

אלגברה מופשטת 2 – תרגיל בית 7

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

1. הוכיחו או הפריכו:

a. $4 - \sqrt{2}, 2 + 3\sqrt{2}$ הם חברים ב $\mathbb{Z}[\sqrt{2}]$.

b. 23 אי-פריק ב $\mathbb{Z}[\sqrt{-19}]$.

c. כאשר R הוא תת-תחום שלמות של S

i. כל איבר א-פריק ב $R[x]$ אי-פריק ב $S[x]$.

ii. כל איבר א-פריק ב $S[x]$ אי-פריק ב $R[x]$.

פיתרון:

$$4 - \sqrt{2} \cdot (2 + 3\sqrt{2})^{-1} = 4 - \sqrt{2} \cdot \frac{2 - 3\sqrt{2}}{(2 - 3\sqrt{2})(2 + 3\sqrt{2})} = \frac{8 + 6 - 14\sqrt{2}}{-14} = \sqrt{2} - 1$$

$\sqrt{2} - 1 \in \mathbb{Z}[\sqrt{2}]$ הוא הפיך, ולכן $4 - \sqrt{2}, 2 + 3\sqrt{2}$ חברים.

$$23 = (2 + \sqrt{-19}) \cdot (2 - \sqrt{-19})$$

שהנורמה שלהם היא 23, ולכן 23 פריק.

מספיק לראות דוגמאות שבהן יש איבר אי פריק ב R שפריק ב S ולהיפך. אם לוקחים

$$S = \mathbb{Z}\left[\frac{1}{2}\right] \text{ ו } R = \mathbb{Z} \text{ אזי } 6 \text{ אי-פריק ב } S \text{ אך לא ב } R. \text{ מאידך, } 2 \text{ אי-פריק ב } R \text{ אך לא ב } S.$$

2. הוכיחו כי אם $d \equiv 1 \pmod{4}$ אזי $\mathbb{Z}[\sqrt{d}]$ אינו תחום פריקות יחידה. [רמז: הסתכלו

$$\text{על } a = 1 + \sqrt{d} \text{ והראו ש } 2 \mid a^2$$

פיתרון:

נביט ב $a = 1 + \sqrt{d}$. כעת, $a^2 = 1 + d + 2\sqrt{d}$. $1 + d$ הוא זוגי משום ש $d \equiv 1 \pmod{4}$ (ולכן d אי-זוגי). לכן

$$a^2 = 2 \cdot \left(\frac{1+d}{2} + \sqrt{d} \right) \text{ משמע } \frac{a^2}{2} = \frac{1+d+2\sqrt{d}}{2} = \frac{1+d}{2} + \sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

ניתן לראות מכך ש 2 לא ראשוני, משום שאינו מחלק את a .

נותר להראות ש 2 אי-פריק, ואז לא ייתכן ש $\mathbb{Z}[\sqrt{d}]$ תפחום פריקות יחידה.

לו היו קיימים $2 = xy$ כך ש x, y לא הפיכים, אזי $N(x) = N(y) = 2$.

נסמן $x = b + c\sqrt{d}$. $2 = N(x) = b^2 - c^2d \equiv b^2 - c^2 \pmod{4}$. אולם,

הריבועים היחידים ב \mathbb{Z}_4 הם 0 ו 1 , והחסור בין שניים לעולם לא יכול להיות 2 , סתירה.

3. הסבירו מדוע זה ש $6 = 2 \cdot 3 = (1 + \sqrt{7})(-1 + \sqrt{7})$ אינו סותר את העובדה כי

$\mathbb{Z}[\sqrt{7}]$ הוא תחום פריקות יחידה.

פיתרון:

שני הצדדים מתפרקים למכפלה $2 = (3 + \sqrt{7})(3 - \sqrt{7})$ $3 = (2 + \sqrt{7})(-2 + \sqrt{7})$

$$-1 + \sqrt{7} = (3 - \sqrt{7})(2 + \sqrt{7}), 1 + \sqrt{7} = (3 + \sqrt{7})(-2 + \sqrt{7})$$

שני הפירוקים לכאורה אינם פירוקים למספרים אי-פריקים, ואם מפרקים כל אחד מהם באמת

לגורמים אי-פריקים מגיעים לאותו הפירוק $(2 + \sqrt{7})(-2 + \sqrt{7})(3 + \sqrt{7})(3 - \sqrt{7})$.

4. הראו כי המספר 21 ניתן להצגה בשלוש דרכים שונות ב $\mathbb{Z}[\sqrt{-5}]$ כמכפלה של שני

איברים. [כלומר קיימים $a, b, c, d, e, f \in \mathbb{Z}[\sqrt{-5}]$ כך ש $21 = ab = cd = ef$ וגם

אף אחד מהאיברים לא מחלק את חמשת האחרים]

פיתרון: $21 = 3 \cdot 7 = (1 + 4\sqrt{-5})(1 - 4\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5})$

הנורמות הן 9 ל-3, 49 ל-7, ו-21 לשאר הארבע, לכן ברור ש-3 ו-7 לא מחלקים ולא מתחלקים באף אחד אחר.

לגבי האחרים, לו אחד היה מתחלק בשני אז שניהם היו חברים, כלומר מתחלקים זה בזה. מספר הבדיקות אם כן מצטמצם, וקל לבדוק בדרך הבאה

$$(1 + 4\sqrt{-5})(4 + \sqrt{5})^{-1} = \frac{(1 + 4\sqrt{-5})(4 + \sqrt{-5})}{21} = \frac{-96 + 17\sqrt{5}}{21} \notin \mathbb{Z}[\sqrt{-5}]$$

ולכן שני המספרים האלה לא מתחלקים זה בזה.

5. האם $\mathbb{Z}[\sqrt{10}]$ הוא תחום פריקות יחידה?

פיתרון:

לא. $6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$. הנורמות הן 4 של 2, 9 של 3 ו-6 של שני האחרים. לו אחד מהמספרים האלה היה פריק אזי היה איבר שהנורמה שלו מחלקת את אחת הנורמות המוזכרות אך לא שווה לה, כלומר הנורמה הייתה 2 או 3. יהי מספר כלשהו $a + b\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$. הנורמה שלו היא $a^2 - 10b^2$, ומודולו 10 זה שווה ל- a^2 . אולם, המספרים 2 ו-3 אינם ריבועים ב- \mathbb{Z}_{10} , ולכן לא קיימים מספרים ב- $\mathbb{Z}[\sqrt{10}]$ מנורמה 2 או 3, ולכן $4 - \sqrt{10}, 4 + \sqrt{10}, 2, 3$ הם אי-פריקים. הפירוקים הם כמובן שונים (בגלל הנורמות) ולכן $\mathbb{Z}[\sqrt{10}]$ אינו תחום פריקות יחידה.

6. יהי $p \in \mathbb{Z}$ ראשוני. הוכיחו כי אם קיימים שלמים x, y כך ש- $p \mid (x^2 + y^2)$ אך

$$p^2 \nmid (x^2 + y^2) \text{ אז } p \text{ לא ראשוני ב-} \mathbb{Z}[i]$$

פיתרון: אם קיימים x, y כאלה, אזי נביט ב- $z = x + yi$. אם $p \mid x, y$ אזי

$$p^2 \mid x^2 + y^2, \text{ בסתירה להנחה. לכן נניח ש-} p \text{ לא מחלק לפחות אחד מהם.}$$

לכן, p לא מחלק את z ולא את \bar{z} . אולם, $p \mid (x^2 + y^2) = z\bar{z}$, ולכן איננו ראשוני.