תרגיל כיתה 7

$$N\left(a+b\sqrt{10}\right)=a^2-10b^2$$

$$\left(a+b\sqrt{10}\right)\left(a-b\sqrt{10}\right)$$

נסמן: $\boxed{k=a^2-10b^2}$

$$a^2=k \pmod{10}$$

הערכים שיכולים להתקבל ב$\pmod{10}$ הם $\{0,1,4,5,6,9\}$.

$$k\neq 3 \pmod{10}$$

$$N(3)=9$$

לא קיימים איברים ב$\mathbb{Z}\left[\sqrt{10}\right]$ שהנורמה שלהם היא $\pm 2 \vee \pm 3$
נניח ש

$$\left(a_1+b_1\sqrt{10}\right)\left(a_2+b_2\sqrt{10}\right)=3$$

ז"א

$$N\left(a_1+b_1\sqrt{10}\right)\cdot N\left(a_2+b_2\sqrt{10}\right)=9$$

נניח ש

$$a_1+b_1\sqrt{10}, a_2+b_2\sqrt{10}$$

איברים לא הפיכים. אזי

$$N\left(a_1+b_1\sqrt{10}\right)\neq\pm 1 \qquad N\left(a_2+b_2\sqrt{10}\right)\neq\pm 1$$

$$a+bi+\langle 1+i\rangle=a+bi-\underbrace{b(1+i)}_{\in\langle 1+i\rangle}+\langle 1+i\rangle=a-b+\langle 1+i\rangle$$

$$\overline{a+bi}=\overline{a-b}$$

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

כל אידיאל $I \lhd \mathbb{Z}\left[\sqrt{D}\right]$ **מכיל מספר טבעי ולכן** $\mathbb{Z}[\sqrt{D}]/I$ **סופי**

$$\mathbb{Z}[\sqrt{D}]/I = \left\{a+b\sqrt{D}+I\right\} = \left\{a+b\sqrt{D}+I \,\middle|\, \begin{array}{c} 0<a,b<N \\ N=a^2-Db^2=N\left(a+b\sqrt{D}\right) \end{array}\right\}$$

x^2+2 **הוא איבר ראשוני ב**$\mathbb{Z}[x]$

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}\left[\sqrt{-2}\right]$$

$$\varphi\left(f(x)\right) = f\left(\sqrt{-2}\right)$$

$$\ker\varphi = h\left(x^2+2\right) = \left\langle x^2+2\right\rangle$$

תרגיל כיתה 8

הגדרה

תחום שלמות R נקרא "אטומי" או "תחום פריקות" אם כל איבר $a \in R$ מתפרק למכפלה $u \cdot p_1 \cdots p_n$ כאשר $u \in U(R)$(משמע הפיך) ו$p_1, \ldots p_n$ אי פריקים.

דוגמאות

$\mathbb{Z}$, $\mathbb{Z}[x]$, ו$\mathbb{F}[x]$ כאשר $\mathbb{F}$ שדה.

הגדרה

תחום אטומי R נקרא "תחום פריקות יחידה" אם לכל שני פירוקים של אותו איבר $u \cdot p_1 \cdots p_n$ ו$v \cdot q_1 \cdots q_m$ מתקיים $m=n$ וגם יש תמורה $\sigma \in S_n$ כך ש$q_{\sigma(k)} \sim p_k$.

דוגמה

- $\mathbb{Z}$

$$-42$$

$$2\cdot(-3)\cdot 7 \qquad 7\cdot(-2)\cdot 3$$

נחליף את הסדר בשמאלי:

$$7 \cdot 2 \cdot (-3) \qquad 7 \cdot (-2) \cdot 3$$

ואז

$$7 \sim 7 \qquad 2 \sim -2 \qquad -3 \sim 3$$

- $\mathbb{Z}\left[\sqrt{10}\right]$ איננו תחום פריקות יחידה.

$$6 = 2 \cdot 3 = \left(4 - \sqrt{10}\right)\left(4 + \sqrt{10}\right)$$

אבל

$$2, 3 \not\sim 4 - \sqrt{10}, 3 + \sqrt{10}$$

משפט

כל תחום ראשי הוא תחום פריקות יחידה

מסקנה

$\mathbb{Z}\left[\sqrt{10}\right]$ איננו תחום ראשי.

משפט

בתחום ראשי R, a אי פריק $\Leftrightarrow$ $\langle a \rangle$ מקסימלי

הוכחה

$\Leftarrow$ אם $\langle a \rangle \subset I \subset R$ אז מכיוון שR ראשי קיים $b \in R$ כך ש$\langle b \rangle = I$, ולכן קיים $c \in R \backslash U(R)$ כך ש$a = bc$.

$$\langle a \rangle \subsetneq \langle b \rangle \subset R$$

אנחנו יודעים שאם $a \sim b$ אז $\langle a \rangle = \langle b \rangle$. מכיוון ש$\langle a \rangle \subset \langle b \rangle$ אז $b|a$ וגם $a \nmid b$, ולכן קיים c לא הפיך כך ש$b = ac$.

$\Rightarrow$ נתון ש$\langle a \rangle$ מקסימלי. צריך להוכיח שa אי פריק. נניח בשלילה שa פריק, ז"א קיימים b, c לא הפיכים כך ש$a = b \cdot c$

$$\langle a \rangle \subset \langle b \rangle$$

כי אם $x \in \langle a \rangle$ אז

$$x = a \cdot y = b \cdot c \cdot y \in \langle b \rangle$$

בסתירה למקסימליות.

תרגיל

הראה כי בתחום ראשי, $p \in R$ אי פריק $\Leftrightarrow$ הוא ראשוני.

פתרון

ראינו כי ראשוני $\Leftarrow$ אי פריק. צריך להראות את הכיוון השני.
אם p אי פריק אז $\langle p \rangle$ מקסימלי ולכן $\langle p \rangle$ ראשוני. ז"א p ראשוני.

הגדרה

יהי R תחום שלמות. פונקציה $d : R \to \mathbb{N} \cup \{-\infty\}$ המקיימת

$$d(x) \Leftrightarrow x = 0$$

נקראת אוקלידית אם

1. $d(a) \leq d(a \cdot b)$ לכל $a, b \in R$
2. לכל $b \neq 0$ ולכן a, קיימים $q, r \in R$ כך ש$a = qb + r$ וגם $d(r) < d(b)$

אם קיימת פונקציה כזו עבור R אז הוא נקרא תחום אוקלידי.