

אלגברה ב' 2 – הרצאה 2

23.02.11

בהרצאה הקודמת דיברנו על חוגים. להזכירכם תמיד עם יחידה. יהי R תחום (R חילופי, $c = ab = 0 \Rightarrow a = 0$ או $b = 0$).

משפט. קיים שדה F כך ש- $R \subseteq F$ תת חוג.

בפרט אם K שדה כלשהו אז $K[x]$ הוא תחום ולכן הוא מוכל בשדה.

הוכחה. מדובר בשדה המנות. נגדיר יחס על הקבוצה:

$$\{(a, b) \in R^2 | b \neq 0\}$$

נגדיר יחס $\sim$ על הקבוצה:

$$(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$$

בתור תרגיל צריך להוכיח שזה יחס שקילות. נסמן את מחלקת השקילות של (a, b) בסימון המוזר והבלתי צפוי $\frac{a}{b}$. כעת אפשר לכתוב:

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b$$

למעשה אנחנו מחכים את בניית הרציונליים מהשלמים. קבוצת כל מחלקות השקילות נסמן ב- $F = \text{Quot}(R)$. נגדיר חיבור וכפל על F :

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$$

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

תרגיל נוסף הוא להוכיח שההגדרות כאן טובות. כלומר, שאין תלות בבחירת הנציג של מחלקת שקילות (אתם זוכרים שזה למעשה מחלקות שקילות ולא שברים? נכון?). כמו כן, F הוא שדה. גם זה צריך לבדוק. וגם זה יישאר כתרגיל. כעת מה הקשר בין השדה לחוג שלנו? יש העתקה $R \rightarrow F$ ע"י

$$a \mapsto \frac{a}{1}$$

זהו מונומורפיזם (הומומורפיזם חח"ע) של חוגים. R לא בדיוק מוכל אך אפשר לזהות אותו עם תת קבוצה של F . נזהה את R עם תמונת ההעתקה הנ"ל ואז $R \subseteq F$ תת חוג. $\square$

הערה. אם F שדה ויש הומומורפיזם $\lambda : R \rightarrow K$ אז λ ניתן להרחבה באופן יחיד להומומורפיזם $\lambda : F \rightarrow K$.

דוגמאות.

1. בניית הרציונליים מהשלמים.

2. שדה הפונקציות הרציונליות מעל שדה K :

$$\text{Quote}(K[x]) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in K[x], g \neq 0 \right\}$$

פריקות בחוגים

בפרק זה R הינו תחום.

טענה. (כלל הצמצום)

אם $a \in R$ וכן $0 \neq a$ וכן $b, c \in R$ כך שמתקיים $ab = ac$ אז $b = c$.

הוכחה. לאו דווקא יש הופכי. אז:

$$a(b - c) = ab - ac = 0$$

□

לכן $b - c = 0$ ולכן $b = c$.

בדיחה. לפעשה יש הופכי. אפשר להרחיב לשדה, להכפיל בהופכי ולהחזיר בחזרה לתחום.

הגדרה. תחום R נקרא ראשי (PID) אם כל אידאל ב- R ראשי. כלומר כל אידאל הוא מהצורה (a) .

משפט. יהי F שדה. אז $R = F[x]$ הוא תחום ראשי.

הוכחה. למי שזוכר יש לנו חילוק עם שארית על פולינומים: יהיו $f, g \in R$ וכן $g \neq 0$ אז יש $q, r \in R$ יחידים כך ש-

$$f = gq + r, \quad \deg(r) < \deg(g)$$

זה הוכיח בורובוי!

יהי $I \in R$ אידאל. נראה שהוא ראשי. בה"כ $I \neq 0$ (כי 0 הינו אידאל ראשי). אזי קיים $g \in I$ וכן $g \neq 0$. נבחר g כזה מהמעלה הקטנה ביותר. $g \in I$ לכן $(g) \subseteq I$. נראה הכלה הפוכה. יהי $f \in I$ נחלק את f עם שארית ב- g .

$$f = gq + r, \quad \deg(r) < \deg(g)$$

$$r = f - gq$$

$f \in I$ וכן בגלל ש- $g \in I$ גם $gq \in I$. לכן גם $r \in I$. בנוסף $\deg(r) < \deg(g)$ לכן ממנימליות g מתקיים $r = 0$. מכאן, $f = gq$ ולכן $f \in (g)$. □

תרגיל. באופן דומה $\mathbb{Z}$ תחום ראשי.

הגדרה. R תחום. ניקח $a, b \in R$.

1. $a|b$ אם יש $u \in R$ כך ש- $b = a \cdot u$.

הערה. אם $a \neq 0$ אז u כנ"ל יחיד. מ"כלל הצמצום".

2. a הפיך אם $a|1$.

הערה. כבר הגדרנו. זאת הגדרה שקולה בסימון החדש.

3. a נקרא ראשוני אם $a \neq 0$, a אינו הפיך ואם $a|a_1a_2$ אז $a|a_1$ או $a|a_2$.

4. a נקרא אי פריק אם $a \neq 0$, a אינו הפיך וכן אם $a = a_1a_2$ אז a_1 הפיך או a_2 הפיך.

באופן שקול במונחי אידאלים:

1. $a|b$ אם ורק אם $b \in (a)$ אם ורק אם $(b) \subseteq (a)$

2. a הפיך $\Leftrightarrow (a) = (1) = R$.

3. a ראשוני $\Leftrightarrow (a) \neq R$ וכן אם $a_1a_2 \in (a)$ אז $(a_1) \subseteq (a)$ או $(a_2) \subseteq (a)$ או $(a) \neq 0$ אידאל ראשוני.

4. a אי פריק $\Leftrightarrow (a)$ מרבי בקבוצה $\{(b)|0 \neq (b) \neq R, b \in R\}$

מסקנה. יהיו $a, b \in R$ שונים מ-0. אז

1. $b = au \Leftrightarrow (b) \subseteq (a)$ בפרט, $u \in R^*$, $b = au \Leftrightarrow a|b, b|a \Leftrightarrow (a) = (b)$
 $u \in R \setminus R^*$

2. אם $u \in R^*$ אז au מקיים את 4 התכונות הנ"ל $\Leftrightarrow a$ מקיים את 4 התכונות הנ"ל.

3. אם a ראשוני אז a אי פריק.

4. יהי R תחום ראשי. אז a אי פריק $\Leftrightarrow (a)$ מרבי $\Leftrightarrow (a)$ ראשוני.

5. היחס $\sim$ שמוגדר ע"י: $a \sim b \Leftrightarrow (a) = (b)$ הוא יחס שקילות על האיברים האי פריקים.

הוכחה.

1. נראה כי $a|b, b|a \Leftrightarrow b = au, u \in R^*$

לפי הגדרה ראשונה יש $u \in R$ כך ש- $b = au$, $a = bu$ אז $a = auv$. לפי היחידות $uv = 1$ ולכן $u, v \in R^*$. כיוון שני ברור. גרירה ראשונה לפי ההגדרה.

2. $(b) = (a) \Leftrightarrow b = au, u \in R^*$ ומכאן זה ברור.

3. נניח $a = a_1 \cdot a_2$ לכן $a|a_1 \cdot a_2$ ולכן a מחלק אחד מהם (כי a ראשוני). נניח בה"כ $a|a_1$. אבל, $a_1|a = a_1 \cdot a_2$ לכן יש $u \in R^*$ כך ש- $a = a_1u$. לפי היחידות של a מתקיים $a_2 = a \in R^*$ ולכן a אי פריק.

לבסוף, נוכיח שקילות בין ההגדרה 4 להגדרה 4 במונחי אידאלים.

הגדרה 4 $\Leftrightarrow (a) \neq 0 \neq R$ ואם $a = a_1a_2$, $a_2 \notin R^*$ אז $a_1 \in R^*$ $\Leftrightarrow (a) \neq 0 \neq R$ ואם $(a_1) = R$ (בעזרת מסקנה 1).

□

לפי (5)

אפשר לכתוב בעזרת מייצגים $\{p_i\}_{i \in I}$ של איברים אי פריקים ב- R מודולו $\sim$. למשל, אם $R = F[x]$ אז $R^* = F^* = F \setminus \{0\}$ ונבחר $\{p_i\}_{i \in I}$ להיות פולינומים אי פריקים מתקונים. ב- $\mathbb{Z}$, $\mathbb{Z}^* = \{\pm 1\}$ נבחר $\{p_i\}_{i \in I}$ חיוביים.

הגדרה. תהי $\{p_i\}_{i \in I}$ מערכת מייצגים של אי פריקים של R . אז R יקרא תחום פריקות (UFD) אם לכל $a \in R$, $a \neq 0$ יש הצגה יחידה מהצורה $a = u \prod_{i \in I} p_i^{m_i}$ כאשר $m_i \geq 0$ שלמים כמעט כולם 0 וכן $u \in R^*$.

תרגיל. ההצגה איננה תלויה בבחירה של $\{p_i\}_{i \in I}$.

תרגיל. אם R תחום פריקות אז a אי פריק $\Leftrightarrow a$ ראשוני.

משפט. תחום ראשי הינו תחום פריקות.

הוכחה. יהי R תחום ראשי. נראה קיום ההצגה המבוקשת. נגיד כי $a \in R$, $a \neq 0$ הוא "רע" אם אין לו הצגה בסימונים הנ"ל:

$$(*) u \prod p_i^{m_i}$$

נניח בשלילה כי a_0 רע. אזי a_0 פריק (אחרת a_0 אי-פריק ואז קיימים u, i כך ש- $a_0 = u \cdot p_i$ ואז $a = u \cdot p_i^1 \cdot \prod_{j \neq i} p_j^0$). לכן, $a_0 = a_1 \cdot a'_1$ כאשר $a_1, a'_1 \notin R^*$. לא ייתכן כי ל- a'_1, a_1 יש הצגות $(*)$, כי אחרת מכפלתן הייתה נותנת הצגה $(*)$ של $a_0 = a_1 \cdot a'_1$. בה"כ a_1 הוא רע. אז $(a_0) \subsetneq (a_1)$. באינדוקציה קיימת סדרה אינסופית של איברים רעים כך שמתקיים:

$$(a_0) \subsetneq (a_1) \subsetneq \dots$$

נסמן $I = \bigcup_{n=0}^{\infty} (a_n) \subseteq R$. כזה הוא אידאל (קל להראות) ולפי ההנחה, יש $a \in R$ כך ש- $(a) = I$ (כי R תחום ראשי). אז $a \in I$ ולכן יש k עבורו $a \in (a_k)$. ואז,

$$(a) \subsetneq (a_k) \subsetneq (a_{k+1}) \subsetneq \dots \subseteq I = (a)$$

□

סתירה.

טענה. לכל $j \in I$ בהצגה $(*)$:

$$p_j | a \Leftrightarrow m_j \geq 1$$

הוכחה. נניח $p_j | a = u \cdot p_j^{m_j} \cdot \prod_{i \neq j} p_i^{m_i}$. p_j הוא אי פריק ולכן ראשוני (כי R תחום ראשי) ולכן מחלק את אחד הגורמים באגף ימין.

לא מתקיים $p_j | a$ כי p_j אינו הפיך (אחרת $(p_j) \supset (a) = R$ ואז p_j הפיך). לכן קיים $i \in I$ כך ש- $p_j | p_i$ וגם $m_i \geq 1$ אחרת p_i לא מופיע בהצגת a . לכן $p_i = p_j \cdot v$ כאשר $v \in R$. p_i לא פריק ולכן r או p_j הפיכים. p_j לא הפיך ולכן v הפיך לכן $p_i \sim p_j$ ולכן $i = j$ (כי זאת מערכת מייצגים) ולכן $m_i = m_j \geq 1$.

□

הכיוון השני ברור. זהו שלב ראשון באינדוקציה ואת השלב השני נעשה בשיעור הבא.