תרגיל 8

שאלה 1. הסבירו מדוע המשוואה $6 = 2 \cdot 3 = \left(1+\sqrt{7}\right)\left(-1+\sqrt{7}\right)$ לא סותרת את העובדה ש-$\mathcal{O}_7 = \mathbb{Z}[\sqrt{7}]$ 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.

שאלה 2. הוכיחו ש $\mathcal{O}_{-6}$ אינו תחום פריקות יחידה.

פתרון. $2 \cdot 3 = \sqrt{-6}\sqrt{-6}$.
הנורמה של איבר כללי היא x^2+6y^2. הנורמה לא יכולה להיות שווה אף פעם ל± 2 או ± 3. ולכן $3, 2, \sqrt{-6}$ אינם פריקים.

שאלה 3. יהי F שדה. הוכיחו שחוג המנה $F[x,y,z]/\left\langle xy-z^2\right\rangle$ אינו תחום פריקות יחידה.

פתרון. בחוג המנה נסתכל על האיבר $z^2+\langle xy-z^2\rangle$ שמקיים: $z^2+\langle xy-z^2\rangle = (z+\langle xy-z^2\rangle)\cdot(z+\langle xy-z^2\rangle)$ וגם $z^2+\langle xy-z^2\rangle = (x+\langle xy-z^2\rangle)(y+\langle xy-z^2\rangle)$. קל לראות שכל הרכיבים המשתתפים בפירוקים אינם פריקים ואינם חברים.

שאלה 4. האם $7 \in \mathbb{Z}[i]$ הוא ראשוני?
האם $5 \in \mathbb{Z}[i]$ הוא ראשוני?

פתרון. נסתכל על חוג המנה $\mathbb{Z}[i]/\langle 7\rangle$. הוא איזומורפי לחוג מהצורה הבאה: האיברים בו הם $x+yi$ כאשר $x,y \in \mathbb{Z}_7$, והפעולות הולכות כך: $(x+yi)+(z+wi) = (x+z) \mod 7 + i(y+w)$ mod 7. והכפל: $(x+yi)(z+wi) = (xz-yw) \mod 7 + i(xw+yz)$ mod 7. למעשה אפשר לקרוא לחוג הזה $\mathbb{Z}_7[i]$. אפשר להגדיר עליו נורמה: מספר כפול הצמוד שלו. וקל לראות שהיא כפלית. לכן בשביל להוכיח שזה תחום שלמות, מספיק להראות שאין איבר מנורמה 0 בחוג, חוץ מ0. ובכן, נניח ש$N(x+iy) = x^2+y^2 = 0$. אם $x=0 \vee y=0$, אז גם השני צריך להיות 0. (זכרו שמדובר על מספרים בין 0 ל6, שהפעולות הן מודולו 7). אחרת, ניתן לחלק בy^2, כי $\mathbb{Z}_7$ הוא שדה, ולכן כל איבר בו הפיך. נקבל: $(\frac{x}{y})^2 = -1$. כלומר, $(\frac{x}{y})^2 \equiv 6 \mod 7$. אבל 6 הוא לא מספר ריבועי ב$\mathbb{Z}_7$.
לגבי 5, ניתן לראות ש $5 = (2-i)(2+i)$, ושמשיקולי נורמה $(2-i), (2+i)$ אי פריקים, ולכן 5פריק, ובפרט לא ראשוני.

שאלה 5. 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 $a,b \in R \setminus \{0\}$ לא הפיכים, כך ש-$a|b$. הוכיחו $\mu(a) \leq \mu(b)$ ושיש שיוויון אם ורק אם $a \sim b$.

פתרון. נכתוב: $b = ac$. נפרק את a וc לגורמים אי פריקים.

מקרה ראשון: c לא הפיך, ולכן יש לו פירוק לגורמים אי פריקים.

$a = p_1 \cdot ... \cdot p_n$. $c = q_1 \cdot ...q_m$. לכן $b = p_1 \cdot ... \cdot p_n \cdot q_1 \cdot ... \cdot q_m$. זהו פירוק של b לגורמים אי פריקים. וניתן לראות ש$\mu(a) < \mu(b)$.

מקרה שני: c הפיך. אז לc אין פירוק לגורמים אי פריקים. $b = ac = p_1 \cdot ... \cdot p_n \cdot c =$ $(p_n c)$ $p_1 \cdot ... \cdot$ זהו פירוק של b לגורמים אי פריקים, מכיוון ש$(p_n c)$ אי פריק, כחבר של אי פריק. וניתן לראות ש$\mu(a) = \mu(b)$.

כמו כן, $a \sim b$ אמ"ם c הפיך.