ בחוג $\mathbb{Z}[\sqrt{-6}]$ כל הגורמים הם אי פריקים, אינם חברים, ואינם ראשוניים.

פתרון. ניזכר בנורמה המוגדרת על $\mathbb{Z}[\sqrt{-6}]$ לפי

$$N(a + b\sqrt{-6}) = (a + b\sqrt{-6})(a - b\sqrt{-6}) = a^2 + 6b^2$$

הנורמה הזו אי-שלילית, כפלית, ובנוסף x הפיך אם ורק אם $N(x) = 1$ (אם x הפיך אז $N(x) \cdot N(x^{-1}) = 1$ ולכן $N(x) = 1$ ואם $N(x) = 1$ אז הצמוד שלו הוא ההופכי). נשים לב שאין ב- $\mathbb{Z}[\sqrt{-6}]$ איברים מנורמה 2 או 3. אכן, אילו היה פתרון למשוואה $a^2 + 6b^2 = 2$ אז $b = 0$, אבל ל-2 אין שורש שלם. עכשיו נוכל להוכיח את הדרוש.

- 2 אי פריק כי אם $2 = ab$ אז $2 = N(2) = N(a) \cdot N(b) = 4$ אין איברים מנורמה 2, לכן $N(a) = 1$ או $N(b) = 1$, כלומר אחד מהם הפיך. לכן 2 אי פריק.
- 3 אי פריק מנימוק דומה.
- $\sqrt{-6}$ אי-פריק מנימוק דומה.

מצד שני, 2 ו-3 הם לא חברים של $\sqrt{-6}$ כי אין להם את אותה נורמה. 2 ו-3 לא מחלקים את $\sqrt{-6}$, וגם לא להיפך, ולכן אף אחד מהם אינו ראשוני.

שאלה 3. יהי F שדה. הוכיחו שחוג המנה $F[x, y, z]/\langle xy - z^2 \rangle$ אינו תחום פריקות יחידה. פתרון. לכל איבר $a \in F[x, y, z]$ נסמן על ידי \bar{a} את המחלקה המתאימה לו בחוג המנה. נשים לב שבחוג המנה מתקיים

$$\bar{x} \cdot \bar{y} = \bar{z}^2$$

החלק הקשה בשאלה הוא להראות ש- \bar{x}, \bar{y} הם אי-פריקים בחוג המנה. נסמן את החוג R . לצורך זה, נטען את הטענות הבאות:

- $xy - z^2$ ראשוני ב- $F[x, y, z]$. כיוון ש- $F[x, y, z]$ תחום פריקות יחידה, מספיק להראות ש- $xy - z^2$ הוא אי-פריק ב- $F[x, y, z]$. נחשוב על חוג הפולינומים כך: $F[x, y, z] = (F[x, y])[z]$ אז אי-פריק לפי קריטריון אייזנשטיין עם $P = \langle x \rangle$ (אפשר גם להוכיח ישירות).

• x אי-פריק ב- R (ההוכחה ל- y, z דומה). נניח בשלילה $\bar{x} = \bar{f} \cdot \bar{g}$ לאילושהם $f, g \in F[x, y, z]$ לכן

$$x - fg = h(xy - z^2)$$

לאיזשהו $h \in F[x, y, z]$ נכתוב $h = \sum_{k=1}^t h_k, g = \sum_{j=0}^n g_j, f = \sum_{i=0}^m f_i$ כשכל f_i, g_j, h_k מדרגה i, j, k נניח בשלילה ש- f, g מכילים מונומים ממעלה 2 או יותר, כלומר $m, n \geq 2$. אפשר להניח $f_m, g_n \nmid (xy - z^2)$, אחרת אפשר יהיה לבחור f, g ממעלה נמוכה יותר (אם $f_m = (xy - z^2) f'$ אז $f_m g_n = (xy - z^2) f' g_n$ ואפשר יהיה לכתוב את המשוואה הקודמת כך: $(x - (f - f_m)g) = (h + f'g)(xy - z^2)$). אבל אז המקדם ההומוגני מהמעלה הכי גבוהה באגף שמאל הוא $f_m g_n$. כיוון ש- $(xy - z^2) \nmid f_m g_n$ הומוגני, כל רכיב הומוגני באגף ימין יתחלק בו. לכן $(xy - z^2) \mid f_m g_n$, בסתירה לכך ש- $xy - z^2 \nmid f_m g_n$.
אפשר להמשיך את הטיעון הזה עד שמצמצמים את כל החזקות הגבוהות ב- f, g ונשארים עם פולינומים ממעלה לכל היותר 1. אבל אז ברור שהדרך היחידה היא שאחד מהם יהיה קבוע והשני כפולה של x , ומכאן ש- x אי-פריק ב- R .
למי שהטיעון קצת בלבל אותנו, אפשר גם להסתכל על חוג המנה: כיוון ש- $xy - z^2$ ראשוני, החוג R הוא תחום שלמות. כל איבר בחוג המנה אפשר גם לכתוב כסכום של רכיבים הומוגניים בדיוק כי $xy - z^2$ הומוגני, ואיבר יהיה $\bar{0}$ אם ורק אם כל רכיב הומוגני שלו הוא $\bar{0}$. אז אפשר לחזור על הטיעון הקודם בחוג המנה, ולהראות ש- f, g חייבים להיות ממעלה לכל היותר 1 מטיעון דומה.

שאלה 4. יהי R חוג. נגדיר עבורו פונקציית נורפת איזאלים לפי $N(0) = 0$ ולכל $a \in R, a \neq 0$,
 $N(a) = |R/\langle a \rangle|$

- א. הוכיחו שאם R תחום שלמות, אז N היא פונקציה כפלית (בחשבון עוצמות).
ב. מצאו דוגמת נגד לסעיף הקודם כאשר R אינו תחום שלמות. רמז: מספיק לקחת R סופי.

פתרון.

א. יהיו $a, b \in R$. אם $a = 0$ או $b = 0$ ברור ש- $N(ab) = 0 = N(a)N(b)$, ולכן נניח $a, b \neq 0$. כיוון ש- R תחום שלמות, $ab \neq 0$.
נגדיר $f: R/\langle ab \rangle \rightarrow R/\langle a \rangle$ לפי $f(r + \langle ab \rangle) = r + \langle a \rangle$. כיוון ש- $\langle ab \rangle \subseteq \langle a \rangle$, ההעתקה מוגדרת היטב, וזהו אפימורפיזם. הגרעין הוא

$$\ker f = \{r + \langle ab \rangle \mid r \in \langle a \rangle\} = \langle a \rangle / \langle ab \rangle$$

לכן $|R/\langle a \rangle| = |R/\langle ab \rangle| \cdot |\ker f| = |R/\langle a \rangle| \cdot |\langle a \rangle / \langle ab \rangle|$. נותר להראות ש- $|R/\langle ab \rangle| = |R/\langle b \rangle| \cdot |\langle a \rangle / \langle ab \rangle|$, ואת זה נעשה על ידי $g: R/\langle b \rangle \rightarrow \langle a \rangle / \langle ab \rangle$ המוגדרת על ידי $g(r + \langle b \rangle) = ar + \langle ab \rangle$. ההעתקה הזו היא חיבורית ועל, אבל הפעם

$$\ker g = \{r + \langle b \rangle \mid ar \in \langle ab \rangle\} = \{r + \langle b \rangle \mid \exists s \in R : ar = abs\} =$$

$$= \{r + \langle b \rangle \mid \exists s \in R : r = bs\} = \{r + \langle b \rangle \mid r \in \langle b \rangle\} = \{0 + \langle b \rangle\}$$

כלומר g גם חח"ע. זה מראה ש- $|R/\langle b \rangle| = |\langle a \rangle / \langle ab \rangle|$, ובסך הכל נקבל $N(ab) = N(a)N(b)$.

שימו לב שההעתקה הטבעית $R/\langle ab \rangle \rightarrow R/\langle a \rangle \times R/\langle b \rangle$ לא תעבוד במקרה הזה, כי אם ניקח למשל $a = b$ היא לא תהיה חח"ע או על.

ב. ניקח את החוג $R = \mathbb{Z}/4\mathbb{Z}$ ואת $a = b = 2 + 4\mathbb{Z}$. במקרה הזה $N(a) = N(b) = 2$ אבל $N(ab) = N(0 + 4\mathbb{Z}) = 0$

שאלה 5. בתרגיל זה נמצא את כל האיברים הראשוניים של $\mathbb{Z}[i]$. כזכור, $\mathbb{Z}[i]$ הוא אוקלידי ביחס לפונקציית הנורמה המושרית מ- \mathbb{C} , ולכן איבר הוא ראשוני אם ורק אם הוא אי-פריק.

- א. הוכיחו שאם $2 < p \in \mathbb{Z}$ מספר ראשוני כך ש- $p \equiv 3 \pmod{4}$, אז אי-פריק ב- $\mathbb{Z}[i]$.
- ב. הוכיחו כי אם π אי-פריק ב- $\mathbb{Z}[i]$, אז קיים מספר ראשוני $p \in \mathbb{Z}$ כך ש- $p \mid \pi$.
- ג. הוכיחו שאם $\alpha \in \mathbb{Z}[i]$ מקיים $N(\alpha)$ מספר ראשוני, אז α אי-פריק.
- ד. הוכיחו שאם $p \equiv 1 \pmod{4}$ אז קיים $a+bi \in \mathbb{Z}[i]$ אי-פריק שעבורו $N(a+bi) = p$ (מותר להשתמש בטענה הבאה מתורת המספרים ללא הוכחה: אם $p \equiv 1 \pmod{4}$ מספר ראשוני, אז קיים $x \in \mathbb{Z}$ כך ש- $x^2 \equiv -1 \pmod{p}$).
- ה. הסיקו מיהם כל האיברים הראשוניים ב- $\mathbb{Z}[i]$ עד כדי חברות (אל תשכחו לפרק את האיבר i !).

פתרון. לאורך כל השאלה ניעזר בנורמה $N(a+bi) = a^2 + b^2$ המוגדרת על $\mathbb{Z}[i]$. כמו כן, נזכור כי היא כפלית (ולמעשה $\mathbb{Z}[i]$ אוקלידי ביחס אליה). שימו לב גם ש- x הפיך ב- $\mathbb{Z}[i]$ אם ורק אם $N(x) = 1$ (זה יכול לנבוע מהאוקלידיות, או מהוכחה ישירה – ההופכי של x ב- \mathbb{C} הוא $\frac{\bar{x}}{N(x)}$, וקל לוודא שזה איבר של $\mathbb{Z}[i]$ אם ורק אם $N(x) = 1$).

א. נניח בשלילה $p = x \cdot y$ עבור $x, y \in \mathbb{Z}[i]$ לא הפיכים. נשווה נורמות: $p^2 = N(p) = N(x) \cdot N(y)$. כיוון ש- x, y לא הפיכים, $N(x), N(y) \neq 1$, ולכן $N(x) = N(y) = p$. נכתוב $x = a+bi$, ונקבל $x^2 = a^2 - b^2 + 2abi = p$. אבל למשוואה הזו אין פתרון: אם נסתכל עליה מודולו 4, נקבל ש-3 הוא סכום של שני ריבועים, אך הריבועים היחידים ב- $\mathbb{Z}/4\mathbb{Z}$ הם 0, 1. קיבלנו סתירה, ולכן p אי-פריק.

ב. נתבונן בנורמה $N(\pi)$ של π . זהו מספר טבעי, ולכן אפשר לפרק $N(\pi) = p_1 \cdots p_k$ למספרים ראשוניים ב- \mathbb{N} . אבל π איבר ראשוני ב- $\mathbb{Z}[i]$ ו- $N(\pi) = p_1 \cdots p_k$ כלומר $N(\pi) = p_1 \cdots p_k$. לכן קיים ראשוני p_i ברשימה שעבורו $\pi \mid p_i$.

ג. נניח $\alpha = \beta\gamma$. אז $N(\alpha) = N(\beta)N(\gamma)$. אבל $N(\alpha)$ ראשוני, לכן $N(\beta) = 1$ או $N(\gamma) = 1$, כלומר β הפיך או γ הפיך. זה מראה ש- α אי-פריק.

ד. לפי הטענה שהוזכרה, קיים $a \in \mathbb{Z}$ שעבורו $a^2 \equiv -1 \pmod{p}$. לכן $a^2 + 1 \equiv 0 \pmod{p}$. כלומר $a^2 + 1 = (a+i)(a-i)$. כיוון ש- $p \mid a^2 + 1$, נניח בשלילה ש- p אי-פריק ב- $\mathbb{Z}[i]$. כיוון ש- $\mathbb{Z}[i]$ אוקלידי, p יהיה ראשוני, ולכן $p \mid (a+i)$ או $p \mid (a-i)$. נניח בה"כ $p \mid (a+i)$. על ידי הצמדה, נקבל $\bar{p} \mid \overline{a+i} = a-i$. כלומר $p \mid (a-i)$. לכן $p \mid (a+i)$ וגם $p \mid (a-i)$. נקבל $p \mid (a+i+a-i) = 2a$. אבל $p \neq 2$ ראשוני ולכן $p \mid a$. בסתירה (כי i הפיך).

זה מראה ש- p פריק. אם נכתוב $p = xy$ עבור $x, y \in \mathbb{Z}[i]$ לא הפיכים, נקבל $p^2 = N(p) = N(x)N(y)$. ומכאן בדומה לקודם $N(x) = N(y) = p$. לכן x ו- y אי-פריקים, מהסעיף הקודם.

ה. האיברים הראשוניים ב- $\mathbb{Z}[i]$ עד כדי חברות הם:

- $1+i$ (וחברו $1-i$) – המחלקים של 2;
- כל ראשוני $p \equiv 3 \pmod{4}$;

• לכל ראשוני $p \equiv 1 \pmod{4}$, אם $p = a^2 + b^2$ (יש הצגה יחידה כזו לפי מה שהוכחנו) אז $a \pm bi$ הם איברים ראשוניים ב- $\mathbb{Z}[i]$.

שאלה 6. יהי R תחום פריקות יחידה. נגדיר לכל $a \in R \setminus \{0\}$ את $\mu(a)$ להיות מספר הגורמים האי פריקים בפירוק של a ב- R . זה מוגדר היטב מפני ש- R הוא תחום פריקות יחידה.

יהיו $a, b \in R \setminus \{0\}$ כך ש- $a \mid b$. הוכיחו $\mu(a) \leq \mu(b)$ ושיש שיוויון אם ורק אם $a \sim b$. בפרט, a הפיך אם ורק אם $\mu(a) = 0$.

פתרון. נכתוב $b = ac$ עבור $c \in R \setminus \{0\}$. נניח שהפירוק של a למכפלה של אי-פריקים הוא $a = p_1 \cdots p_n$. נחלק לשני מקרים:

• הפיך: במקרה הזה הפירוק של b לאיברים אי-פריקים הוא (למשל) $b = (cp_1)p_2 \cdots p_n$. קל להשתכנע שכל איבר במכפלה הזו אי-פריק (חוץ מהראשון כולם אי-פריקים, והראשון הוא חבר של אי-פריק ולכן אי-פריק בעצמו מתרגיל שפתרנו). במקרה זה $\mu(a) = \mu(b)$.

• לא הפיך: אז אפשר לפרק את c למכפלה $c = q_1 \cdots q_m$ של אי-פריקים. כעת אפשר לכתוב $b = p_1 \cdots p_n q_1 \cdots q_m$. לא יכול להיות שמופיע פה איבר וההופכי שלו, כי כל איבר אי-פריק הוא לא הפיך. לכן $\mu(b) = n + m > \mu(a)$.

בסך הכל מתקיים $\mu(a) \leq \mu(b)$, ורואים שהשוויון הוא בדיוק כאשר c הפיך, כלומר $a \sim b$.

שאלה 7. יהי F שדה. לכל $n \in \mathbb{N}$ נגדיר $R_n = F[x^{1/n!}]$. למשל $R_1 = F[x]$ ו- $R_2 = F[x^{1/2}]$ שימו לב שמתקיים

$$R_1 \subseteq R_2 \subseteq R_3 \subseteq \dots$$

(למה? כי בשלב n מוסיפים ל- R_{n-1} איבר t שמקיים $t^n = x^{1/(n-1)!}$, ונסתכל על החוג שהוא האיחוד $R = \bigcup_n R_n$.)

א. הוכיחו שלכל $0 < r \in \mathbb{Q}$ מתקיים $x^r \in R$. השתכנעו שאיברי R הם סכומים סופיים מהצורה $\sum a_i x^{r_i}$ עבור $a_i \in F$ ו- $0 < r_i \in \mathbb{Q}$.

ב. הוכיחו כי R אינו תחום אטומי (תחום פריקות). רמז: הראו שאם $y \in R$ הוא מחלק אמיתי של x , אז הוא מן הצורה $\pm x^r$ עבור $0 < r < 1$, ואילו $\pm x^r$ פריק.

ג. הראו שלכל $n, m \in \mathbb{N}$ החוגים R_n, R_m איזומורפיים, אבל R לא איזומורפי אליהם.

פתרון.

א. יהי $0 < r = \frac{m}{n}$. נשים לב כי $r = \frac{m \cdot (n-1)!}{n!}$, ולכן $x^r \in R_n \subseteq R$. לגבי הטענה השנייה, כל איבר של R הוא איבר באיזשהו R_n , וכל איבר ב- R_n הוא פולינום ב- $x^{1/n!}$, שיהיה מהצורה הנ"ל.

ב. שימו לב שיש פה טעות קטנה בניסוח: יהיה מהצורה αx^r לאיזשהו α הפיך. מה שכתוב היה נכון אם היינו מחליפים את F ב- \mathbb{Z} למשל.

נניח ש- y מחלק של x^r . אפשר לכתוב $x^r = yz$ לאיזשהו $z \in R$. נכתוב $y = \sum_{i=1}^n a_i x^{r_i}$ ו- $z = \sum_{j=1}^m b_j x^{s_j}$ עבור $0 < r_i, s_j \in \mathbb{Q}$, $a_i, b_j \in F^\times$. במכפלה נקבל

$$yz = \sum_{i,j} a_i b_j x^{r_i + s_j}$$

נניח בה"כ $r_1 < \dots < r_n$ ו- $s_1 < \dots < s_m$. אז המונום עם המעלה הכי נמוכה ב- yz הוא $a_1 b_1 x^{r_1 + s_1}$, והמונום עם המעלה הכי גבוהה ב- yz הוא $a_n b_m x^{r_n + s_m}$. אבל התוצאה צריכה להיות x^r , כלומר מכילה רק מונום אחד; לכן אין ברירה וחייבים לקחת $m = n = 1$ (אחרת במכפלה יהיה יותר ממונום אחד), כלומר y הוא מהצורה המבוקשת.

למה זה מראה ש- R אינו תחום אטומי? אילו הוא היה תחום אטומי, היה איבר אי-פריק שמחלק את x^r , אבל עכשיו הוכחנו שכל המחלקים שלו פריקים.

ג. נראה שלכל $R_{n+1} \cong R_n, n \in \mathbb{N}$. נגדיר $\varphi : R_{n+1} \rightarrow R_n$ לפי $\varphi(f(x)) = f(x^{n+1})$. בצורה ברורה יותר, ההומומורפיזם φ שומר על הסקלרים מ- F (שולח אותם לעצמם), ואת $x^{1/(n+1)!}$ שולח ל- $x^{1/n!}$. קל לוודא שזה מגדיר איזומורפיזם. מצד שני, כל אחד מהחוגים R_n הוא תחום אטומי (ואפילו אוקלידי, כי הוא איזומורפי לחוג פולינומים מעל שדה), ואילו R אפילו לא תחום אטומי.

שאלה 8. רשות: יהי F שדה. הוכיחו שבחוג $F[x]$ יש אינסוף איברים ראשוניים. רמז: הוכחה המיוחסת לאוקלידס.

פתרון. נניח בשלילה שיש מספר סופי של ראשוניים p_1, \dots, p_n . נגדיר $f = p_1 \cdots p_n + 1$. כזכור, החוג $F[x]$ הוא תחום פריקות יחידה, ולכן f הוא הפיך, אי-פריק (ולמעשה ראשוני) או שאפשר לפרק אותו למכפלה של ראשוניים. קל לראות ש- f לא מתחלק באף p_i , ולכן האפשרות האחרונה נפסלת. כמו כן, f לא הפיך כי הוא לא קבוע (ראינו שהאיברים ההפיכים ב- $F[x]$ הם הקבועים, והפולינום x הוא ראשוני, לכן אפשר להניח $p_1 = x$ ואז f לא קבוע). נותרנו עם כך ש- f הוא אי-פריק, ולכן ראשוני, בעצמו. אך הוא לא אף פולינום מהרשימה, בסתירה.

פתרון (בחזרה לשאלה 1). הפירוק של 6 לגורמים אי-פריקים ב- $\mathbb{Z}[\sqrt{7}]$ הוא

$$6 = (3 + \sqrt{7})(3 - \sqrt{7})(2 + \sqrt{7})(-2 + \sqrt{7})$$

כל אחד מהגורמים האלו אי-פריק (ולמעשה ראשוני) כי הנורמה שלו ראשונית (הנורמה של השניים הראשונים היא 2, ואילו הנורמה של השניים האחרונים היא 3).

בהצלחה!