

אלגברה מופשטת 2 – תרגיל כיתה 8

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

הגדרה:

תחום שלמות R נקרא "אטומי" או "תחום פריקות" אם כל איבר $a \in R$ מתפרק למכפלה $up_1 \dots p_n$ כאשר $u \in U(R)$ (משמע הפיך) ו p_1, \dots, p_n אי-פריקים.

דוגמאות:

1. החוגים \mathbb{Z} , $\mathbb{Z}[x]$ ו $F[x]$ (כאשר F שדה) הם אטומיים.

2. החוג $F[x^r : r \in \mathbb{Q}]$ איננו אטומי.

הגדרה:

תחום אטומי R נקרא "תחום פריקות יחידה" אם לכל שני פירוקים של אותו איבר $up_1 \dots p_n$ ו $vq_1 \dots q_m$ מתקיים $m = n$ וגם ישנה תמורה $\sigma \in S_n$ כך ש $q_{\sigma(k)} \sim p_k$.

דוגמאות:

1. \mathbb{Z} הוא תחום פריקות יחידה.

2. $\mathbb{Z}[\sqrt{10}]$ איננו תחום פריקות יחידה משום

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

התנאי הנ"ל.

משפט: כל תחום ראשי הוא תחום פריקות יחידה.

מסקנה: $\mathbb{Z}[\sqrt{10}]$ איננו תחום ראשי.

משפט: בתחום ראשי R , a אי-פריק $\Leftrightarrow \langle a \rangle$ מקסימלי.

הוכחה: (\Leftarrow) אם $\langle a \rangle \subset I \subset R$ אזי מכיוון ש- R ראשי קיים $b \in R$ כך ש- $\langle b \rangle = I$ ולכן קיים $c \in R \setminus U(R)$ כך ש- $a = bc$, משמע a פריק.
 (\Rightarrow) אם $\langle a \rangle$ מקסימלי וגם $a = bc$ כך ש- $b \notin U(R)$ אזי $b \mid a$ ולכן $\langle a \rangle \subseteq \langle b \rangle \subset R$. בגלל המקסימליות של $\langle a \rangle$, $\langle a \rangle = \langle b \rangle$, משמע $a \sim b$, כלמור a אי-פריק.

[שימו לב כי בכוון ההפוך אין צורך להשתמש בהנחה כי התחום R הוא דווקא ראשי]

תרגיל: הראה כי בתחום ראשי, $p \in R$ אי-פריק אם ורק אם הוא ראשוני.
פיתרון: ידוע כבר כי בכל תחום ראשי, ראשוני גורר אי-פריק. נראה כי במקרה זה אי-פריק גורר ראשוני. אם p אי-פריק אזי $\langle p \rangle$ מקסימלי, ולכן $\langle p \rangle$ ראשוני, משמע p ראשוני.

תרגיל: יהי p שלם ראשוני גדול מ-2, $d \in \mathbb{Z}$ כך ש- $p \nmid d$. אם $x^2 \equiv d \pmod{p}$ פתירה אז בחוג $\mathbb{Z}[\sqrt{d}]$ מתקיים $\langle p \rangle = P_1 \cdot P_2$ כך ש- $P_1 \neq P_2$.
פיתרון: נקרא לפיתרון לקונגרואנציה a . איבר כללי הנמצא במכפלת האידיאלים ב- $\mathbb{Z}[\sqrt{d}]$ הוא מהצורה $\langle p, a + \sqrt{d} \rangle \cdot \langle p, a - \sqrt{d} \rangle$
 $c_1 p^2 + c_2 p(a - \sqrt{d}) + c_3 p(a + \sqrt{d}) + c_4 (a - \sqrt{d})(a + \sqrt{d})$ ולכן
 $\langle p, a + \sqrt{d} \rangle \cdot \langle p, a - \sqrt{d} \rangle = \langle p \rangle \cdot \langle p, a + \sqrt{d}, a - \sqrt{d}, \frac{a^2 - d}{p} \rangle$

כעת $2a = (a - \sqrt{d}) + (a + \sqrt{d})$. אם $p \mid a$ אזי $p \mid a^2$ ולכן $p \mid d$ וזו סתירה. לכן

$$, 1 \in \langle p, a + \sqrt{d}, a - \sqrt{d}, \frac{a^2 - d}{p} \rangle \text{ ולכן } \gcd(2a, p) = 1 \text{ משמע } , p \nmid a$$

$$\text{משמע } \langle p, a + \sqrt{d}, a - \sqrt{d}, \frac{a^2 - d}{p} \rangle = \mathbb{Z}[\sqrt{d}] \text{ כלומר}$$

$$. \langle p, a + \sqrt{d} \rangle \cdot \langle p, a - \sqrt{d} \rangle = \langle p \rangle$$

אם הם היו שווים אז $\langle p, a + \sqrt{d} \rangle$ היה מכיל את p ואת $2a$ ולכן מאותם שיקולים

$$\langle p, a + \sqrt{d} \rangle = \mathbb{Z}[\sqrt{d}] \text{ ולכן גם } \langle p \rangle = \mathbb{Z}[\sqrt{d}] \text{ וזו סתירה.}$$

הגדרה: יהי R תחום שלמות. פונקצייה $d : R \rightarrow \mathbb{N} \cup \{-\infty\}$ המקיימת

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

$$. 1 \quad d(a) \leq d(ab) \text{ לכל } a, b \in R$$

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

$$. r = 0$$

אם קיימת פונקצייה כזאת עבור R אזי הוא נקרא "תחום אוקלידי".

דוגמאות:

$$. 1 \quad \mathbb{Z}[i] \text{ הוא תחום אוקלידי, עם הפונקצייה } d(a + bi) = a^2 + b^2$$

$$. 2 \quad \mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right] \text{ איננו תחום אוקלידי [לא ניתן לזה הוכחה בשלב זה].}$$

טענה (לבית): הראה כי אם R חוג קומוטטיבי עם יחידה ו $f, g \in R[x]$ כך ש $g(x)$ פולינום מתוקן, אזי קיימים $r, q \in R[x]$ כך ש $f = gq + r$ וגם $\deg(r) < \deg(g)$ או $r = 0$.

טענה: תחום אוקלידי הוא תחום ראשי.

הוכחה: אם $0 \neq I \triangleleft R$ אזי ניקח $0 \neq b \in I$ כך

ש $d(b) = \min\{d(c) : 0 \neq c \in I\}$. אזי בגלל האוקלידיות, כל איבר אחר ב I חייב להתחלק ב b (כי אחרת יש סתירה למינימליות) ולכן $\langle b \rangle = I$.

תרגיל: אם F שדה אזי $F[[x]]$ אוקלידי עם $d(\sum_{n=0}^{\infty} a_n x^n) = \min\{i : a_i \neq 0\}$.

פיתרון: קל לראות ש $d(fg) = d(f) + d(g) > d(f)$ לכל $f, g \in F[[x]]$.

נניח $g \neq 0$. צריך להוכיח כי קיימים $r, q \in F[[x]]$ שעבורם $f = gq + r$ וגם $d(r) < d(g)$ או $r = 0$. אם מלכתחילה $d(f) < d(g)$ אז ניקח $r = f$ ו $q = 0$.

נניח ש $m = d(f) \geq d(g) = n$. אזי $f = x^m f_0$ ו $g = x^n g_0$ כאשר

$d(f_0) = d(g_0) = 0$ [כלומר יש להם מקדם חופשי שונה מאפס]. לכן הפיך g_0 ניקח $q = x^{m-n} g_0^{-1} f_0$ ו $r = 0$ וסיימנו.

תרגיל: הראה כי בתחום אוקלידי, a הפיך אם ורק אם $d(a) = d(1)$.

הוכחה: אם a הפיך אזי $d(a) \leq d(a \cdot a^{-1}) = d(1)$ וגם $d(a) \leq d(1 \cdot a) = d(a)$,

ולכן $d(a) = d(1)$. אם $d(a) = d(1)$ אז נרשום $1 = qa + r$ במקרה זה $r = 0$ או

$d(r) < d(1)$ אך האופצייה השנייה לא אפשרית, ולכן $1 = qa$, כלומר a הפיך.

תרגיל בית:

ב $\mathbb{Z}[\sqrt{3}]$, $N(-5 + \sqrt{3}) = 25 - 3 = 22$. הוכיחו כי

$$|\mathbb{Z}[\sqrt{3}] / \langle -5 + \sqrt{3} \rangle| = 22.$$