

תרגיל 6

1. 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- $a|b$. הוכיחו $\mu(a) \leq \mu(b)$ ושיש שיויון 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:

- c 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 $\mu(b) = \mu(a)$.

- c 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 $a \sim b$.

2. 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. נשים לב שאלו לא גורמים אי פריקים! למשל $2 = (3 + \sqrt{7})(3 - \sqrt{7})$.

פתרון. 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 $(a + b\sqrt{7})(a - b\sqrt{7}) = 2$.

3. בתרגיל זה נמצא את כל האיברים האי-פריקים של $\mathbb{Z}[i]$.

(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- $p | \pi$.

(ג) הוכיחו שאם $\alpha \in \mathbb{Z}[i]$ מקיים $N(\alpha)$ מספר ראשוני, אז 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 האי-פריקים ב- $\mathbb{Z}[i]$ עד כדי חברות (אל תשכחו לפרק את האיבר 2!)

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 $N(x) = 1$).

i. 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 $p = N(x) = a^2 + b^2 = N(y) = p$. נכתוב $x = a + bi$, ונקבל $x = a + bi$, $x = a + bi$ ונקבל 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.

ii. 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- $N(\pi) = \pi \bar{\pi}$, כלומר $N(\pi) = p_1 \cdots p_k$. לכן קיים ראשוני p_i ברשימה שעבורו $\pi \mid p_i$.

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

iv. לפי הטענה שהוזכרה, קיים $a \in \mathbb{Z}$ שעבורו $a^2 \equiv -1 \pmod{p}$. לכן $a^2 + 1 \equiv 0 \pmod{p}$, כלומר $(a+i)(a-i) \equiv 0 \pmod{p}$.

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 $p \mid (a+i+a-i) = 2i$. אבל $p \neq 2$ ראשוני ולכן $p \mid i$, 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.

v. 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- $\mathbb{Z}[i]$.

4. יהיו $x, y \in \mathcal{O}_D$ איברים בחוג שלמים ריבועיים. הוכחנו בכיתה שאם $x \sim y$ אז $N(x) = \pm N(y)$.

(א) מצאו D ואיברים x, y המקיימים $N(x) = N(y)$, אבל הם לא חברים ולא צמודים זה לזה.

נקח $D = -3$. אז ל-2 ול- $\sqrt{-3}$ יש נורמה 4. קל לראות שהם אינם צמודים זה לזה. כדי להוכיח שהם לא חברים נבדוק מי האיברים ההפיכים בחוג. כזכור, איבר הפך אמ"ם הנורמה שלו היא ± 1 . אבל

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

יכול להיות שווה ל1 רק עבור $x = \pm 1, y = 0$, ואף פעם לא שווה ל-1. כלומר, האיברים ההפיכים היחידים הם ± 1 . וניתן לראות ש $2 \cdot (\pm 1) \neq 1 + \sqrt{-3}$.

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!