

תרגול 10 - חילוק פולינומים

1 ביוני 2021

1 שאריות מתרגול קודם

תרגילים:

1. יהי R חוג עם יחידה, $S \leq R$ תת-חוג. אם $1_R \in S$ אז S חוג עם יחידה, והיחידה היא: 1_R .

פתרון: יהי $s \in S$, מהגדרת יחידה ומכיון ש- $s \in R$ מתקיים:

$$s \cdot 1_R = 1_R \cdot s = s$$

ולכן 1_R יחידה של S , ומיחידות היחידה, זוהי היחידה של S .

2. האם $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$ תת-חוג של $\mathbb{R}^{2 \times 2}$? אם כן, האם זהו תת-חוג עם יחידה?

פתרון: ראינו בתרגול קודם שזהו אכן תת-חוג.

מה לגבי היחידה? נתחיל באופן כללי. תרגיל קודם אומר שאם $1_R \in S$ אז הוא איבר

היחידה של S . מה קרוה כאשר $1_R \notin S$?

תשובה - הכל יכול להיות: אפשרי ש- S חוג בלי יחידה. אפשרי גם ש- S חוג עם

יחידה, עבור $1_S \neq 1_R$.

ועכשיו נחזור לתרגיל שלנו. נשים לב ש- S חוג עם יחידה עבור

$$1_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

2 אלגוריתם אוקלידוס לפולינומים

משפטים:

1. יהי $\mathbb{F}, \mathbb{F}[x]$ חוג הפולינומים. אזי לכל $a(x), b(x) \in \mathbb{F}[x]$ כך ש- $b(x) \neq 0$ קיימים $q(x), r(x)$ כאשר $\deg(r) < \deg(b)$, כך ש-:

$$a(x) = q(x)b(x) + r(x)$$

2. קיום מחלק משותף מקסימלי: לכל $a(x), b(x)$ קיים פולינום מתוקן $d(x)$ (מתוקן = פולינום בו המקדם של החזקה הגבוהה ביותר הוא 1, כלומר מהצורה $x^k + \dots + \alpha_{k-1}x^{k-1} + \dots$) כך ש-:

$$d(x) | a(x), b(x) \quad (\text{א})$$

$$\deg(d') \leq \deg(d) \text{ אז } d' | a, b \quad (\text{ב})$$

(ג) מתקיים: קיימים $m(x), n(x)$ כך ש-:

$$d(x) = \gcd(a, b) = m(x)a(x) + n(x)b(x)$$

3. משפט הקיום מתבסס על המשפט הבא: אם $a = qb + r$ אז:

$$\gcd(a, b) = \gcd(b, r)$$

הוכחה: נראה שכל פולינום שמחלק את a, b מחלק גם את r : נניח $d | a, b$ כלומר, קיימים p, w כך ש-:

$$a = dp, b = dw$$

נקבל:

$$r = a - bq = dp - dwq = d(p - wq)$$

ולכן

$$d | r$$

בנוסף, נראה שאם $d | b, r$ אז $d | a$: קיימים p, w כך ש-:

$$b = dw, r = dp$$

ואז נקבל:

$$a = bq + r = dwq + dp = d(wq + p)$$

ולכן

$$d|a$$

בסה"כ קיבלנו שקבוצת המחלקים המשותפים של b, r שווה לזו של a, b , ולכן גם המקסימלי (המתוקן) ביניהם זה אותו אחד. מש"ל.

4. האלגוריתם למציאת $\gcd(a_1, b_1)$ עבור $\deg(a_1) \geq \deg(b_1)$:

(א) נרשום $a = q_1 b + r_1$ ואז $\gcd(a, b) = \gcd(b, r_1)$ ואז נמשיך עם $a_2 = b_1, b_2 = r_1$

(ב) תנאי עצירה: כאשר $r_{k+1} = 0$ אז

$$\gcd(a, b) = r_k$$

תרגילים:

1. מצאו את $\gcd(a, b)$ עבור: $a(x) = x^6 + x^5 + x^4 + x^2 + 1, b(x) = x^3 + x + 1$.
ורשמו אותו כצ"ל שלהם.
פתרון: נתחיל בחילוק:

$$\begin{array}{r|l} q_1(x) = x^3 + x^2 - 2 & \\ \hline x^6 + x^5 + x^4 + x^2 + 1 & x^3 + x + 1 \\ x^6 + x^4 + x^3 & \\ \downarrow & \\ x^5 - x^3 + x^2 + 1 & \\ x^5 + x^3 + x^2 & \\ \downarrow & \\ -2x^3 + 1 & \\ -2x^3 - 2x - 2 & \\ \downarrow & \\ r_1(x) = 2x + 3 & \end{array}$$

בסה"כ: $a(x) = q_1(x) \cdot b(x) + r_1(x)$ או בפולינומים עצמם:

$$x^6 + x^5 + x^4 + x^2 + 1 = (x^3 + x^2 - 2)(x^3 + x + 1) + 2x + 3$$

כעת אנחנו יודעים: $\gcd(a, b) = \gcd(b, r)$ נחלק שוב:

$$\begin{array}{r|l}
 q_2 = \frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8} & \\
 \hline
 x^3 + x + 1 & 2x + 3 \\
 x^3 + \frac{3}{2}x^2 & \\
 \downarrow & \\
 -\frac{3}{2}x^2 + x + 1 & \\
 -\frac{3}{2}x^2 - \frac{9}{4}x & \\
 \downarrow & \\
 \frac{13}{4}x + 1 & \\
 \frac{13}{4}x + \frac{39}{8} & \\
 \downarrow & \\
 r_2 = -\frac{31}{8} &
 \end{array}$$

קיבלנו: $b = q_2r_1 + r_2$, ומתקיים: $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2)$
 שימו לב שמתקיים: $r_2 | r_1$ כי:

$$r_1 = 2x + 3 = -\frac{31}{8} \cdot \left(-\frac{16}{31}x - \frac{24}{31} \right)$$

ולכן r_2 הוא מחלק משותף מקסימלי שאיננו מתוקן, נתקן וניקח

$$\gcd(a, b) = 1$$