

אלגברה מופשטת 2 – תרגול 9

הגדרה

$0 \neq p \in R$ יקרא ראשוני אם p לא הפיך ואם $p \mid ab$ אז $p \mid a$ או $p \mid b$.

תרגיל

כל איבר ראשוני הוא אי פריק.

פתרון

נניח בשלילה ש $0 \neq p \in R$ ראשוני פריק אז $p = ab$ כך ש a, b לא הפיכים, ולכן $p \mid ab$ נניח ב.ה.ג.כ ש $p \mid a$ ז"א קיים $0 \neq c \in R$ כך ש $a = pc$ ולכן $p = ab = pcb$ $\Rightarrow p(1 - cb) = 0 \Rightarrow p = ab = pcb$ הפיך. סתירה.

הערה

p איבר ראשוני $\Leftrightarrow R_p$ אידיאל ראשוני $\Leftrightarrow R/R_p$ תחום שלמות.

יש איברים פריקים שאינם ראשוניים.

דוגמא

למשל $3 \in \mathbb{Z}[\sqrt{10}]$ הוא איבר אי פריק (ראינו זאת) שאינו ראשוני.

נשים לב ש $6 = (4 + \sqrt{10})(4 - \sqrt{10})$ אבל $3 \nmid 6$ לא מחלק את $4 \pm \sqrt{10}$. נראה

למשל ש 3 לא מחלק את $4 + \sqrt{10}$, אילו $4 + \sqrt{10} = 3\alpha, \alpha \in \mathbb{Z}[\sqrt{10}]$ אז

$6 = N(4 + \sqrt{10}) = N(3)N(\alpha) = 9N(\alpha)$ סה"כ נקבל ש $N(\alpha) = \frac{6}{9} \notin \mathbb{Z}$ סתירה.

הערה

2 הוא ראשוני ב \mathbb{Z} אך אינו ראשוני ב $\mathbb{Z}[i]$ מכיוון ש 2 פריק ב $\mathbb{Z}[i]$ כי $2 = (1+i)(1-i)$, אז הוא אינו ראשוני. לעומת זאת $1+i$ הוא איבר ראשוני ב $\mathbb{Z}[i]$.

ההוכחה ש $1+i$ הוא איבר ראשוני ב $\mathbb{Z}[i]$: נוכיח ש $\mathbb{Z}[i]/\langle 1+i \rangle$ הוא תחום שלמות,

ולכן $1+i$ הוא איבר ראשוני. נסמן $\bar{x} = x + \langle 1+i \rangle \in \mathbb{Z}[i]/\langle 1+i \rangle$ אז

שווה $\mathbb{Z}[i]/\langle 1+i \rangle$ שווה $a+bi - (a-b) = b+bi \in \langle 1+i \rangle$ ולכן $\overline{a+bi} = \overline{a-b}$ ז"א כל מחלקה ב $\mathbb{Z}[i]/\langle 1+i \rangle$

למחלקה שנציגה הוא מספר שלם. בנוסף $N(1+i) = 2 = (1+i)(1-i) \in \langle 1+i \rangle$ ולכן

$$\mathbb{Z}[i]/\langle 1+i \rangle = \{a+bi + \langle 1+i \rangle : a, b \in \mathbb{Z}\} = \{a-b + \langle 1+i \rangle : a, b \in \mathbb{Z}\} = \{\overline{(a-b)} \pmod{2} : a, b \in \mathbb{Z}\} = \{\bar{0}, \bar{1}\} \cong \mathbb{Z}_2$$

תרגיל

כל אידיאל $I \triangleleft \mathbb{Z}[\sqrt{D}]$ מכיל מספר טבעי ולכן $\mathbb{Z}[\sqrt{D}]/I$ סופי.

פתרון

יהי $a+b\sqrt{D} \in I$. אז מצד אחד $(a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Z}$ ומצד שני

$$(a+b\sqrt{D})(a-b\sqrt{D}) \in I \quad \text{נסמן } N = a^2 - Db^2 \in I \text{ אז}$$

$$\mathbb{Z}[\sqrt{D}]/I = \{a+b\sqrt{D} + I : a, b \in \mathbb{Z}\} = \{a+b\sqrt{D} + I : 0 \leq a, b \leq N\}$$

אידיאל ראשוני ב $\mathbb{Z}[\sqrt{D}]$ אז $\mathbb{Z}[\sqrt{D}]/I$ הוא תחום שלמות סופי ולכן שדה ז"א I

אידיאל מקסימאלי.

תרגיל בית

הוכיחו, באותה דרך כמו בהערה הקודמת ש $\mathbb{Z}_{10} \cong \mathbb{Z}[i] / \langle 3+i \rangle$ ולכן $3+i$ אינו ראשוני ב $\mathbb{Z}[i]$.

תרגיל

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

פתרון

מוכיחים את האיזומורפיזם בצורה הבאה: $\mathbb{Z}[x] / \langle x^2 + 2 \rangle \cong \mathbb{Z}[\sqrt{-2}]$.

נגדיר הומו' $\varphi: \mathbb{Z}[x] \rightarrow \mathbb{Z}[\sqrt{-2}]$ ע"י הצבת $\sqrt{-2}$:

$$\varphi: f(x) \mapsto f(\sqrt{-2})$$

אח"כ מראים שהגרעין הוא בדיוק $\langle x^2 + 2 \rangle$ ומסיימים עם איזו' 1.

זהו תחום שלמות (בגלל שהנורמה שווה לאפס רק עבור איבר האפס), ולכן האידיאל $\langle x^2 + 2 \rangle$ הוא ראשוני ז"א $x^2 + 2$ ראשוני.

הגדרה

R הוא בעל פריקות (או אטומי) אם לכל $0 \neq a \in R$ קיימים $p_1, \dots, p_r \in R, u \in U(R)$ אי פריקים כך ש $a = u \cdot p_1 \cdot p_2 \cdot \dots \cdot p_r$.

דוגמאות

1. \mathbb{Z} . 2. כל שדה הוא אטומי. 3. אם F שדה אז $F[x]$ אטומי. 4. $\mathbb{Z}[x]$.

דוגמא: לתחום שלמות שהוא לא אטומי.

$$R = \left\{ \sum_{final} \alpha_i x^{b_i} : \alpha_i \in \mathbb{Z}, 0 \leq b_i \in \mathbb{Q} \right\}$$

הוכחה

R קומוטטיבי ותחום שלמות – מידי. לכל $0 < r \in \mathbb{Q}$, פריק x^r ב R : $x^r \notin U(R)$ כי

$$\text{ההופכי שלו הוא } x^{-r} \notin R \text{ ו- } x^r = x^{\frac{r}{2}} \cdot x^{\frac{r}{2}} \text{ ו- } x^{\frac{r}{2}} \notin U(R)$$

אם $\alpha \in R$ מחלק אמיתי של x אז α חייב להיות מהצורה $\pm x^r$ כש $0 < r < 1, r \in \mathbb{Q}$.

ניתן להוכיח את העובדה האחרונה בכמה דרכים:

סקירת פתרון אפשרי: נניח ש $x = \alpha\beta$ פירוק אמיתי, כך ש α או β אינם מהצורה

$\pm x^r$. אזי ניתן להוציא את חזקת x^r החיובית המקסימלית (בהכרח $r < 1$) מ $\alpha\beta$

ולקבל $x = x^r \gamma$, כאשר ל γ בהכרח יש מקדם חפשי. נקבל $x^{1-r} = \gamma$ אבל לפונקציה

משמאל מתאפסת כאשר מציבים 0, והפונקציה מימין לא, סתירה.

לכן אין ל x מחלק אי פריק, כל מחלק של x יהיה פריק, לכן R לא אטומי.

הגדרה

R הוא תחום פריקות יחידה אם R אטומי לכל שני פירוקים של אותו איבר:

$$a = vq_1 \cdot \dots \cdot q_s = up_1 \cdot \dots \cdot p_r \text{ מתקיים } r = s \text{ וקיימת תמורה } \sigma \text{ של } \{1, \dots, r\} \text{ כך ש } p_i \sim q_{\sigma(i)}$$

דוגמא

$\mathbb{Z}[\sqrt{10}]$ אינו תחום פריקות יחידה: $6 = 2 \cdot 3 = (4 + \sqrt{10}) \cdot (4 - \sqrt{10})$. ראינו כבר ש

$2, 3, 4 \pm \sqrt{10}$ אי פריקים. נשאר להוכיח שכל הגורמים בפירוקים השונים אינם

חברים. זה מתקבל ישירות בגלל הנורמות.