

אלגברה ב2

© ארזים

21 במרץ 2017

1 חוגי פולינומים

1.1 חלוקה עם שארית

בשיעור שעבר הגדרנו חוגי פולינומים. ראינו כמה תכונות שלהם, שנעבור עליהן עכשיו: ראשית יש חלוקה עם שארית: לכל f, g קיימים h, r עם $\deg r < \deg g$ המקיימים

$$f = gh + r$$

אפשר להוכיח באינדוקציה, אבל אנחנו מכירים חלוקת פולינומים - אותה שיטה עובדת כאן.

מסקנה 1.1 בחוג $\mathbb{F}[x]$ כל אידאל הוא ראשי (כלומר נוצר על ידי איבר אחד). יתר על כן, יש התאמה חד-חד-ערכית ועל בין אידאלים שאינם 0 לבין פולינומים מתוקנים - כל פולינום כזה ניקח לאידאל שהוא יוצר, וכל אידאל ניקח לפולינום המתוקן מדרגה מינימלית שנמצא בו.

הוכחה: נסמן את ההעתקות שתיארנו:

$$I \xrightarrow{\Psi} f \text{ s.t. } f \in I, (g \in I \Rightarrow \deg f \leq \deg g) \\ f \xrightarrow{\Phi} (f)$$

כך שהטווח של Ψ הוא רק פולינומים מתוקנים. נוכיח שאלה הן הופכיות. נראה ראשית כי $\Psi \circ \Phi(f) = f$ לכל f מתוקן.

נרצה להראות למעשה כי אם $g \in (f)$ מתוקן, $\deg g \leq \deg f$, אזי $g = f$. אכן, אם $g \in (f)$ אזי $g = fh$. לכן $\deg f \geq \deg g = \deg f + \deg h$. נובע כי $\deg h = 0$, כלומר $g = cf$, כאשר c קבוע. f, g שניהם מתוקנים, לכן $c = 1$.

נותר להראות כי $\Phi \circ \Psi(I) = I$ לכל אידאל $I \neq 0$. יהי $f = \Psi(I)$. אזי $f \in I$ מתוקן מדרגה מינימלית. כעת, $\Phi(f) = (f)$. בבירור, $(f) \subseteq I$. אם נוכיח את ההכלה השנייה, נסיים.

יהי $g \in (f)$, ונראה כי $g \in I$, אזי קיימים h, r המקיימים

$$g = fh + r$$

כאשר $\deg r < \deg f$. כעת,

$$r = g - hf \in I$$

מהצד השני, אם $r \neq 0$, אזי על ידי כפל בקבוע, ניתן להניח כי r מתוקן, בסתירה למינימליות הדרגה של f . לכן נובע כי $r = 0$, כלומר $g = fh$, כנדרש. ■

לסיכום קיבלנו שהאידיאלים של $\mathbb{F}[x]$ הם בדיוק 0 וכן (f) , עבור כל f מתוקן.

מסקנה 1.2 בחוג $\mathbb{F}[x]$, קיים מחלק משותף מקסימלי $(\gcd)$, כלומר לכל $f, g \in \mathbb{F}[x]$, שלפחות אחד מהם אינו 0, קיים פולינום d מתוקן כך שמתקיים:

1.

$$d \mid f, d \mid g$$

2. אם $h \mid f, h \mid g$ אזי $h \mid d$.

הוכחה: נתבונן באידאל $(f, g) \subseteq \mathbb{F}[x]$. לפי הטענה הקודמת, קיים d מתוקן המקיים

$$(d) = (f, g)$$

מכאן כמובן שנובע כי $d \mid f, d \mid g$. כעת, אם $h \mid f, h \mid g$, אזי קיימים h_1, h_2 עבורם $d = fh_1 + gh_2$, ונקבל כי $h \mid d$. לכן $d = \gcd(g, f)$. ■

הערה 1.3 ראינו שקיימים h_1, h_2 כך שמתקיים

$$\gcd(f, g) = h_1f + h_2g$$

יתר על כן, קיים אלגוריתם שמוצא את הצירוף הזה (ואת אותו $\gcd$): **אלגוריתם אוקלידס**. בהנתן f, g , נמצא a, b המקיימים

$$af + bg = \gcd(f, g)$$

עובדים כך:

$$f = gh_1 + r_1, \deg r_1 < \deg r_0 \quad (r_0 = g) \quad (1)$$

$$g = r_1h_2 + r_2, \deg r_2 < \deg r_1 \quad (2)$$

$$\vdots \quad (3)$$

$$r_{n-2} = r_{n-1}h_n + r_n, \deg r_n < \deg r_{n-1} \quad (4)$$

$$r_{n-1} = r_nh_{n+1} + 0, r_{n+1} = 0 \quad (5)$$

טענה 1.4 $r_n = \gcd(f, g)$ וכן

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1}h_n = r_{n-2} - (r_{n-3} - r_{n-2}h_{n-1}) = \dots = \\ &= af + bg \end{aligned}$$

הוכחה: שורה 5 אומרת $r_n \mid r_{n-1}$ שורה 4 $r_n \mid r_{n-2}$ כך ממשיכים, עד שמגיעים לכך שלפי שורה 2, $r \mid g$, ולפי שורה 1, $r \mid f$. לכן הוא מחלק משותף. בבירור הוא מקסימלי, כי $r_n = af + bg$. ■

1.2 פירוק פולינומים

הגדרה 1.5 פולינום $f \in \mathbb{F}[x]$ ייקרא פריק אם קיימים g, h ממעלה חיובית המקיימים $gh = f$.

פולינום ממעלה חיובית שאינו פריק נקרא אי-פריק. פולינום ממעלה 0 נקרא הפיך.

"ופולינום האפס נקרא - פולינום האפס. הנה, יש לנו שמות לכל הפולינום, לפי איך הם מתפרקים" - המרצה.

משפט 1.6 (המשפט הקטן של בזו) יהי $f \in \mathbb{F}[x]$, ויהי $\alpha \in \mathbb{F}$. אם $f(\alpha) = 0$ אזי קיים פולינום g כך שמתקיים

$$f(x) = (x - \alpha)g(x)$$

בפרט, אם $\deg f \geq 2$, וקיים שורש של f בשדה, אזי f פריק.

הוכחה: נכתוב

$$f(x) = (x - \alpha)g(x) + r(x)$$

כאשר $\deg r < 1$, כלומר r קבוע. נציב ונקבל

$$0 = f(\alpha) = (\alpha - \alpha)g(\alpha) + r = r$$

■

$$f(x) = (x - \alpha)g(x)$$

דוגמא האם הפולינום $x^6 - x^5 - 2x + 2$ אי פריק מעל $\mathbb{Q}$? לא, כי 1 שורש.

טענה 1.7 אם $f(x) \in \mathbb{Q}[x]$ פולינום שכל המקדמים שלו שלמים (אפשר להניח על ידי כפל במכנה משותף), וכן $\frac{p}{q} \in \mathbb{Q}$ שבר מצומצם המקיים $f\left(\frac{p}{q}\right) = 0$, אזי $a_n \mid p$, $a_0 \mid q$. בפרט יש כמות סופית של אפשרויות לשורשים.

הוכחה: ידוע כי

$$\sum_{i=0}^n a_{n-i} \frac{p^i}{q^i} = 0$$

נכפיל הכל פי q^n :

$$\sum_{i=0}^n a_{n-i} p^i q^{n-i} = 0$$

נעביר אגפים ונקבל

$$\sum_{i=1}^n a_{n-i} p^i q^{n-i} = -a_n q^n$$

p מחלק את אגף שמאל, ולכן $a_n q^n \mid p$, אבל $\frac{p}{q}$ מצומצם, כלומר p, q זרים, ולכן $a_n \mid p$.
 באופן דומה, $a_0 \mid q$. ■

מסקנה 1.8 אם f פולינום מתוקן מעל $\mathbb{Q}$ שכל המקדמים שלו שלמים, אזי כל השורשים הרציונאליים שלו הם שלמים.

קיימת הכללה נרחבת:

משפט 1.9 (הלמה של גאוס) אם $f \in \mathbb{Q}[x]$ עם מקדמים שלמים, וכן $f(x) = g(x)h(x)$ כך שהפולינומים $g, h \in \mathbb{Q}[x]$ מתוקנים, אזי כל המקדמים של g, h שלמים. המסקנה הקודמת היא המקרה בו $\deg g = 1$.