לינארית 2א ~ סיכום שביעי ~ פולינומים וכו'

שחר פרץ

28 באפריל 2025

הערות: אנחנו סימנו אידיאל ב־aR ובקורס מסמנים Ra, באופן כללי אפשר לדבר על אידיאל שמאלי ואידיאל ימני. תזכורת: $I \subseteq R$ היא אידיאל אם היא סגורה לחיבור ומקיימת את תכונת הבליעה. בתחום ראשי כל אידיאל הוא אידיאל ראשי.

משפט 1. ב־$R \neq \{0\}$ תחום ראשי אז כל אי פריק הוא ראשוני.

הוכחה. יהי o אי פריק (א"פ). יהיו $a, b \in \mathbb{R}$ כך ש־$p \mid ab$. תיקון [משבוע שעבר]: במקום $I = Ra + Rb$, נשתמש ב־$I = Ra + Rp$. בכלל ש־R תחום ראשי, קיים $c \in R$ כך ש־$I = Rc$, ו־$a, p \in I$ כלומר $p \mid c \wedge c \mid a$. p א"פ ולכן $p \sim c$ או c הפיך.

- c הפיך $\implies \in I \implies R = R \cdot 1 \in I \subseteq R \implies I = R$. קיימים $r, s \in R$ כך ש־$ra + sp = 1$. נכפיל ב־b ונקבל $rab + spb = b$ וסה"כ $p \mid b$.
- אם $p \sim c$, אז $a \mid c \wedge c \mid p$ ולכן $p \mid a$.

■

מסקנה 1. אם R תחום שלמות ראשי אזי יש פריקות יחידה למכפלה של אי פריקים עד כדי חברות.

משפט 2. יהיו $a, b \in R$, אז a, b ייקראו זרים אם $\forall c \in R \colon c \mid a \wedge c \mid b \implies c \in R^x$

הגדרה 1. יהי $g \in R$ כך ש־:

1. $g \mid a \wedge g\imath b$
2. $\forall \ell \in R \colon \ell \mid a \wedge \ell \mid b$
3. $\ell \mid g$

אז g כנ"ל הוא הגורם המשותף המקסימלי של a, b, הוא $\gcd(a, b)$

משפט 3. יהי R תחום שלמות ויהיו $a, b \in R$. נניח שקיימים $r, s \in R$ כך ש־$g = ra + sb$ אשר מחלק את a, b. אז:

- $\gcd(a, b) = g$
- ה־$\gcd$ מוגדר ביחידות עד לכדי חברות.
- בתחום ראשי, לכל a, b קיים g כנ"ל.

(הערה: רק 3 באמת דורש תחום ראשי)

הוכחה.
- יהי $\ell \mid a, b$ אז $\ell \mid ra, sb$ וסה"כ $\ell \mid g$.
- מ־1 (בערך) אם g, g' מקיימים את היותם $\gcd$ אז $g \mid g' \wedge g' \mid g$ ולכן $g \sim g'$.
- נסמן $I = Ra + Rb$. אז $I = Rg$, וקיימים $r, s \in R$ כך ש־$ra + sb = g$ ולכן $a, b \in I$ אז $g \mid a, b$ וסיימנו מ־1.

■

מסקנה 2. בתחום ראשי, אם a, b זרים אז $\exists r, s \in \mathbb{R} \colon ra + sb = 1$ (אלגוריתם אוקלידס המורחב).

משפט 4. $\mathbb{F}[x]$ תחום ראשי.

הוכחה. יהי $I \subseteq \mathbb{F}[x]$ אידיאל. אם $I = \{0\}$, הוא ראשי. אחרת, $I \neq \{0\}$, ואז: יהי $0 \neq p \in I$ פולינום מדרגה מינימלית, ויהי $f \in I$. אז קיימים $q, r \in \mathbb{F}[x]$ כך ש־$f = qp + r$. ידוע $\deg r < \deg p$. בגלל ש־$f \in I \wedge p \in I$ אז $f - qp \in I$. אם r אינו 0, קיבלנו סתירה למינימליות הדרגה של p. ■

הוכחה זהה עובדת בשביל להראות ש־$\mathbb{Z}$ תחום ראשי, אך עם דרגה במקום ערך מוחלט.

הגדרה 2. תחום שלמות נקרא אוקלידי אם קיימת $N \colon R \setminus \{0\} \to \mathbb{Z}$ כך ש־$\forall a, b \in R \setminus \{0\} \, \exists u, r \in R \colon a = ub + r$ כאשר $r = 0$ או $N(b) > N(r)$

ברגע שיש לנו את ההגדרה של תחום אוקלידי, N הפונקציה שתשתמש אותנו בשביל להראות את ההוכחה שכל תחום אוקלידי הוא תחום ראשי (בדומה לערך מוחלט או $\deg$ בהוכחות קודמות). ההפך אינו בהכרח נכון.

הגדרה 3. נורמה היא פונקציה $N: R \to \mathbb{Z}$ כך שהיא סאב־אדטיבית $N(a+b) \leq N(a) + N(b)$, כיפלית ו־$N(1) = 1$.

דוגמה (חוג השלמות של גאוס)**.**

$$R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

הנורמה:

$$N: \mathbb{R} \to \mathbb{Z}_{\geq 0},\ \ N(a+bi) = a^2 + b^2 = |a + bi|^2$$

בדומה להוכחה לפיה הערך המוחלט של מורכב הוא כפלי, ניתן להראות ש־N כפלית. מי הם ההפיכים ב־$\mathbb{Z}[i]$? מי שמקיים $\alpha\beta = 1$, כלומר:

$$N(\alpha)N(\beta) = 1 = N(1),\ \ \alpha = a + bi,\ \ a^2 + b^2 = 1 \implies a + bi = \pm 1, \pm i$$

משפט 5. יהי $p \in \mathbb{Z}$ ראשוני. התנאים הבאים שקולים:

- p פריק ב־$\mathbb{Z}[i]$
- $p = m^2 + n^2$ עבור $n, m \in \mathbb{Z}$
- $p = 2$ או $p \equiv 1 \pmod 4$
- קיימים $r, s \in R$ כך ש־$ra + sb = 1$

שימו לב ש־$\mathbb{Z}$ בתוך $\mathbb{Z}[i]$ לא סגורים לבליעה.

. . . .

שחר פרץ, 2025

קומפל ב־LaTeX ונוצר באמצעות תוכנה חופשית בלבד