

אלגברה מופשטת 2 – תרגיל כיתה 7

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

יהי R מעתה תחום שלמות ויהיו $a, b \in R$. נאמר ש $a|b$ אם יש $k \in R$ כך ש $ak = b$.
למשל $2|4$ ב \mathbb{Z} אבל לא מתקיים $2|3$ ב \mathbb{Z} , אך $2|3$ ב \mathbb{Q} .

הערה

1. $ak = b \iff Ra \subseteq Rb$ כי $ak = b$.

2. יהיו $a, b \in R \setminus \{0\}$. אם $a|b$ ו $b|a$ אז קיים $u \in U(R)$ כך ש $a = bu$.

הסבר: נתון ש $a = bc$ ו $a = bu$ אז $b(1 - cd) = 0 \iff b = bcd \iff b = ad$ ו $a = bc$.
 $b \neq 0$ נקבל ש $cd = 1$. ניקח $u = c$ הפיך ונקבל ש $a = bu$.

הגדרה

נאמר ש $a, b \in R$ חברים אם $a|b$ ו $b|a$. נסמן $a \sim b$. אז \sim יחס שקילות.

הערה

$Ra = Rb \iff a \sim b$. $a \leftrightarrow a \sim 1$ הפיך.

תרגיל

מה הם ההפיכים ב \mathbb{Z} , $\mathbb{Z}[i]$, $F[x]$?

פתרון

ב \mathbb{Z} ± 1 .

ב $F[x]$ ידוע ש $U(F[x]) = U(F) = F^*$.

ב $\mathbb{Z}[i]$. נגדיר לכל $a + bi \in \mathbb{Z}[i]$ את הנורמה $n: \mathbb{Z}[i] \rightarrow \mathbb{N} \cup \{0\}$ ע"י

$n(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. נקבל צמצום הנורמה של \mathbb{C} על $\mathbb{Z}[i]$, ולכן הנורמה

היא כפליית ז"א לכל $\alpha, \beta \in \mathbb{Z}[i]$ $n(\alpha \cdot \beta) = n(\alpha) \cdot n(\beta)$.

יהיו $x, y \in \mathbb{Z}[i]$ כך ש $x \cdot y = 1$ אז $n(x \cdot y) = n(1) = 1$ ולכן (מכיוון שהנורמה

ב $\mathbb{Z}[i]$ היא מספר שלם חיובי) $n(x) = 1$. נרשום $x = a + bi$ ואז $n(x) = a^2 + b^2 = 1$. מכיוון ש

$a, b \in \mathbb{Z}$ הפתרונות היחידים למשוואה זו הם: $(b=0, a=\pm 1) \vee (a=0, b=\pm 1)$ ולכן

הם האיברים ההפיכים בחוג זה. $x = \pm 1, \pm i$

הגדרה

יהי $D \in \mathbb{Z}$ חופשי מריבועים. עבור השדה $\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$ נגדיר את:

$$O_D = \begin{cases} \mathbb{Z}[\sqrt{D}] & D \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & D \equiv 1 \pmod{4} \end{cases}$$

תרגיל

עבור $D = -3$ מהם ההפיכים ב $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

פתרון

נסמן $w = \frac{1+\sqrt{-3}}{2}$. יהי $\alpha = a + bw \in \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ נגדיר $n: \mathbb{Z}[w] \rightarrow \mathbb{N} \cup \{0\}$ ע"י

$$n(\alpha) = \alpha \cdot \bar{\alpha} \text{ ונקבל}$$

$$n(\alpha) = \left(\left(a + \frac{1}{2}b \right) + \frac{\sqrt{3}}{2}bi \right) \left(\left(a + \frac{1}{2}b \right) - \frac{\sqrt{3}}{2}bi \right) = \left(a + \frac{1}{2}b \right)^2 + \frac{3}{4}b^2 = a^2 + ab + b^2$$

באותו אופן, כמו התרגיל הקודם נקבל ש α הפיך $\Leftrightarrow a^2 + ab + b^2 = 1$ הפתרונות היחידים

הם: $(a = \pm 1, b = 0) \vee (a = 0, b = \pm 1) \vee (a = \pm 1, b = \pm 1)$ ז"א $\alpha = \pm w, \pm 1, \pm 1 \pm w$.

אם $2 \leq |a|, |b|$ אז $8 \leq a^2 + b^2 + ab \leq 4$ ולכן אין יותר מספרים הפיכים.

הערה

כאשר המכפלה מחושבת בשדה השברים של R שקיים מכיוון ש R תחום $b \cdot a^{-1} \in R \Leftrightarrow a|b$

שלמות. שימו לב: אם R לא תחום שלמות אז שדה השברים לא קיים ולא ניתן לכתוב a^{-1} .

דוגמאות

1. ב \mathbb{Z} $2|4$ מכיוון ש $4 \cdot 2^{-1} \in \mathbb{Z}$ למרות ש $2^{-1} \notin \mathbb{Z}$.

2. בחוג $\mathbb{Z}[\sqrt{5}]$ $7+\sqrt{5}$, $2+\sqrt{5}$ מכיוון ש

$$(7+\sqrt{5}) \cdot (2+\sqrt{5})^{-1} = (7+\sqrt{5}) \cdot (-2+\sqrt{5}) = -9+5\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$$

הגדרה

$0 \neq a \in R$ נקרא אי פריק אם a אינו הפיך ולכל $b, c \in R$ כך ש $a = bc$ אז $b \vee c$ הפיכים.

$0 \neq a \in R$ נקרא פריק אם a אינו הפיך וקיימים $b, c \in R$ לא הפיכים כך ש $a = bc$.

דוגמאות

1. $x \in F[x]$ הוא אי פריק ולא קיימים $f(x), g(x) \in F[x]$ לא הפיכים כך ש

$$x = f(x) \cdot g(x)$$

2. $x^2 + 1$ הוא אי פריק ב $\mathbb{R}[x]$ אבל פריק ב $\mathbb{C}[x]$ כי $(x+i)(x-i) = x^2 + 1$.

3. ב \mathbb{Z} כל מספר ראשוני הוא אי פריק.

4. ב $\mathbb{Z}[i]$ המספר 2 הוא פריק מכיוון ש $(1+i) \cdot (1-i) = 2$ וראינו ש $1+i, 1-i$ אינם הפיכים

ב $\mathbb{Z}[i]$.

5. בשדה או בחוג עם חילוק אין משמעות לפריקות/אי פריקות של איבר מכיוון שכל איבר

שונה מאפס הוא הפיך.

תרגיל

יהי $p \in R$ אי פריק ונניח ש $p \sim q$. אז אי פריק.

פתרון

נתון ש $p \sim q$ הראינו בתחילת התרגול שקיים הפיך u כך ש $q = up$. נניח ש $q = bc$ יש

להראות ש $b \vee c$ הפיכים. $p = u^{-1}q = u^{-1}(bc) = (u^{-1}b)c$ מכיוון ש p אי פריק אז או ש $u^{-1}b$

הפיך או ש c הפיך. אם c הפיך סיימנו, אם c אינו הפיך אז b הפיך ואז $u^{-1}b$ הפיך כמכפלה

של איברים הפיכים.

הגדרה

יהי $D \in \mathbb{Z}$ חופשי מריבועים. נגדיר $N: O_D \rightarrow \mathbb{Z}$ ע"י $N(\alpha) = \alpha \cdot \bar{\alpha}$ כאשר אם

$$\alpha = a + b\sqrt{D} \text{ אז } \alpha = a - b\sqrt{D} \text{ אז } N(xy) = N(x)N(y) \text{ ו } N(x) = 0 \leftrightarrow x = 0$$

תרגיל

$$. N(x) = \pm 1 \leftrightarrow x \in O_D \text{ הפיך}$$

פתרון

x הפיך ולכן קיים y כך ש $xy=1$ ולכן $N(x)N(y) = N(xy) = N(1) = 1$ ולכן (בגלל ש $N(x) = \pm 1$ ($N(x) \in \mathbb{Z}$)).

אם $N(x) = \pm 1$ אז $x \cdot \bar{x} = \pm 1$ ז"א $x^{-1} = \pm \bar{x}$ ולכן x הפיך.

תרגיל

אם $N(x)$ אי פריק (ז"א ראשוני כי $N(x) \in \mathbb{Z}$), אז x אי פריק.

פתרון

אם $x = y \cdot z$ אז $N(x) = N(y \cdot z) = N(y)N(z)$ מכיוון ש $N(x)$ מספר ראשוני נקבל ב.ה.ג.כ ש $N(y) = \pm 1$ ז"א y הפיך ולכן x אי פריק.

הערה

נראה בדוגמא הבאה מקרה ש x אי פריק ו $N(x)$ אינו ראשוני.

דוגמא

נוכיח ש $2, 3, 4 \pm \sqrt{10} \in O_{10} = \mathbb{Z}[\sqrt{10}]$ אי פריקים.

למשל: אם $4 + \sqrt{10} = x \cdot y$ לא הפיכים אז $6 = N(4 + \sqrt{10}) = N(x)N(y)$ מכיוון ש x אי פריק נקבל ש $N(x) \neq \pm 1$ כי אז x הייה הפיך, ז"א $N(x) = \pm 2, \pm 3$.

יהי $a + b\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ אז $N(a + b\sqrt{10}) = a^2 - 10b^2 = k$ נראה אילו ערכים k נעבור למודולו 10: $a^2 = k \pmod{10}$.

נשים לב שבמודולו 10, k יכול לקבל את הערכים הבאים: $\{0, 1, 4, 5, 6, 9\}$.

שימו לב: $k \neq \pm 3 \leftarrow k \neq 3, 7 \pmod{10}$
 $k \neq \pm 2 \leftarrow k \neq 2, 8 \pmod{10}$
ולכן לא קיימים איברים ב $\mathbb{Z}[\sqrt{10}]$ שהנורמה שלהם

היא ± 2 ו ± 3 .

באופן דומה $N(4 - \sqrt{10}) = 6$, $N(2) = 4$, $N(3) = 9$. מכיוון שלא קיימים מספרים שהנורמה שלהם שווה ל $\pm 2 \vee \pm 3$ נקבל שגם 2,3 אי פריקים.

תרגיל

הוכיחו ש $1 + \sqrt{-5}$ אינו פריק ב $\mathbb{Z}[\sqrt{-5}]$.

פתרון

נניח ש $s \cdot t = 1 + \sqrt{-5}$ לא הפיכים, אז $N(s) \cdot N(t) = N(s \cdot t) = 6$. אם $N(s) = 1$ אז s הפיך, ולכן מתקיים $(N(s) = 2, N(t) = 3) \vee (N(s) = 3, N(t) = 2)$.

שימו לב ש $\mathbb{N} \subseteq N[\mathbb{Z}[\sqrt{-5}]]$ כי אם $t = a + b\sqrt{-5}$ אז

$$N(a + b\sqrt{-5}) = a^2 - (-5b^2) = a^2 + 5b^2$$

$$a^2 = 2, 3 \pmod{5} \text{ אבל } (\mathbb{Z}_5)^2 = \{0, 1, 4\}$$

תרגיל

הוכיחו ש $\mathbb{Z}[\sqrt{-5}]$ אינו חוג ראשי. ז"א שקיים אידיאל שלא נוצר ע"י איבר אחד.

פתרון

נסתכל על $I = \langle 2, 1 + \sqrt{-5} \rangle$. נראה כי $I \neq \mathbb{Z}[\sqrt{-5}]$:

ניקח איבר כללי $2a + (1 + \sqrt{-5})b \in I$, אזי

$$N(2a + (1 + \sqrt{-5})b) = 4a\bar{a} + 2((1 + \sqrt{-5})b\bar{a} + \overline{(1 + \sqrt{-5})b\bar{a}}) + 6b\bar{b}$$

מתחלקת ב2. לכן $1 \notin I$.

נניח ש $I = \langle m \rangle$, אז קיימים $r_1, r_2 \in \mathbb{Z}[\sqrt{-5}]$ כך ש $r_1 m = 2, r_2 m = 1 + \sqrt{-5}$ ולכן

$$N(r_1)N(m) = 4, N(r_2)N(m) = 6 \text{ ולכן } N(m) \mid 4, 6 \text{ ז"א } N(m) = 2 \vee N(m) = 1 \text{ על פי}$$

התרגיל הקודם $N(m) \neq 2$ ולכן $N(m) = 1$ ז"א m הפיך ז"א $I = \mathbb{Z}[\sqrt{-5}]$ וקיבלנו סתירה.

הגדרה

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

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 $p | ab$ נניח

ב.ה.ג.כ ש $p | a$ ז"א קיים $0 \neq c \in R$ כך ש $a = pc$ ולכן

$$b \leftarrow cb = 1 \leftarrow p(1 - cb) = 0 \leftarrow p = ab = pcb$$

הערה

p איבר ראשוני $\leftrightarrow Rp$ אידיאל ראשוני $\leftrightarrow R/Rp$ 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 $6 = (4 + \sqrt{10})(4 - \sqrt{10})$ ו $3 | 6$ אבל 3 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

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

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

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

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

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

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

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

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

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

אידיאל ראשוני ב $\mathbb{Z}[\sqrt{D}]$ או $\mathbb{Z}[\sqrt{D}]/I$ 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

$$\mathbb{Z}[x]/\langle x^2 + 2 \rangle \cong \mathbb{Z}[\sqrt{-2}]$$

וזהו 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 $u \in U(R)$, $p_1, \dots, p_r \in R$ אי

$$a = u \cdot p_1 \cdot p_2 \cdots p_r \text{ ש פריקים כך}$$

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.

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

הוכחה

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

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

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

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

$2, 3, 4 \pm \sqrt{10}$ אי פריקים. נשאר להוכיח שכל הגורמים בפירוקים השונים אינם חברים. זה מתקבל ישירות בגלל הנורמות.