

אלגברה מופשטת 2 – תרגול 8

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} .
עוד דוגמה מעניינת כזאת, היא החוג $S \subset F[x]$ של כל הפולינומים (עם מקדמים בשדה F) בהם המקדם של x^1 הוא 0, כלומר כל הפולינומים מהצורה $a_n x^n + \dots + a_2 x^2 + a_0$ (ודאו שזה חוג). אזי $x^2 \nmid x^3$ ב S , למרות ש $x^2 | x^3$ ב $F[x]$.

הערה

1. $ak = b \Leftrightarrow Ra \supseteq Rb$ 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 $b = ad$ אז $b = bcd \leftarrow b = bcd = b(1 - cd) = 0$ מכיוון ש R תחום שלמות ו $b \neq 0$ 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

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

תרגיל

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

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

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 $D = -3$ מה הם 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 $\Leftrightarrow a^2 + ab + b^2 = 1$ (הנורמה היא תמיד מספר שלם, והיא גם סכום של שני ריבועים ממשיים, ולכן תמיד חיובית)

אם $|b| \leq 2$ אז $\frac{3}{4}b^2 \geq 3$ ואז $\left(a + \frac{1}{2}b \right)^2 + \frac{3}{4}b^2 > 1$, לכן בהכרח $|b| \leq 1$. בנוסף

$$a^2 + ab + b^2 = \left(b + \frac{1}{2}a \right)^2 + \frac{3}{4}a^2$$

ניתן לעבור על כל

האפשרויות ולקבל שהפתרונות היחידים הם:

הפתרונות היחידים הם: $(a = 0, b = \pm 1) \vee (b = 0, a = \pm 1) \vee (a = \pm 1, b = -a)$ ז"א

$$\alpha = \pm w, \pm 1, \pm(1-w)$$

הערה

$b \cdot a^{-1} \in R \Leftrightarrow a|b$ כאשר המכפלה מחושבת בשדה השברים של R שקיים מכיוון ש R תחום שלמות. שימו לב: אם R לא תחום שלמות אז שדה השברים לא קיים ולא ניתן לכתוב a^{-1} .

דוגמאות

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

2. בחוג $\mathbb{Z}[\sqrt{5}]$ $2 + \sqrt{5} \mid 7 + \sqrt{5}$ 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 q 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 $\alpha = a + b\sqrt{D}$ אז $\bar{\alpha} = a - b\sqrt{D}$. אז $N(xy) = N(x)N(y)$ ו $N(x) = 0 \Leftrightarrow x = 0$.

תרגיל

$N(x) = \pm 1 \Leftrightarrow x \in O_D$ הפיך.

פתרון

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

אם $N(x) = \pm 1$ אז $x \cdot \bar{x} = \pm 1$ ז"א $x^{-1} = \bar{x}$ 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 $\pm 2 \vee \pm 3$.

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

$N(a + b\sqrt{-5}) = a^2 - (-5b^2) = a^2 + 5b^2$ אבל למשוואה $a^2 + 5b^2 = 2, 3$ אין פתרון, מכיוון ש $a^2 = 2, 3 \pmod{5}$ 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 ב 2. 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

$N(r_1)N(m) = 4, N(r_2)N(m) = 6$ ולכן $4, 6 \mid N(m)$ ז"א $N(m) = 2 \vee N(m) = 1$ 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.