

חוג הפולינומים

יהי F שדה. חוג הפולינומים $F[x]$ מתנהג, מבחינות רבות, כמו חוג המספרים השלמים \mathbb{Z} . בדף זה נתייחס לנושאים הבאים: חילוק עם שארית, מחלק משותף מרבי, אלגוריתם אוקלידס, פולינום אי-פריק, שדות סופיים.

חילוק עם שארית

תזכורת: המעלה של פולינום $a(x) = \sum_{i=0}^n a_i x^i \in F[x]$ מוגדרת על-ידי:
 $\deg a(x) := \max\{i \mid a_i \neq 0\}$.

עבור $a(x) = 0$ (פולינום האפס) נגדיר $\deg(0) := -\infty$ (לעתים אומרים ש- $\deg(0)$ פשוט לא מוגדר).

משפט: יהיו $a(x), b(x) \in F[x]$, $b(x) \neq 0$. אזי קיימים פולינומים $q(x), r(x) \in F[x]$ המקיימים:

$$a(x) = b(x) \cdot q(x) + r(x), \quad \deg r(x) < \deg b(x)$$

(כולל האפשרות $r(x) = 0$). המנה $q(x)$ והשארית $r(x)$ מוגדרים באופן יחיד ע"י התנאים הנ"ל.

אם $r(x) = 0$ נאמר ש- $b(x)$ מחלק את $a(x)$ (בלי שארית), ונרשום: $b(x) \mid a(x)$.

דוגמא:

$$a(x) = x^3 + 2x^2 + 3, \quad b(x) = 2x^2 + 2x + 1 \in \mathbf{R}[x]$$

ביצוע בפועל של חילוק עם שארית הוא על-ידי "חילוק ארוך", כמו במספרים שלמים. כאן:

$$\begin{array}{r} \frac{1}{2}x + 1 \\ \hline x^3 + 3x^2 + 0x + 3 \quad | \quad 2x^2 + 2x + 1 \\ - (x^3 + x^2 + \frac{1}{2}x) \\ \hline 2x^2 - \frac{1}{2}x + 3 \\ - (2x^2 + 2x + 1) \\ \hline -\frac{5}{2}x + 2 \end{array}$$

ולכן

$$x^3 + 2x^2 + 3 = (2x^2 + 2x + 1) \cdot (\frac{1}{2}x + 1) + (-\frac{5}{2}x + 2)$$

כאשר

$$q(x) = \frac{1}{2}x + 1, \quad r(x) = -\frac{5}{2}x + 2 \in \mathbf{R}[x]$$

$$1 = \deg r(x) < \deg b(x) = 2$$

מחלק משותף מרבי

עבור $a(x), b(x) \in F[x]$, מחלק משותף הוא פולינום $d(x) \in F[x]$ המקיים:
 $d(x) | a(x)$, $d(x) | b(x)$.

תזכורת: פולינום $a(x) = \sum_{i=0}^n a_i x^i \in F[x]$ ממעלה $n \geq 0$ נקרא מתוקן אם המקדם של חזקת x הגבוהה ביותר בו הוא: $a_n = 1$.

המחלק המשותף המרבי (ממ"מ) ($\gcd = \text{greatest common divisor}$) של שני פולינומים $a(x), b(x) \in F[x]$ הוא מחלק משותף שלהם שהוא פולינום מתוקן ממעלה גדולה ביותר. מסמנים: $\gcd(a(x), b(x))$.

ניתן להראות שמחלק משותף ממעלה גדולה ביותר של שני פולינומים, שלפחות אחד מהם אינו פולינום האפס, קיים וגם יחיד עד כדי כפל בקבוע $0 \neq c \in F$. כדי להגדירו באופן יחיד, דורשים שהמחלק המשותף יהיה מתוקן. $\gcd(0, 0)$ אינו מוגדר.

שיטה מעשית לחישוב $\gcd(a(x), b(x))$ היא שימוש באלגוריתם אוקלידס.

אלגוריתם אוקלידס

יהיו $a(x), b(x) \in F[x]$. נניח: $b(x) \neq 0$.
 נגדיר:

$$r_1(x) := a(x), \quad r_2(x) := b(x).$$

נחלק עם שארית את $r_1(x)$ ב- $r_2(x)$:

$$r_1(x) = r_2(x) \cdot q_3(x) + r_3(x), \quad \deg r_3(x) < \deg r_2(x)$$

ונמשיך כך:

$$r_k(x) = r_{k+1}(x) \cdot q_{k+2}(x) + r_{k+2}(x), \quad \deg r_{k+2}(x) < \deg r_{k+1}(x) \quad (k = 2, 3, \dots)$$

נעצור כאשר נקבל לראשונה שארית $r_{k+1}(x) = 0$.

משפט:

א. אלגוריתם אוקלידס תמיד עוצר.

ב. עד כדי כפל בקבוע, $\gcd(a(x), b(x)) = r_k(x)$ (השארית האחרונה שאינה מתאפסת).

ג. קיימים $s(x), t(x) \in F[x]$ כך ש-:

$$\gcd(a(x), b(x)) = a(x) \cdot s(x) + b(x) \cdot t(x)$$

ההוכחה דומה להוכחת המשפט המקביל עבור אלגוריתם אוקלידס בחוג השלמים, ולא תפורט כאן.

פולינומים אי-פריקים ושדות סופיים

נמשיך את האנלוגיה בין חוג המספרים השלמים \mathbb{Z} לבין חוג הפולינומים מעל שדה $F[x]$.

תזכורת: לכל $n \geq 2$ שלם ניתן להגדיר את החוג \mathbb{Z}_n , שאבריו הם מחלקות השקילות עבור יחס השקילות (על \mathbb{Z}) "שוויון מודולו n ":

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$$

כל מחלקת שקילות \bar{a} ניתנת לייצוג (יחיד) על-ידי שארית מודולו n : $\bar{a} = \bar{r}$: n ($0 \leq r < n$).

ב- \mathbb{Z}_n מוגדרות פעולות (חיבור וכפל מודולו n), ההופכות אותו לחוג קומוטטיבי עם יחידה. למשל, ב- \mathbb{Z}_6 :

$$\bar{2} + \bar{5} = \bar{7} = \bar{1}$$

$$\bar{2} \cdot \bar{5} = \bar{10} = \bar{4}$$

אם $a \in \mathbb{Z}$ כלשהו, אז: $\bar{a} \in \mathbb{Z}_n \Leftrightarrow \gcd(a, n) = 1$ הפיך

ואת ההפכי ניתן למצוא בעזרת אלגוריתם אוקלידס.

בפרט, \mathbb{Z}_n הוא שדה (כל איבר שונה מאפס הוא הפיך) אם ורק אם $n \geq 2$ הוא מספר ראשוני, ז"א: אין ל- n מחלקים טבעיים פרט ל- n עצמו ול-1; או בניסוח שקול: $n = n_1 \cdot n_2$ עבור n_2, n_1 טבעיים גורר $n_1 = 1$ או $n_2 = 1$.

נעבור עתה לחוג הפולינומים מעל שדה.

לכל פולינום $p(x) \in F[x]$ שאינו קבוע ($\deg p(x) > 0$) ניתן להגדיר את החוג $F[x]/(p(x))$, שאבריו הם מחלקות השקילות עבור יחס השקילות (על $F[x]$) "שוויון מודולו $p(x)$ ":

$$a(x) \equiv b(x) \pmod{p(x)} \Leftrightarrow p(x) \mid (a(x) - b(x))$$

דוגמא: כל איבר בחוג $\mathbb{R}[x]/(x^2-x+1)$ אפשר לכתוב בצורה $\bar{r(x)}$ כאשר $\deg r(x) < \deg(x^2-x+1) = 2$, ז"א: $r(x) = r_1x + r_0$. למשל:

$$\overline{2x^2} = \overline{2(x^2-x+1) + 2x-2} = \overline{2x-2}$$

ב- $F[x]/(p(x))$ מוגדרות פעולות (חיבור וכפל מודולו $p(x)$), ההופכות אותו לחוג קומוטטיבי עם יחידה. לדוגמא, בחוג $\mathbb{R}[x]/(x^2-x+1)$:

$$\overline{x+2} \cdot \overline{x+3} = \overline{(x+2) \cdot (x+3)} = \overline{x^2+5x+6} = \overline{(x^2-x+1) + (6x+5)} = \overline{6x+5}$$

פולינום $p(x) \in F[x]$ שאינו קבוע ($\deg p(x) > 0$) נקרא ראשוני (או אי-פריק) אם אין לו מחלקים לא טריביאליים, ז"א: אם השוויון $p(x) = p_1(x) \cdot p_2(x)$ (מכפלת פולינומים) גורר $\deg p_1(x) = 0$ או $\deg p_2(x) = 0$. אם $p(x), a(x) \in F[x]$ לא קבוע, אז:

$$\overline{a(x)} \in F[x]/(p(x)) \Leftrightarrow \gcd(a(x), p(x)) = 1$$
 הפיך

את ההפכי ניתן למצוא בעזרת אלגוריתם אוקלידס למציאת gcd : נרשום (ב- $F[x]$)
 $1 = \gcd(a(x), p(x)) = a(x) \cdot s(x) + p(x) \cdot t(x)$

ואז, ב- $F[x]/(p(x))$:

$$\bar{1} = \overline{a(x) \cdot s(x) + p(x) \cdot t(x)} = \overline{a(x) \cdot s(x)} + \overline{0 \cdot t(x)} = \overline{a(x) \cdot s(x)}$$

בפרט, $F[x]/(p(x))$ הוא שדה אם ורק אם $p(x) \in F[x]$ הוא פולינום ראשוני (אי-פריק).

אם F הוא שדה סופי (ז"א: מספר אבריו סופי), אז גם $F[x]/(p(x))$ חוג סופי. מספר אבריו :

$$\left| F[x]/(p(x)) \right| = |F[x]|^{\deg p(x)}$$

דוגמא: נגדיר שדה עם 9 אברים. תחילה נסמן

$$F := \mathbf{Z}_3 = \{0, 1, 2\}$$

למען הפשטות, רשמנו כאן את אברי \mathbf{Z}_3 בתור 2, 1, 0 במקום $\bar{2}, \bar{1}, \bar{0}$. נבחר :

$$p(x) := x^2 + 1 \in \mathbf{Z}_3[x]$$

אפשר להוכיח שהפולינום $p(x)$ הוא אי-פריק: אי-אפשר לכתוב אותו כמכפלת שני פולינומים (מתוקנים) ממעלה ראשונה $(x-a)(x-b)$, כי אין ל- $p(x)$ שורשים ב- \mathbf{Z}_3 .

לכן $F[x]/(p(x)) = \mathbf{Z}_3[x]/(x^2+1)$ הוא שדה בעל 9 אברים :

$$F_9 := \mathbf{Z}_3[x]/(x^2+1) = \left\{ \overline{r(x)} \mid \deg r(x) < 2 \right\} = \left\{ \overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2} \right\}$$

למשל :

$$\overline{x+x+1} = \overline{2x+1} = \bar{1}$$

$$\overline{x+1 \cdot x+2} = \overline{x^2+2} = \overline{(x^2+1)+1} = \bar{1}$$

ולכן $\overline{x+2}$ הוא ההפכי של $\overline{x+1}$ ולהיפך.

ניתן להראות שיש פולינום אי-פריק (אחד לפחות) מכל מעלה מעל כל שדה. בשיטה זו ניתן לקבל שדות סופיים שמספר אבריהם הוא חזקת ראשוני כלשהי :

$$2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, \dots$$

מודגשות כאן החזקות שאינן פשוט מספרים ראשוניים, כיוון שהראשוניים כבר מוכרים לנו כמספרי האברים של שדות מהצורה הפשוטה \mathbf{Z}_p .

לסיים: ניתן להראות שפולינומים אי-פריקים שונים, מאותה מעלה מעל אותו שדה סופי, נותנים בשיטה הנ"ל בעצם אותו שדה; ליתר דיוק: שדות "איזומורפיים" – בעלי פעולות (חיבור וכפל) זהות, אחרי סימון מחדש של האברים. כמו כן, כל שדה סופי מתקבל (ליתר דיוק: "איזומורפיים" לשדה המתקבל) בשיטה הנ"ל. אם כן, יש בידינו שיטה לייצר את כל השדות הסופיים האפשריים. בפרט, אין שדה סופי שמספר אבריו הוא 6, או כל מספר לא-ראשוני אחר.