

מבוא לתחומים ומודולים - תרגול 7

לב תרגול, R תהי' R

הצורה:

יהיו $a, b \in R$. אם $a \mid b$ ו- $b \mid a$, אומרים ש a ו- b תכרם, ומסמנים $a \sim b$.
הצורה שקולת:

א. $Ra = Rb \Leftrightarrow a \sim b$

ב. $a \sim b \Leftrightarrow$ קיים $\underbrace{u \in R^x}_{u \text{ הסיק}}$ כך ש- $a = ub$

בפרט, $a \sim 1 \Leftrightarrow a$ הסיק.

תרגיל:

מצאו את האיברים החזקים של איבר היחידה ב- \mathbb{Z} , $F[x]$ ו- $\mathbb{Z}[i]$.

פתרון:

האיברים החזקים של איבר היחידה = האיברים ההרטיכים.

ב- \mathbb{Z} אלו ± 1 . ב- $F[x]$ = הפולינומים הקבוצים חוץ מ-0.

ב- $\mathbb{Z}[i]$: אלו אלו שהצד נורמה $N: \mathbb{Z}[i] \rightarrow \mathbb{N} \cup \{0\}$

$$N(a+bi) = a^2 + b^2$$

הוכחתי בתרגיל הקודם שהאיברים ההרטיכים הם האיברים מנוחה 1. (כי אקזיסטנציה $\mathbb{Z}[i]$)

לפי $a+bi \in \{1, -1, i, -i\} \Leftrightarrow a^2 + b^2 = N(a+bi) = 1 \Leftrightarrow a+bi$ הסיק

הצורה:

אם $a \in R, a \neq 0$ הוא אי-פריק אם הוא לא הסיק וגם \exists שיווק שלו $a = bc$

הוא אריוואלי, כלומר מהצורה $a = au \cdot u^{-1}$ כאשר u הסיק.

טענות:

התנאים הבאים שקולים ל-a ראשוני:

א. a אי-פריק.

ב. אם $a=xy$ אז $a \sim x$ או $a \sim y$.

ג. אם $a=xy$ אז x הפיך או y הפיך (ראו לעיל).

ד. אם $a=xy$ אז $a \sim x$ או x הפיך.

ה. אם $a|x$ אז $a \sim x$ או x הפיך.

דוגמאות:

א. $x \in F[x]$ אי-פריק: כי אם $x = f(x)g(x)$ אז נקבל ש-f או

g קבועים ושלמים מ-0, ולכן הפיכים.

ב. x^2+1 אי-פריק ב- $\mathbb{Z}[x]$ אבל פריק ב- $\mathbb{C}[x]$.

ג. \mathbb{Z} מספר ראשוני ב- \mathbb{Z} הוא אי-פריק ב- \mathbb{Z} , אבל 2 פריק ב- $\mathbb{Z}[i]$

כי $2 = (1+i)(1-i)$.

תרגיל:

יהי $p \in \mathbb{R}$ אי-פריק, ויהי $q \sim p$. אז q אי-פריק.

פתרון:

$q \sim p \Leftrightarrow \exists u \in R^x$ הפיך כן ש- $q = up$. נניח $q = bc$ עבור $b, c \in R$.

אם $c = (b^{-1}p)$ אז p אי-פריק, אכן $b^{-1}u$ הפיך או c הפיך.

אם c הפיך - סימני, אחרת $b^{-1}u$ הפיך, גם u הפיך $\Leftrightarrow b$ הפיך. \square

הערה:

אם $p \in R$ (ראשוני) אז p ראשוני ו- $pl \leq plab \Leftrightarrow pl \leq plab$.

טענה:

אם ראשוני (הוא אי-פריק).

\cdot $R/R_p \Leftrightarrow$ תחום ראשוני $\langle p \rangle = R_p \Leftrightarrow p \in R$

תוצאה:

הוכיחו כי $1+i$ ראשוני ב- $\mathbb{Z}[i]$.

הוכחה:

ניבנו איבר $x \in \mathbb{Z}[i]$ כך ש- $\mathbb{Z}[i]/\langle 1+i \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

$$\bar{x} = x + \langle 1+i \rangle$$

$$\overline{1+i} = \overline{1+i} = \bar{0} \Rightarrow \bar{i} = -\bar{1}$$

$$N(1+i) = (1+i)(1-i) = 2 \in \langle 1+i \rangle$$

וכן, $\mathbb{Z}[i]/\langle 1+i \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

$$\mathbb{Z}[i]/\langle 1+i \rangle = \{ \overline{a+bi} \mid a, b \in \mathbb{Z} \} = \{ \overline{a-b} \mid a, b \in \mathbb{Z} \} =$$

$$= \{ \overline{a-b \pmod{2}} \mid a, b \in \mathbb{Z} \} = \{ \bar{0}, \bar{1} \}$$

\uparrow
 $2 \in \langle 1+i \rangle$ כי $\bar{2} = \bar{0}$

\square \cdot $\mathbb{Z}[i]$ - בראשוני $1+i$ תחום ראשוני $\mathbb{Z}[i]/\langle 1+i \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

דוגמה:

ניתן דוגמה מאיזה אי-פריק שאינו ראשוני. ניקח ב- $\mathbb{Z}[\sqrt{10}]$ את האיבר 3. נראה כי 3 אי-פריק אבל לא ראשוני.

פתרון ראשוני

$$3 \mid 6 = (4 + \sqrt{10})(4 - \sqrt{10})$$

נראה ש-3 לא מתחלק את אחד מהם. לכן 3 אי-פריק.

$$\cdot 3 \mid 4 + \sqrt{10}$$

(כי $4 - \sqrt{10}$ זוגי)

$$N(3\alpha) = N(4 + \sqrt{10}) \Leftrightarrow 3 \cdot \alpha = 4 + \sqrt{10}$$

$$N(3)N(\alpha) = N(4 + \sqrt{10})$$

$$9 \cdot N(\alpha) = 6$$

סתירה.

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

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

(זה אוקסידי.)

$$3 = \underbrace{(a+b\sqrt{10})}_x \underbrace{(c+d\sqrt{10})}_y$$

לפי זה $\boxed{10}$ חייב להיות

$$9 = N(3) = N(x) \cdot N(y)$$

היינו $x \in x \cdot \bar{x} = 1 \Leftrightarrow N(x) = \pm 1$ (כל a, b) $N(x) = N(y) = \pm 3$ לפי

$$N(x) = 3 \Rightarrow a^2 - 10b^2 = 3 \pmod{10}$$

$$a^2 \equiv 3 \pmod{10}$$

כל a מתקיים $a^2 \equiv 1, 4, 6, 9 \pmod{10}$

הוכחה:

הוכיחו שיש איבר $\neq 1$ ב- $\mathbb{Z}[\sqrt{D}]$ מסדר גבוה, והסיקו כי $D \in \mathbb{Z}$ כל חיובי

הוכחה:

היי' $a+b\sqrt{D} \in I$ $\neq 0$. נניח $(x+y\sqrt{D}) \in I$ $N(x+y\sqrt{D}) = x^2 - Dy^2$

$$N(a+b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Z}_{\neq 0}$$

כל $a^2 - Db^2 \in I$ הוא מסדר גבוה $\neq 0$. כל $(a^2 - Db^2) \in I$ $\neq 0$ קטן מסדר גבוה. k

$$\mathbb{Z}[\sqrt{D}]/I = \{x+y\sqrt{D} + I \mid x, y \in \mathbb{Z}\} \xrightarrow[k \in I]{} \{x+y\sqrt{D} + I \mid 0 \leq x, y < k\}$$

זוהי סופי.

הוכחה:

ה- $\mathbb{Z}[\sqrt{D}]$ איננו רגולרי $\neq 0$ הוא מקסימלי.

הוכחה:

היי' $P \subset \mathbb{Z}[\sqrt{D}]$ $\neq 0$ רגולרי $\mathbb{Z}[\sqrt{D}]/P \leftarrow$ הוכחה: $\mathbb{Z}[\sqrt{D}]/P \leftarrow$ הוכחה: $\mathbb{Z}[\sqrt{D}]/P \leftarrow$ הוכחה: $\mathbb{Z}[\sqrt{D}]/P \leftarrow$

$P \leftarrow$ מקסימלי.

טענה:

פ תחום שלמח סופי הוא שדה.

הוכחה:

יהי $a \in R, a \neq 0$. נגדיר

$$l_a: R \rightarrow R$$

$$l_a(x) = ax$$

זו פונקציה ההי"ח, כי $x=y \Leftrightarrow x-y=0 \stackrel{\text{מ"ש}}{\Leftrightarrow} a(x-y)=0 \Leftrightarrow ax=ay$

אלה R סופי, לפי l_a ג"כ l_a ג"כ, למחר קיים $b \in R$ כן $ab=1$.

מהחלופיות, $ba=1$ ו- a הסיק.

תרגיל:

הוכיחו כי $x^2+2 \in \mathbb{Z}[x]$ אינו ראשוני.

הוכחה:

נכינו $\mathbb{Z}[x]/\langle x^2+2 \rangle \cong \mathbb{Z}[\sqrt{-2}]$ בעזרת הומומורפיזם ההיבנה $\varphi: \mathbb{Z}[x] \rightarrow \mathbb{Z}[\sqrt{-2}]$
 $f(x) \mapsto f(\sqrt{-2})$

$\ker \varphi = \langle x^2+2 \rangle$, φ איז הומומורפיזם היחיד, $\mathbb{Z}[\sqrt{-2}]$ איז איזומורפיזם הראשוני.

$\mathbb{Z}[\sqrt{-2}]$ תחום $\Leftrightarrow x^2+2$ ראשוני ב- $\mathbb{Z}[x]$.

הצגה:

תחום שלמח R נקרא אטומי אם לכל $a \in R, a \neq 0$ קיים פירוק למכפלה של אי-פריקים (עד כדי איבר הסיק).

דוגמאות:

$\mathbb{Z}, F, F[x], \mathbb{Z}[x]$ - אטומיים.

דוגמאות לפירוק לא יחיד:

$\mathbb{Z}[\sqrt{5}]$ - ראיתם בהורצאה.

יהי F שדה. $R = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in F\}$ של x^2, x^3 אי-פריקים כי המקדם של x הוא 0 הם איברי R .
 $x^2 \cdot x^2 \cdot x^2 = x^3 \cdot x^3$

$$x^2 y^2 = (xy)^2$$

$$R = \mathbb{Q}[x^2, xy, y^2] \not\subseteq \mathbb{Q}[x, y]$$

תרגיל רביעי:

$$R = \left\{ \sum_{i=1}^n a_i x^{b_i} \mid a_i \in \mathbb{Z}, 0 \leq b_i \in \mathbb{Q} \right\}$$

החוג

לא אטומי.

הערה:

חוג אטומי R יקרא תחום פריק יחידה (תפ"י) אם כל שני פריקים של
אחד אחר

$$p_1 \dots p_r = a = q_1 \dots q_s$$

מתקיים $r=s$ וזו קיימת $\sigma \in S_r$ כך של $p_i \sim q_{\sigma(i)}$.

דוגמה:

$$2 \cdot 3 = 6 = (4 + \sqrt{10})(4 - \sqrt{10}) \quad \text{כ} \quad \mathbb{Z}[\sqrt{10}] \text{ לא תפ"י, כ}$$

כל האיברים שהם אי-פריקים, ואף יזו חילוב נייטרלי נייטריאלים
לאן נגז אברים חברים.

משפט:

תחום ראשי \Leftarrow תפ"י.

וכן $\mathbb{Z}[\sqrt{10}]$ לא תחום ראשי.

$I = \langle 2, \sqrt{10} \rangle$ איזוהו לא ראשי. למה? אם $I = \langle \alpha \rangle$,

$$\alpha \mid 2, \sqrt{10} \Rightarrow N(\alpha) \mid N(2)=4, N(\sqrt{10})=-10$$

$$\Rightarrow N(\alpha) = \pm 2$$

$$N(\alpha) = \pm 2 \Leftarrow \alpha \text{ (הסיק)}$$

$$\alpha = a + b\sqrt{10} \Rightarrow a^2 - 10b^2 = 2$$

$$a^2 \equiv 2 \pmod{5}$$

אין פתרונות

(הערה: חלוקה אצל לא פריקים ופ"י:

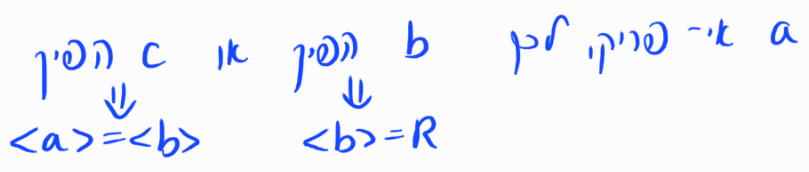
$$\left[a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow a \text{ איש שונה מודולו } p \text{ מודולו } p+2 \right]$$

טענה:

יהי R תחיל. $a \in R$ הוא אי-סופי אם ורק אם $\langle a \rangle < R$ הוא מקסימלי.
מבין \mathcal{B} האידיאלים הראשיים הנאיבטיים של R .

הוכחה:

$\square \Leftarrow$ נ"ל $\langle a \rangle \subseteq \langle b \rangle \Leftrightarrow a \in \langle b \rangle \Leftrightarrow a = bc$ כאשר $c \in R$.



\Rightarrow

נ"ל כי $\langle a \rangle$ מקסימלי בין האידיאלים הראשיים.

אם $a = bc$ עבור b לא הסוף $\Leftrightarrow \langle a \rangle \subseteq \langle b \rangle \Leftrightarrow \langle a \rangle = \langle b \rangle$
 $\Leftarrow b$ חבו של a .

\square

משפט:

בתחום ראשי, אי-סופי \Leftarrow ראשוני.

הוכחה:

יהי p מספר ראשוני אי-זוגי, ויהי $D \in \mathbb{Z}$ כך ש- $D \not\equiv 0 \pmod{p}$. תכינו את

רמטוריה $x^2 \equiv D \pmod{p}$ יש פתרון, אך בחוג $\mathbb{Z}[\sqrt{D}]$ מתקיים $\langle p \rangle = P_1 P_2$ עבור שני אידיאלים P_1, P_2 קו-מקסימליים.

דוגמה:

$p=11, D=5$, קל לראות ש- $4^2 \equiv 5 \pmod{11}$. לפי 11 לא ראשוני ב- $\mathbb{Z}[\sqrt{5}]$,

ואפשר לראות זאת גם יד הסיווק $(4+\sqrt{5})(4-\sqrt{5})=11$

כפי שהרמז נקרא

$\mathbb{Z}[\sqrt{5}] / \langle 11 \rangle = \mathbb{Z}[\sqrt{5}] / P_1 P_2 \stackrel{\text{CRT}}{\cong} \mathbb{Z}[\sqrt{5}] / P_1 \times \mathbb{Z}[\sqrt{5}] / P_2$

