

פתרון תרגיל בית 7 אלגברה מופשטת 2

1. הוכיחו או הפריכו עבור תח"ש $S \subseteq R$:

- (א) כל איבר אי-פריק ב $S[x]$ הוא אי-פריק ב $R[x]$.
הפרכה: $\mathbb{R} \subseteq \mathbb{C}$, $x^2 + 1$ הוא אי-פריק ב $\mathbb{R}[x]$ (כי אין לו שורש), ופריק ב $\mathbb{C}[x]$.
- (ב) כל איבר אי-פריק ב $R[x]$ הוא אי-פריק ב $S[x]$.
הפרכה: $\mathbb{Z} \subseteq \mathbb{Q}$, $2x + 2$ הוא אי-פריק ב $\mathbb{Q}[x]$ אבל פריק ב $\mathbb{Z}[x]$.

2. חוג R נקרא reduced אם לכל $x \in R$, $x = 0 \iff x^2 = 0$.

(א) הוכיחו כי חוג קומוטטיבי הוא reduced אם"ם אין בו איברים נילפוטנטים פרט ל-0.

\Rightarrow אם $x^2 = 0$ אז הוא נילפוטנט ולכן לפי ההנחה $x = 0$.
 \Leftarrow נניח $x^n = 0$, אם n זוגי אז $(x^{n/2})^2 = 0$ ולכן $x^{n/2} = 0$ ובאינדוקציה.
 אם n אי-זוגי אז נכפול ב x ונקבל $x^{n+1} = 0$ שזה חזקה זוגית, וכמו קודם נקבל $x^{\frac{n+1}{2}} = 0$.

(ב) הוכיחו כי חוג קומוטטיבי הוא תח"ש אם"ם הוא reduced וחיתוך של כל שני אידיאלים לא אפסיים הוא לא אפס.

\Leftarrow ראינו בתירגול שבתח"ש החיתוך של שני אידיאלים לא אפסיים הוא לא אפס. וכמו כן, בתח"ש אין נילפוטנטים פרט לאפס.

\Rightarrow נניח $a, b \in R$, $a \neq 0$ ונניח בשלילה ש $ab = 0$.
 האידיאלים $Ra, Rb \neq 0$ ולכן לפי ההנחה יש $c \in Ra \cap Rb$, $c \neq 0$.
 נרשום $c = xa = yb$ עבור איזשהם $x, y \in R$.
 מכיוון שהחוג הוא reduced, $c^2 \neq 0$.
 אבל אם $ab = 0$ אז $0 = xyab = (xa)(yb) = c^2$ — סתירה!

3. (א) הוכיחו כי בחוג \mathcal{O}_d , אם איברים x, y הם חברים אז $N(x) = \pm N(y)$.
 ראינו שאיבר הפיך הוא מנורמה ± 1 .

אם $x = uy$ עבור איבר הפיך u , אז מכפלות הנורמה
 $N(x) = N(uy) = N(u)N(y) = \pm N(y)$

(ב) הסיקו כי $3 + \sqrt{2}, 5 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ הם לא חברים.

נחשב את הנורמות שלהם:

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

$$N(5 + 2\sqrt{2}) = 5^2 - 2^2 \cdot 2 = 17$$

ולכן הם לא יכולים להיות חברים.

(ג) תנו דוגמה לאיברים בעלי אותה נורמה, שהם לא חברים ולא צמודים זה לזה.

פתרון: $3 + 4i, 4 + 3i$

4. יהי $d \in \mathbb{Z}$ חופשי מריבועים, ונתבונן בחוג

$$S = \left\{ \begin{pmatrix} a & b \\ bd & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\} \subseteq M_2(\mathbb{Z})$$

(א) הוכיחו כי $\varphi: \mathbb{Z}[\sqrt{d}] \rightarrow S$ המוגדר ע"י $\varphi(a + b\sqrt{d}) = \begin{pmatrix} a & b \\ bd & a \end{pmatrix}$ הוא

איזומורפיזם של חוגים.

(ב) הוכיחו כי אם $d \equiv 1 \pmod{4}$ אז $\varphi: \mathcal{O}_d \rightarrow \left\{ \begin{pmatrix} a & b \\ b\frac{d-1}{4} & a+b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$ הוא

איזומורפיזם.

להבהרה, הפונקציה היא $\varphi \left(a + b \left(\frac{1 + \sqrt{d}}{2} \right) \right) = \begin{pmatrix} a & b \\ b\frac{d-1}{4} & a+b \end{pmatrix}$

למשל

$$\begin{aligned} \varphi \left(\begin{pmatrix} a + b \left(\frac{1 + \sqrt{d}}{2} \right) \\ \left(x + y \left(\frac{1 + \sqrt{d}}{2} \right) \right) \end{pmatrix} \right) &= \varphi \left(\begin{pmatrix} ax + by \frac{d-1}{4} + (ay + bx + by) \left(\frac{1 + \sqrt{d}}{2} \right) \\ \left(ax + by \frac{d-1}{4} \right) \quad \left(ay + bx + by \right) \end{pmatrix} \right) = \\ &= \begin{pmatrix} * & * \\ * & * \end{pmatrix} = \\ &= \begin{pmatrix} a & b \\ b\frac{d-1}{4} & a+b \end{pmatrix} \begin{pmatrix} x & y \\ y\frac{d-1}{4} & x+y \end{pmatrix} \end{aligned}$$

(ג) חשבו מהי התמונה של הנורמה של איבר כללי ב \mathcal{O}_d (כלומר מהו $\varphi(N(x))$ עבור

איבר כללי $x \in \mathcal{O}_d$ בכל אחד מהמקרים $d \equiv 1 \pmod{4}, d \not\equiv 1 \pmod{4}$.

נשים לב ש $\varphi(N(x)) = \det(\varphi(x)) I_2$ (הוכיחו את הפרטים...)

5. נתבונן בחוג $\mathbb{Z}[\sqrt{3}]$ ובאידיאל $I = \langle -5 + \sqrt{3} \rangle$.

(א) הוכיחו כי בחוג המנה $\mathbb{Z}[\sqrt{3}]/I$ יש 22 איברים.

נשים לב כי $N(-5 + \sqrt{3}) = 22$, ולכן לפי טענה מהתרגול אנחנו יודעים שהמנה צריכה להיות מגודל 22.

נוכיח זאת ישירות:

מכיוון ש $22 = (-5 + \sqrt{3})(-5 - \sqrt{3}) \in I$ או $22 = \bar{0}$ במנה ולכן

$$\mathbb{Z}[\sqrt{3}]/I = \{ \overline{a + b\sqrt{3}} \mid a, b \in \{0, 1, 2, \dots, 21\} \}$$

בנוסף, $\sqrt{3} = \bar{5}$ ולכן $\overline{a + b\sqrt{3}} = \overline{a + 5b}$

מה שנותן $\mathbb{Z}[\sqrt{3}]/I = \{ \bar{a} \mid a, b \in \{0, 1, 2, \dots, 21\} \}$

נשאר להראות ש \bar{a} הם איברים שונים, ואז יש בדיוק 22 איברים.

ניח $\bar{a} = \bar{b}$ כאשר $a, b \in \{0, 1, 2, \dots, 21\}$, אזי $a - b \in I$ כלומר

$$\begin{aligned} b - a &= (-5 + \sqrt{3})(x + y\sqrt{3}) \\ &= (-5x + 3y) + (-5y + x)\sqrt{3} \end{aligned}$$

$$b - a = -22y \Leftrightarrow \begin{cases} x - 5y = 0 \\ -5x + 3y = b - a \end{cases} \quad \text{נשווה אגפים ונקבל}$$

ומכיוון $|b - a| \leq 21$ אז בהכרח $b - a = 0$.

(ב) נגדיר $\varphi: \mathbb{Z}[\sqrt{3}] \rightarrow \mathbb{Z}_{11}$ ע"י $\varphi(a + b\sqrt{3}) = a + 5b$. השתכנעו שזהו אפימורפיזם.

(ג) הוכיחו כי $I \not\subseteq \ker \varphi$.

$\varphi(-5 + \sqrt{3}) = -5 + 5 = 0$ שכן $I \subseteq \ker \varphi$.

$\varphi(11) = 11 \equiv 0 \pmod{11}$ אבל $11 \notin I$.

נוכיח זאת: אם $11 = (-5 + \sqrt{3})(x + y\sqrt{3})$

$$\text{אז נקבל מערכת} \begin{cases} 11 = -5x + 3y \\ 0 = x - 5y \end{cases} \text{ שאין לה פתרון בשלמים.}$$

(ד) הוכיחו כי $\mathbb{Z}[\sqrt{3}]/\langle -5 + \sqrt{3}, 11 \rangle \cong \mathbb{Z}_{11}$.

ראינו ש $-5 + \sqrt{3}, 11 \in \ker \varphi$ ולכן $\langle -5 + \sqrt{3}, 11 \rangle \subseteq \ker \varphi$.

נקח $x + y\sqrt{3} \in \ker \varphi$, אזי $x + 5y \equiv 0 \pmod{11}$ כלומר $x \equiv 6y \pmod{11}$.

זה נותן איברים מצהצורה

$$6y + 11k + y\sqrt{3} = y(-5 + \sqrt{3}) + 11(y + k) \in \langle -5 + \sqrt{3}, 11 \rangle$$

וכך האיזומורפיזם הדרוש נובע ממשפט האיזומורפיזם הראשון.

6. קבעו ונמקו האם האיברים הבאים הם אי-פריקים בחוג המצויין, באם הם פריקים-מצאו פירוק שלהם :

(א) 7 בחוג $\mathbb{Z}[i]$.

פתרון: אי פריק.

כי אם $7 = (a + ib) \cdot z$ אז מכפילות הנורמה $49 = (a^2 + b^2)N(z)$ וכדי שהפירוק יהיה לא טריוויאלי בהכרח $a^2 + b^2 = 7 \equiv 3 \pmod{4}$ ולזה אין פתרון.

(ב) $1 + 3i$ בחוג $\mathbb{Z}[i]$.

פתרון: פריק.

$$1 + 3i = (1 + i)(2 + i)$$

(ג) 23 בחוג $\mathbb{Z}[\sqrt{-19}]$.

פתרון: אי פריק.

נניח בשלילה ש $23 = (a + b\sqrt{-19}) \cdot z$. מכפילות הנורמה $23^2 = (a^2 + 19b^2)N(z)$ בשביל שהפירוק יהיה אמיתי בהכרח $23 = a^2 + 19b^2$ ניקח מודולו 4: $a^2 + b^2 \equiv 3 \pmod{4}$ ואין לזה פתרון.

7. מצאו את כל הפתרונות או הוכיחו כי אין פתרונות מעל \mathbb{Z} למשוואות:

(א) $x^2 + y^2 = 3z^2$

פתרון: אין פתרונות חוץ מהטריוויאלי.

נניח שיש בשלילה שיש פתרון (x, y, z) ,

אפשר להניח ש x, y זרים, אחרת נחלק ב \gcd^2 שלהם (ונקבל ש $(\frac{x}{\gcd}, \frac{y}{\gcd}, \frac{z}{\gcd})$

הוא גם פתרון).

$x^2 + y^2 \equiv 0 \pmod{3}$ גורר ש $x \equiv y \equiv 0 \pmod{3}$ (אין עוד פתרונות מודולו 3)

מה שאומר ש $3|x, y$ בסתירה לכך שהם זרים.

(ב) $x^2 + 1 = y^3$

פתרון:

אם x הוא אי זוגי אז $x^2 + 1 \equiv 2 \pmod{4}$ (הוא או 1 או 3 והריבוע בכל

מקרה 1) ואז אין פתרון.

נניח ש x הוא זוגי.

מעל החוג $\mathbb{Z}[i]$ נקבל ש $(x + i)(x - i) = y^3$.

[קבלנו שני פירוקים לאותו איבר ובגלל ש $\mathbb{Z}[i]$ הוא תפ"י, זה מלמד אותנו על

הקשר בין הגורמים (צריכים להיות חברים).]

ראשית נלמד טוב את הפירוק השמאלי:

$x + i$ ו $x - i$ הם זרים בחוג, כי כל גורם אי פריק שמחלק את $x + i$ וגם את

$x - i$ מחלק גם את $2i$ $(x + i) - (x - i) = 2i$.
 אבל את $2i$ מחלק רק $1 + i$ והוא לא מחלק את $x \pm i$ (כי x זוגי).

מכיוון שהגורמים השמאליים זרים, הגורמים האי-פריקים שמחלקים את y מחלקים או את $x + i$ או את $x - i$ ולא את שניהם.
 ולכן יוצא שאם נניח $p|y$ ו $p|(x + i)$ אז $p^3|(x + i)$.
 וזה אומר שיש איבר $a + bi \in \mathbb{Z}[i]$ כך ש

$$x + i = (a + bi)^3$$

אחרי פתיחת סוגרים מקבלים

$$\begin{aligned} x &= a(a^2 - 3b^2) \\ 1 &= (3a^2 - b^2)b \end{aligned}$$

מהמשוואה השנייה רואים ש $b = \pm 1$, אם נציב $b = 1$ נקבל סתירה, ונשארו רק אם הפתרון $a = 0, b = -1$ מה שאומר ש $-i = (-i)^3 - i$, $x = 0, y = 1$ הוא הפתרון היחיד.

$$(ג) \quad x^2 + 19 = y^3$$

פתרון:

מעל החוג $\mathbb{Z}[\sqrt{-19}]$ נקבל $(x + \sqrt{-19})(x - \sqrt{-19}) = y^3$.
 נרצה להראות ששני הגורמים בפירוק הם זרים, כל גורם משותף מחלק את $2\sqrt{-19}$ ולכן מספיק להראות ש $x + \sqrt{-19}$ ו $2\sqrt{-19}$ הם זרים.

אם x הוא אי-זוגי אז $x^2 + 19 \equiv 4 \pmod{8}$ ואין פתרון למשוואה.
 אם x מתחלק ב-19 אז $x^2 + 19 \equiv 19 \pmod{19^2}$ ואין פתרון.
 נניח x הוא זוגי ולא מתחלק ב-19, אזי $x^2 + 19$ זר ל-19 ולכן (תכונת בזו של \mathbb{Z}) יש α, β כך ש $\alpha(x^2 + 19) + \beta 38 = 1$ זה נותן

$$(\alpha(x - \sqrt{-19}))(x + \sqrt{-19}) + (\beta\sqrt{-19})(2\sqrt{-19}) = 1$$

ולכן (לפי תכונת בזו של $\mathbb{Z}[\sqrt{-19}]$, ו $x + \sqrt{-19}$ ו $2\sqrt{-19}$ זרים).
 כעת, כמו בסעיף הקודם, מכיוון שהגורמים זרים יש $a + b\sqrt{-19}$ כך ש $x + \sqrt{-19} = (a + b\sqrt{-19})^3$.
 זה נותן משוואות

$$\begin{aligned} x &= a(a^2 - 57b^2) \\ 1 &= (3a^2 - 19b^2)b \end{aligned}$$

לפי המשוואה השנייה $b = \pm 1$, ע"י הצבה רואים ששניהם לא אפשריים, ולכן
המסקנה היא שאין פתרון למשוואה!