# לינארית 2א ~ חוגים ושאר ירקות

שחר פרץ

23 באפריל 2025

## RINGS ........................................................................................ (1)

**הגדרה 1.** תחום שלמות הוא חוג קומוטטיבי עם יחידה ללא מחלקי 0.

**הגדרה 2.** חוק ייקרא ללא מחלקי 0 אם: $\forall a, b \in \mathbb{R} \colon ab = 0 \implies a = 0 \lor b = 0$

דוגמאות לחוגים עם מחלקי 0:

- $M_2(\mathbb{R})$: הוכחה $a = b = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right),\ a \cdot b = 0$
- $\mathbb{Z}/_{6\mathbb{Z}}$ הוכחה $2 \cdot 3 = 0$.

**משפט 1.** בתחום שלמות יש את כלל הצמצום בכפל: אם $ab = ac \land a \neq 0$ אז $b = c$.

הוכחה.

$$ab \cdot ac = 0 \implies a(b \cdot c) = 0 \implies a = 0 \lor b - c = 0$$

בגלל ש־$a \neq 0$, אז $b - c = 0$. נוסיף את $c$ הנגדי של $-c$ ונקבל $b = c$. ■

דוגמאות לתחום שלמות:

- שדות
- השלמים
- חוג הפולינומים

**משפט 2.** לכל $f, g \in \mathbb{F}[x]$, אם $g \neq 0$ אז קיימים ויחידים פולינומים $q, r \mathbb{F}[x]n$ כך ש־$f = qg + r \land \deg r < \deg g$

**הגדרה 3.** נאמר שפולינום $q$ מחלק את $f$ אם $r = 0$ ומסמנים $q \mid f$.

**הגדרה 4.** חוק אוקלידי הוא חוג שמעליו אפשר לבצע פירוק פולינום כזה.

דוגמה לחוג שאינו אוקלידי: $\mathbb{Z}[\sqrt{-5}]$ הוא $\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

**משפט 3.** חוג אוקלידי $\Longleftarrow$ פריקות יחידה (דומה למשפט היסודי של האריתמטיקה).

לדוגמה בחוג לעיל $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ על אף ש־$2, 3$ אי־פריקים וכן $(1 + \sqrt{-5}), (1 - \sqrt{-5})$ אי פריקים.

**מסקנה 1.**

- $(x - a) \mid f \iff f(a) = 0$ (משפט בזו)
- אם $\deg f = n > -\infty$, ל־$f$ לכל היותר $n$ שורשים כולל ריבוי.
- נניח ש־$f, g \in \mathbb{F}[x]$ ו־$F \subseteq K$, כאשר $K$ שדה. אם $g \mid f$ מעל $K$ אז $g \mid f$ מעל $\mathbb{F}$.

הוכחה.

1. $\Longrightarrow$ נניח $x - a \mid f$. אז קיים פולינום $g$ כך ש־$f = (x - a)g$. אז $f(a) = (a - a)g(a) = 0$.
   $\Longleftarrow$ נניח $f(a) = 0$. אז קיימים $q, r \in \mathbb{F}[x]$ כך ש־$f = q(x - a)$ ועל כן $0 = f(a) = q(a)(a - a) + r(a) = 0$ ולכן $r(a) = 0$.
   משום ש־$r$ פולינום קבוע (דרגתו קטנה מ־1, כי חילקנו ב־$(x - a)$ מדרגה 1), אז $r(x) = 0$.
2. אינדוקציה
3. נוכיח ב"contrapositive": אנו יודעים ש־$P \to Q \iff \neg Q \to \neg P$. נניח ש־$f \nmid g$ מעל $\mathbb{F}$. קיימים $q, r \in \mathbb{F}[x]$ כך ש־$f = qg + r,\ r \neq 0$. הפירוק הזה הוא גם ב־$K[x]$. מיחידות $r$, נקבל ש־$f \nmid g$ כל מעל $K$.

■

### 1.1 עוד על תחומי שלמות

**הגדרה 5.** יהי $R$ תחום שלמות, $a, b \in R$. נאמר ש־$b \mid a$ אם קיים $c \in \mathbb{R}$ כך ש־$ac = b$.

**הגדרה 6.** $u \in R$ נקרא הפיך אם קיים $\alpha \in R$ כך ש־$\alpha u = 1$.

**משפט 4.** יהי $R$ תחום שלמות, $u \in R$ הפיך. יהי $a \in \mathbb{R}$. אז $u \mid a$.

הוכחה. $1 \mid a,\ u \mid 1$. יחס החלוקה טרנזטיבי ולכן $u \mid a$. ■

**סימון 1.** קבוצת ההפיכים מוסמנת ב־$R^x$.

**דוגמאות.**

1. אם $R = \mathbb{F}$, אז $\mathbb{F}^x = \mathbb{F} \setminus \{0\}$
2. אם $R = \mathbb{Z}$ אז $\mathbb{Z}^2 = \{\pm 1\}$
3. אם $R = \mathbb{F}[x]$ אז $R^x = \mathbb{F}^x$ (ההתייחסות לסקלרים $\mathbb{F}$ היא כאל פונקציות קבועות)

**הגדרה 7.** $a, b \in R$ נקראים חברים אם קיים $u \in R^x$ הפיך כך ש־$a = ub$, ומסמנים $a \sim b$

"אני אני חבר של עומר, ועומר חבר של מישהו בכיתה שאני לא מכיר, אני לא חבר של מי שאני לא מכיר." המרצה: "למה לא? תהיה חבר שלו".

**משפט 5.** יחס החברות הוא יחס שקילות.

הוכחה. א. $a \sim a$ כי $1 \in R^x$

ב. אם $a \sim b$ אז קיים $u \in R^x$ כך ש־$a = ub$. קיים ל־$u$ הופכי $\alpha$ אז $\alpha a + \alpha ub = b$ ולכן $b \sim a$.

ג. נניח $a \sim b \wedge b \sim c$, כי מכפלת ההופכיים הפיכה $a \sim c$ וסיימנו.

■

**משפט 6.** הופכי הוא יחיד

(אותה ההוכחה כמו בשדה. לא בהכרח בתחום שלמות, מעל כל חוג)

הוכחה. יהי $a \in R^x$ ו־$u, u'$ הופכיים שלו, אז:

$$u = u \cdot 1 = u \cdot a \cdot u' = 1 \cdot u' = u'$$

■

**משפט 7.** אם $a \mid b$ וכס $b \mid a$ אז $a \mid b$ (בתחום שלמות).

הוכחה.

$$a \mid b \implies \exists c \in \mathbb{R}\colon ac = b$$
$$b \mid a \implies \exists d \in \mathbb{R}\colon bd = a$$

לכן:

$$ac = b \implies acd = a \implies a(cd-1) = 0 \implies a = 0 \vee cd = 1$$

■

אם $a = 0$ אז $b = 0$ (ממש לפי הגדרה) ו־$\sim$ שקילות (רפליקסיביות). אחרת, $cd = 1$ ולכן $c$ הפיך, סה"כ $b \mid a$.

"אני חושב שבעברית קראו להם ידידים, לא רצו להתחייב לחברות ממש".

**הגדרה 8.** איבר $p \in R$ נקרא אי־פריק אם מתקיים $p = ab \implies a \in R^x \vee b \in R^x$.

**הגדרה 9.** איבר $p \in R$ יקרא ראשוני אם $p \mid (a \cdot b) \implies p \mid a \vee p \mid b$.

הערה: איברים הפיכים לא נחשבים אי־פריקים או ראשוניים. הסיבה להגדרה: בשביל נכונות המשפט היסודי של האריתמטיקה (יחידות הפירוק לראשוניים).

**משפט 8.** בתחום שלמות כל ראשוני הוא אי פריק.

הערה: שקילות לאו דווקא.

הוכחה. יהי $p \in R$ ראשוני. יהיו $a, b \in R$ כך ש־$p = ab$. בה"כ $p \mid a$. אז קיים $c$ כך ש־$pc = a$ ולכן $pcb = p$. סה"כ $p \neq 0$ ולכן $cb = 1$ (ראה לעיל) ו־$b$ הפיך. ■

**משפט 9.** נניח שבתחום שלמות $R$, כל אי־פריק הוא גם ראשוני. אז $R$ תחום פריקות יחידה.

**הגדרה 10.** $R$ תחום פירוקת יחידה אם $\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_i$ עבור $p_i, q_j$ ראשוניים, אז $m = n$, ועד לכדי סידור מחדש, לכל $i \in [n]$ $p_i \sim q_i$

ההוכחה: זהה לחלוטין לזו של המשפט היסודי.

הוכחה. באינדוקציה על $n+m$. בסיס: $n+m=2$ ולכן $n=m=1$ (כי מעפלה ריקה לא רלוונטית מאוד) אז $p=q$. נעבור לצעד. נניח שהטענה נכונה לכל $n+m<k$. נניח ש־$n+m=k$. אז $p_1 \mid \prod_{j=1}^{m} q_j$. בה"כ $p_1 \mid q_1$. $q_1$ אי־פריק ולא הפיך. $p_1$ לא הפיך. לכן $p_1 \sim q_1$. אז עד כדי כפל בהופכי נקבל ש־$\prod_{i=2}^{n} p_i = \prod_{j=2}^{n} q_j$. הערה: ראשוני כפול הפיך נשאר ראשוני. מכאן הקענו לדרוש וסיימנו (הערה שלי: כאילו תכפילו בחברים ותקבלו את מה שצריך). ■

**הגדרה 11.** יהי $R$ תחום שלמות. תת־קבוצה $0 \neq I \subseteq R$ נקראת אידיאל אם:

A. $\forall a,b \in I\colon a+b \in I$ – סגירות לחיבור.

A. $\forall a \in I \, \forall b \in R\colon ab \in I$ – תכונת הבליעה. [בפרט $0 \in I$]

**דוגמאות:**

1. $0$ תמיד אידיאל, כך החוג תמדי אידיאל.
2. הזוגיים ב־$\mathbb{Z}$.
3. לכל $n \in \mathbb{Z}$, $n\mathbb{Z}$ אידיאל ($n$ כפול השלמים). הזוגיים מקרה פרטי.
4. $\langle f \rangle \subseteq \mathbb{F}[x]$ המוגדר לפי $\langle f \rangle := \{g \in \mathbb{F}[x] \mid f|g\}$
5. הכללה של הקודמים: עבור $a \in R$ נסמן $\langle a \rangle := \{a \cdot b \mid b \in R\}$
6. $I = \{f \in \mathbb{F}[x] \mid f(0)=0\}$ (לעיתים מסומן $\forall a \in R\colon aR = \langle a \rangle$)
7. נוכל להכליל את 4 עוד: ("הכללה של הכללה היא הכללה. זה סגור להכללה. זה קורה הרבה במתמטיקה")

$$I = aR + bR = \{ar + bs \mid r,s \in R\}$$

וניתן להכליל עוד באינדוקציה.

**הגדרה 12.** אידיאל $I$ נקרא ראשי אם הוא מהצורה $aR$ עבור $a \in R$ כלשהו.

**הגדרה 13.** תחום שלמות נקרא ראשי אם כל אידיאל שלו ראשי.

**משפט 10.** נניח ש־$R$ ראשי, אז כל אי־פריק ב־$R$ הוא ראשוני.

(תנאי מספיק אך לא הכרחי)

הוכחה. יהי $p \in R$ אי פריק. נראה שהוא ראשוני. נביט ב־$ab \in R$ כך ש־$p \mid ab$. נביט ב־$I = aR + bR$. מהיותו ראשי קיים איזשהו $c \in R$ כך ש־$I = cR$. אז $c \in I$ (כי $c \cdot 1 \in R$). אז $a,p \in I$. $a$ ברור. קיים $d \in R$ כך ש־$pd = a \cdot b$. למה $p \in I$ – המרצה דפק קליגמן ולא יודע להוכיח. אחרי משהו כמו 5 דק' של בהיה בלוח הוא בה עם הדבר הבא:

$$c \in I \implies \exists r,s \in \mathbb{R}\colon ar + bs = c$$

"אני אחושב על זה ואני אמשיך פעם הבאה". ■

.................................................................................................................

**שחר פרץ, 2025**

קומפל ב־$\LaTeX$ ונוצר באמצעות תוכנה חופשית בלבד