

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 $\mu(a) = 0$.

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

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 p 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- $\pi | p$.

(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 האי-פריקים ב- $\mathbb{Z}[i]$ עד כדי חברות (אל תשכחו לפרק את האיבר 2!).

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.