

מבנים אלגבריים - תירגול 9

22 במאי 2019

משפט (חילוק פולינומים): יהא \mathbb{F} שדה. $\mathbb{F}[x]$ חוג הפולינומים. אזי לכל $a(x), b(x) \in \mathbb{F}[x]$ כך ש $b(x) \neq 0$ קיים $r(x), q(x)$ כך ש

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

המקיימים $deg(r) < deg(b)$ או $r = 0$. והם יחידים.

סימון $a|b$ אם קיים q כך ש $a = qb$.

משפט (נקיטת gcd): יהא \mathbb{F} שדה. $\mathbb{F}[x]$ חוג הפולינומים. אזי לכל $a(x), b(x) \in \mathbb{F}[x]$ קיים פולינום מתוקן $d(x) = \gcd(a, b)$ המקיים

1. $d | a, b$

2. אם $d' | a, b$ אז $deg(d') \leq deg(d)$.

3. בנוסף קיימים m, n כך ש

$$d = an + bm$$

דוגמא: $a(x) = x^6 + x^5 + x^4 + x^2 + 1, b(x) = 1 + x + x^3$ חלק את a ב b ומצאו $\gcd(a, b)$

פתרון

$\begin{array}{r} x^3 + x^2 - 2 \\ \hline x^6 + x^5 + x^4 + x^2 + 1 \\ x^6 + x^4 + x^3 \\ \hline \downarrow \\ x^5 - x^3 + x^2 + 1 \\ x^5 + x^3 + x^2 \\ \hline \downarrow \\ -2x^3 + 1 \\ -2x^3 - 2x - 2 \\ \hline \downarrow \\ 2x + 3 \end{array}$	$\begin{array}{r} x^3 + x + 1 \\ \hline \end{array}$
---	--

מתקיים כי

$$deg(2x + 3) < deg(x^3 + x^2 + 1)$$

$$a(x) = b(x) \cdot (x^3 + x^2 - 2) + (2x + 3)$$

נעבור ל gcd :

$$\begin{aligned} a(x) &= (x^3 + x^2 - 2) \cdot b(x) + (2x + 3) \\ &\downarrow \\ b(x) &= \left(\frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8}\right)(2x + 3) + \left(\frac{-31}{8}\right) \\ &\downarrow \\ (2x + 3) &= \left(-\frac{16}{31}x - \frac{24}{31}\right)\left(\frac{-31}{8}\right) + 0 \end{aligned}$$

ולכן ע"י הפיכת המקדם המוביל ל 1 נקבל כי gcd = 1
נקלף אחורה על מנת למצוא צירוף לינארי של a, b שנותן את ה gcd :

$$\begin{aligned} \frac{-31}{8} &= b(x) - \left(\frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8}\right)(2x + 3) \\ &= b(x) - \left(\frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8}\right)(a(x) - (x^3 + x^2 - 2) \cdot b(x)) \\ &= -\left(\frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8}\right)a(x) + \left[1 + \left(\frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8}\right)(x^3 + x^2 - 2)\right]b(x) \end{aligned}$$

ולכן

$$1 = \frac{8}{13} \left(\frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8}\right)a(x) - \frac{8}{31} \left[1 + \left(\frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8}\right)(x^3 + x^2 - 2)\right]b(x)$$

הגדרה: פולינום $p(x) \in \mathbb{F}[x]$ מדרגה גדולה מ-0 יקרא ראשוני אם מתקיים

$$\forall a(x), b(x) \in \mathbb{F}[x] : p(x) | a(x)b(x) \Rightarrow ([p(x) | a(x)] \vee [p(x) | b(x)])$$

הגדרה: פולינום $p(x) \in \mathbb{F}[x]$ מדרגה גדולה מ-0 יקרא פריק אם ניתן להציגו כמכפלה של פולינומים $a(x), b(x)$ מדרגה קטנה ממש מדרגת $p(x)$.

והוא יקרא אי פריק אם הוא לא פריק.

תרגיל: הוכיחו כי p אי פריק אמ"מ הוא ראשוני.

פתרון: בש.ב. תוכיחו כי אם p אי פריק אזי p ראשוני. בכיוון השני נניח כי p ראשוני ונוכיח כי הוא אי פריק. אכן נניח $p(x) = a(x)b(x)$ וצ"ל כי $a(x)$ או $b(x)$ שווים דרגה ל $p(x)$. כיוון ש $p(x)$ ראשוני ומתקיים כי $p(x) | a(x)b(x)$ אזי הוא מחלק אחד מהם. אם $p(x) | a(x)$ אזי מכיוון שגם $\deg(a(x)) \geq \deg(p(x))$ כיוון שדרגתו לא יכולה להיות גדולה ממש אזי הם שווים. באופן דומה אם $p(x) | b(x)$ אזי $\deg(p(x)) = \deg(b(x))$.

תרגיל: נסמן את קבוצת הפולינומים הראשוניים ב X . הוכיחו כי לכל פולינום $0 \neq a(x) \in \mathbb{F}[x]$ קיימת $S \subseteq X$ מולטי קבוצה סופית ואיבר $c \in \mathbb{F}$ כך ש

$$a(x) = c \cdot \prod_{p \in S} p$$

פתרון: באינדוקציה על הדרגה של $a(x)$ שנשמנה n . עבור $n = 0$ נקבל כי $a(x) \equiv c \in \mathbb{F}$ ניקח $S = \emptyset$ והטענה מתקיימת. כעת נניח כי הטענה מתקיימת לכל פולינום עד דרגה n (לא כולל) ונוכיח כי הטענה נכונה לכל פולינום מדרגה n .
 אכן יהיה $a(x)$ מדרגה n . אם קיימים b_1, b_2 ממעלה קטנה ממש מ n כך ש $a(x) = b_1(x)b_2(x)$ אזי לפי הנחת האינדוקציה קיימות $S_1, S_2 \subseteq X$ סופית ואיברים $c_1, c_2 \in \mathbb{F}$ כך ש

$$b_1(x) = c_1 \cdot \prod_{p \in S_1} p, \quad b_2(x) = c_2 \cdot \prod_{q \in S_2} q$$

ואז

$$a(x) = b_1 b_2 = c_1 \cdot c_2 \cdot \prod_{q \in S_2} q \prod_{p \in S_1} p$$

נגדיר $S = S_1 \cup S_2$ ו $c = c_1 c_2$ והטענה מתקיימת. אם לא קיימים b_1, b_2 כ"ל אזי $a(x)$ אי פריק ולכן ראשוני ולכן הטענה מתקיימת (ניקח $S = \{p(x)\}$).