

אלגברה ב' 2 - הרצאה 3

28.02.11

היינו באמצע משפט:

משפט. R תחום ראשי $\Leftarrow R$ תחום פריקות. כלומר לכל $a \in R$ יש הצגה יחידה $a = u \prod_{i \in I} p_i^{m_i}$ כך ש- $u \in R^*$ וכן $m_i \geq 0$ שלמים כמעט כולם 0.

הוכחה. הוכחנו קיום והוכחנו שאם $j \in I$ אז $m_j > 0$ $\Leftrightarrow p_j | a$. מזה רוצים להוכיח יחידות. נניח

$$v \prod_{i \in I} p_i^{n_i} = a = u \prod_{i \in I} p_i^{m_i}$$

$v, u \in R^*$ וכן $m_i, n_i > 0$ שלמים כמעט כולם 0. יהי $j \in I$ נראה $m_j = n_j$. בה"כ $m_j \leq n_j$ ונראה שוויון באינדוקציה על m_j . לפי הטענה שהוכחנו, אנחנו יודעים ש- $n_j > 0 \Leftrightarrow m_j > 0$ כי זה תלוי רק באם $p_j | a$ או לא. לכן אם $m_j = 0$ אז גם $n_j = 0$. נניח $m_j > 0$. לכן $n_j \geq m_j > 0$. נצמצם במשוואת הפירוק ב- p_j :

$$vp_j^{n_j-1} \prod_{i \neq j} p_i^{n_i} = up_j^{m_j-1} \prod_{i \neq j} p_i^{m_i}$$

מהנחת האינדוקציה $n_j - 1 = m_j - 1$ ולכן $m_j = n_j$. כעת, מדוע $u = v$? המכפלה $\prod_{i \in I} p_i^{m_i} = \prod_{i \in I} p_i^{n_i}$ נחלק בביטוי זה ונקבל $u = v$. אז ההצגה יחידה ותחום ראשי הוא תחום שלמות. $\square$

מסקנה. יהי F שדה, אז $F[x]$ וכן $\mathbb{Z}$ הם תחומי פריקות (כי ראשיים).

תרגיל. יהיו $a, b \in R$ כאשר $0 \neq a, b$ תחום ראשי. יהיו $a = u \prod_{i \in I} p_i^{m_i}$ ו- $b = v \prod_{i \in I} p_i^{n_i}$ פירוקים כמו במשפט. אז $a | b \Leftrightarrow m_i \leq n_i \forall i \in I$.

הוכחה. $a | b \Leftrightarrow$ קיים c כך ש- $ac = b$. נכתוב פירוק גם ל- c :

$$c = w \prod_{i \in I} p_i^{k_i}$$

$\Leftrightarrow$

$$v \prod_{i \in I} p_i^{n_i} = uw \prod_{i \in I} p_i^{m_i + k_i}$$

$\Leftrightarrow$ יש $w \in R^*$ ויש $k_i > 0$ שלמים כמעט כולם 0 כך ש- $v = uw$, $n_i = m_i + k_i$. $\square$ $n_i \geq m_i$

הערה. יהי R תחום שלמות ויהיו $a_1, \dots, a_n \in R$ אז

$$(a_1, \dots, a_n) := (a_1) + \dots + (a_n) = \left\{ \sum_{i=1}^n b_i a_i \mid b_i \in R \right\}$$

הוא אידאל כסכום של אידאלים והוא האידאל הקטן ביותר (לפי הכלה) המכיל את $a_1, \dots, a_n$.

מחלק מרבי מקסימלי

R הוא תחום. עד שנאמר אחרת.

הגדרה. איבר $d \in R$ יקרא מחלק מרבי משותף של $a_1, \dots, a_n \in R$ אם מתקיים: $d \mid a_1, \dots, d \mid a_n$ וכן אם $d' \mid a_1, \dots, d' \mid a_n$ אז $d' \mid d$.

הערה. היות והוא לא יחיד נסמן: $d \in \gcd(a_1, \dots, a_n)$.

נכתוב ניסוח שקול באמצעות אידאלים:

הגדרה. איבר $d \in R$ יקרא מחלק מרבי משותף של $a_1, \dots, a_n \in R$ אם מתקיים: $a_1, \dots, a_n \in (d)$ וכן אם $a_1, \dots, a_n \in (d')$ אז $(d) \subseteq (d')$. כלומר, (d) הוא האידאל הראשי הקטן ביותר שמכיל את $a_1, \dots, a_n$.

לא ברור שקיים d כזה. בחוג ראשי זה בסדר.

דוגמא. $R = \mathbb{Z}$

$$\pm 3 \in \gcd(6, 9)$$

כי כל המחלקים הם $\pm 1, \pm 3$.

למה. יהי $a_1, \dots, a_n, d, d' \in R$

$$1. \text{ אם } d \in \gcd(a_1, \dots, a_n) \text{ אז } d' \in \gcd(a_1, \dots, a_n) \Leftrightarrow (d') = (d) \Leftrightarrow (d' = u \cdot d \quad u \in R^*)$$

$$2. \text{ אם } R \text{ תחום פריקות אז } \gcd(a_1, \dots, a_n) \neq \emptyset. \text{ ביתר דיוק: אם } a_j = u_j \prod_{i \in I} p_i^{n_{ij}} \text{ הפירוק עבור } j = 1, \dots, n \text{ אז } d = \prod_{i \in I} p_i^{\min_j(n_{ij})} \in \gcd(a_1, \dots, a_n)$$

$$3. \text{ אם } R \text{ תחום פריקות ו- } c \in R \text{ אז } \gcd(ca_1, \dots, ca_n) = c \cdot \gcd(a_1, \dots, a_n)$$

$$4. \text{ אם } R \text{ תחום ראשי אז } d \in \gcd(a_1, \dots, a_n) \Leftrightarrow (d) = (a_1, \dots, a_n)$$

$$5. \text{ אם } R \text{ תחום ראשי ו- } d \in \gcd(a_1, \dots, a_n) \text{ אז יש } b_1, \dots, b_n \in R \text{ כך ש-} d = \sum_{j=1}^n a_j b_j$$

הוכחה.

1. לפי הניסוח השקול עבור אידאלים.

$$2. \text{ יהי } d' = u' \prod_{i \in I} p_i^{k_i} \text{ אז } d' \mid a_1, \dots, a_n \Leftrightarrow k_i \leq n_{ij} \text{ לכל } j \text{ ולכל } i \in I \Leftrightarrow k_i \leq \min_j(n_{ij})$$

$$\text{מכאן, } d \text{ מקיים תנאי זה וגם מקיים } d' \mid d \text{ לכל } d' \text{ כזה אם } k_i = \min_j(n_{ij}) \text{ לכל } i \in I. \text{ לכן מכפלה } u \prod_{i \in I} p_i^{\min_j(n_{ij})} \in \gcd(a_1, \dots, a_n) \text{ לכל } u \in R^*$$

3. נעשה בשיעור הבא.

4. $(d) = (a_1, \dots, a_n)$ וזה האידאל הקטן ביותר שמכיל את $a_1, \dots, a_n$.

5. מהסעיף הקודם וההגדרה של $(a_1, \dots, a_n)$.

□