פולינומים

אלגברה מודרנית ח' (עודכן ב - 17.6.01)

דף זה מרכז את המבוא הקשור לנושא הפולינומים. אנא, קיראו אותו היטב ודאגו להבין את התיאוריה ואת הטכניקה.

א הגדרות

<u>הגדרה:</u>

יהי K שדה (אנו נעסוק בעיקר ב: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ וב - $\mathbb{Z}_p$ עבור p ראשוני). <u>פולינום</u> מעל לשדה K הוא ביטוי מן הצורה:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

כאשר $a_0, a_1, \ldots, a_n \in K$.

<u>הגדרה:</u>

אם $p(x)$ פולינום מן הצורה:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

ו - n הוא השלם הגדול ביותר כך ש: $a_n \neq 0$, נאמר כי: <u>מעלת הפולינום</u> $p(x)$ היא n, ונסמן:

$$deg\left(p(x)\right) = n$$

מעלת הפולינום היא מעין קריטריון ל"גודל" הפולינום, בדומה לגודל המספר בשלמים. מעלת פולינומים תאפשר לנו "השוואה" בין פולינומים במובן שיוסבר בהמשך.

<u>דוגמא:</u>

1. $p_1(x) = 3x^2 + \sqrt{2}x + 5$

   הינו פולינום ממעלה 2 מעל הממשיים (וגם מעל המרוכבים).

2. $p_2(x) = 8x^7 + ix^3 - 2$

   הינו פולינום ממעלה 7 מעל המרוכבים

<u>הערות:</u>

- כש - $deg\left(p(x)\right) = 0$, אזי $p(x)$ הינו פולינום קבוע, ז"א: $p(x) = c$.
- $p(x) = 0$ (פולינום האפס) אם"ם $a_i = 0$ לכל $i \in \mathbb{Z}$. מעלת פולינום זה אינה מוגדרת!

ב פעולות על פולינומים

בסעיף זה, נבחין כיצד מבצעים פעולות בסיסיות בין פולינומים. נעבוד עם שני פולינומים, אשר יסומנו:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

בלי הגבלת הכלליות, נניח כי: $m \geq n$ ונניח כי: $b_j = 0$ עבור: $j = m+1, \ldots, n$.

חיבור וחיסור פולינומים

תוצאת החיבור (או החיסור) של שני הפולינומים הנ"ל מוגדרת להיות הפולינום הבא:

$$p(x) \pm q(x) = (a_n \pm b_n)\, x^n + (a_{n-1} \pm b_{n-1})\, x^{n-1} + \cdots + (a_1 \pm b_1)\, x + (a_0 \pm b_0)$$

הערות:

- נשים לב כי אם: $p(x) \pm q(x) \neq 0$, אזי מתקיים: $deg\,(p(x) + q(x)) \leq max\,\{deg\,(p(x))\,, deg\,(q(x))\}$
- פעולת ה"חיבור" (או ה"חיסור) בין אברי a_i, b_i היא הפעולה המוגדרת בשדה מעליו אנו עובדים.

דוגמא: $\left(2x^5 + x^2 + 3x - 5\right) - \left(x^4 + x^2 - 8\right) = 2x^5 - x^4 + 3x + 3$

כפל פולינומים

תוצאת הכפל של שני הפולינומים הנ"ל מוגדרת להיות הפולינום הבא:

$$p(x) \cdot q(x) = c_{n+m} x^{n+m} + c_{n+m-1} x^{n+m-1} + \cdots + c_1 x + c_0$$

כאשר המקדמים c_i הם:

$$c_i = \sum_{k=0}^{i} a_k b_{i-k}$$

הערות:

- נשים לב כי מתקיים: $deg\,(p(x) \cdot q(x)) = deg\,(p(x)) + deg\,(q(x))$
- פעולות ה"כפל" וה"חיבור" בין אברי a_i, b_i הן הפעולה המוגדרת בשדה מעליו אנו עובדים.

דוגמא: $\left(x^2 - 5\right) \cdot (x + 2) = x^3 + 2x^2 - 5x - 10$

חלוקת פולינומים

בדומה לתהליך החלוקה בשלמים, גם כאן נוכיח (בכיתה) טענה יסודית וחשובה מאוד, אשר תהווה מרכיב מרכזי בחומר שלנו:

<u>טענה:</u>

יהיו $p(x), g(x) \neq 0$ שני פולינומים מעל השדה K, אזי קיימים פולינומים $q(x), r(x)$ כך ש:

$$p(x) = q(x) \cdot g(x) + r(x)$$

כאשר: $deg\,(r(x)) < deg\,(g(x))$ או ש: $r(x) = 0$. אם $r(x) = 0$, נאמר ש: $g(x)$ מחלק את $p(x)$, ונסמן: $g(x)\big|p(x)$

בהקבלה לתהליך החלוקה בשלמים, אנו צריכים להבין כי $r(x)$ הוא שארית החלוקה של $p(x)$ ב - $g(x)$, ואפשר להתייחס אליו - אם כי זה מעט מוקדם לכך - באופן הבא: $p(x) \equiv r(x)\ (mod\ g(x))$.

חלקכם מכירים את תהליך החלוקה מקורסים קודמים (אלגברה 1/מ'), אך חלקכם לא ראיתם חלוקת פולינומים עד כה. נתאר כאן את תהליך החלוקה בקצרה, ולאחר מכן בעזרת דוגמא מפורטת.

תהליך החלוקה בפולינומים דומה לתהליך החלוקה של מספרים שלמים. כדי להתקדם משלב אחד לבא אחריו - עלינו להוריד את מעלת הפולינום אותו אנו מחלקים. בכל שלב, נחלק את המעלה הגבוהה של הפולינום אשר קיבלנו במעלה הגבוהה של הפולינום בו אנו מחלקים, נכפיל את התוצאה ב<u>כל</u> הפולינום בו אנו מחלקים, ונחסר מן הפולינום אותו חילקנו. נשמע מסובך?! הדוגמא הבאה תבהיר את הכל.

<u>דוגמאות:</u>

1. ניקח שני פולינומים:

$$p(x) = x^5 + x^4 - 2x^3 + 2x^2 + 5x + 5,\ \ g(x) = x^2 + x + 1$$

ונמצא את הפולינומים $q(x), r(x)$ מן הטענה. תהליך החילוק מתבצע כך:

$$\begin{array}{l|l}
x^3 - 3x + 5 & \\
\hline
x^5 + x^4 - 2x^3 + 2x^2 + 5x + 5 & x^2 + x + 1 \\
x^5 + x^4 + x^3 & \\
\hline
\qquad -3x^3 + 2x^2 + 5x + 5 & \\
\qquad -3x^3 - 3x^2 - 3x & \\
\hline
\qquad\qquad 5x^2 + 8x + 5 & \\
\qquad\qquad 5x^2 + 5x + 5 & \\
\hline
\qquad\qquad\quad 3x &
\end{array}$$

עצרנו את התהליך, כאשר קיבלנו שמעלת $r(x)$ קטנה ממעלת $g(x)$. ז"א, קיבלנו ש:

$$p(x) = \overbrace{\left(x^3 - 3x + 5\right)}^{q(x)} \cdot g(x) + \overbrace{3x}^{r(x)}$$

2. כעת, נתבונן בתהליך החלוקה של $p(x)$ ב - $g(x)$ עבור:

$$p(x) = 5x^4 + 3x^3 + x^2 + 2x - 1,\ g(x) = x + 1$$

נקבל:

$$\begin{array}{r|l}
\multicolumn{1}{l}{5x^3 - 2x^2 + 3x - 1} & \\
\cline{1-1}
5x^4 + 3x^3 + x^2 + 2x - 1 & \quad x+1 \\
5x^4 + 5x^3 & \\
\hline
-2x^3 + x^2 + 2x - 1 & \\
-2x^3 - 2x^2 & \\
\hline
3x^2 + 2x - 1 & \\
3x^2 + 3x & \\
\hline
-x - 1 & \\
-x - 1 & \\
\hline
0 &
\end{array}$$

כאן, עצרנו כאשר השארית היא 0, ולכן:

$$g(x) \big| p(x)$$

ג שורשים של פולינומים

בסעיף זה מרוכזות כמה תוצאות חשובות בקשר לשורשים של פולינומים. באופן כללי, מציאת שורשים של פולינום היא משימה קשה ומורכבת ואנו נטפל בה במקרים מיוחדים. מציאת שורשים של פולינומים, תסייע לנו בקביעת הפריקות של פולינומים - נושא חשוב שנעסוק בו בהמשך.

<u>הגדרה:</u>

יהי $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0$ פולינום. מספר c נקרא <u>שורש</u> של $p(x)$ אם הוא מקיים:

$$p(c) = 0$$

כלומר:

$$a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0 = 0$$

<u>דוגמאות:</u>

1. לפולינום: $p(x) = 3x^4 - 2x^2 - 1$ מעל $\mathbb{R}$ יש שורש: $x = 1$, כיוון ש: $p(1) = 0$.
2. לפולינום: $q(x) = x^2 + x + 1$ מעל $\mathbb{Z}_2$ אין שורש, כיוון ש:

$$q(0) = q(1) = 1$$

משפט (המשפט היסודי של האלגברה):

יהי $p(x)$ פולינום ממעלה $n \geq 1$ מעל לשדה $\mathbb{C}$, אזי $p(x)$ ניתן לכתיבה באופן יחיד (עד כדי סדר הגורמים) בצורה הבאה:

$$p(x) = k \cdot (x - x_1)(x - x_2) \cdots (x - x_n)$$

כאשר: $k \in \mathbb{C}$ ו - x_i הם שורשי הפולינום $p(x)$.

דוגמאות:

1. $q_1(x) = 2x^2 + 4x + 2 = 2(x+1)(x+1)$
2. $q_2(x) = x^2 - 1 = (x+1)(x-1)$

הערות:

- הריבוי של שורש x_i, הוא מספר הפעמים אשר x_i מופיע בפירוק מלמעלה.
- ידוע ש: x_i הוא שורש מריבוי k אם"ם:

$$p(x_i) = \cdots p^{(k-1)}(x_i) = 0, \quad p^k(x_i) \neq 0$$

כאשר: $p^{(m)}$ מציין את הנגזרת ה - m-ית של $p(x)$.

משפט:

יהי $p(x)$ פולינום שמקדמיו ממשיים, אזי השורשים הלא ממשיים של $p(x)$ מופיעים בזוגות של צמודים - כלומר, אם z הוא שורש, גם $\overline{z}$ הוא שורש.

משפט (הניחוש האינטיליגנטי):

יהי $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ פולינום ב - $\mathbb{Z}[x]$. אם יש ל - $p(x)$ שורש רציונלי מצורת: $\frac{p}{q}$, אזי:

$$p \big| a_0, \quad q \big| a_n$$

דוגמאות:

1. נניח, כי נתון הפולינום: $p_1(x) = 2x^4 + 5x^3 + 3x^2 - 3x$. ראשית, נוציא את x כגורם משותף, ונקבל: $p_1(x) = x\left(2x^3 + 5x^2 + 3x - 3\right)$. לכן, שורש אחד הוא: $x_1 = 0$. נחפש שורש לפולינום שבתוך הסוגריים - נסמנו ב: p. אם לפולינום זה שורש רציונלי מצורת: $\frac{p}{q}$, אזי: $p|3, \quad q|2$, ולכן: $p = \pm 1, \pm 3$ ו - $q = \pm 1, \pm 2$. נותר לנו רק לבדוק את הצירופים האפשריים של p, q ולמצוא האם אחד מהם הוא שורש. שימו לב: מספיק לקחת את p עם סימנים מתחלפים ואת q עם סימן קבוע! נבדוק ונמצא ש: $p\left(\frac{1}{2}\right) = 0$ ולכן $\frac{1}{2}$ הוא שורש של הפולינום.

2. $p_2(x)=x^6+x^4+x^2+x-1$. אם לפולינום זה שורש רציונלי, הרי שלפי משפט הניחוש האינטיליגנטי, הוא חייב להיות ± 1. אבל:

$$p_2(1)=3,\ \ p_2(-1)=1$$

ולכן, אין לפולינום זה שורשים רציונליים.

ד פריקות פולינומים

הגדרה:

יהי $p(x)$ פולינום ממעלה n מעל K. $p(x)$ נקרא פריק מעל K אם קיימים $h(x),g(x)$ - פולינומים מעל K, כך ש:

$$p(x)=h(x)\cdot g(x)$$

ו: $n >$ מעלותיהם של $h(x),g(x) \geq 1$.

$p(x)$ נקרא אי-פריק מעל K אם הוא אינו פריק מעל K.

משפט:

יהי $p(x)$ פולינום מעל $\mathbb{R}$, אזי $p(x)$ ניתן לפירוק יחיד (עד כדי סדר הגורמים) בצורה הבאה:

$$p(x)=\alpha\cdot h_1(x)h_2(x)\cdots h_k(x)$$

כאשר $h_i,\ i=1,\ldots,k$ הם פולינומים אי-פריקים ומתוקנים ממעלה 1 או 2 ו - α קבוע.

דוגמאות:

1. נתבונן בפולינום $p(x)=x^2+1$. פולינום זה אינו פריק מעל $\mathbb{R}$, כיוון שאין לו שורש ממשי. אבל, $p(x)$ פריק מעל $\mathbb{C}$ כיוון ש:

$$p(x)=x^2+1=\underbrace{(x+i)}_{\text{מעלה } 1}\underbrace{(x-i)}_{\text{מעלה } 1}$$

2. הפולינום: $q(x)=x^3-x^2+x-1$ הינו פריק מעל $\mathbb{Q}$, כיוון ש:

$$q(x)=(x^2+1)(x-1)$$

ולכן, הוא גם פריק מעל $\mathbb{R}$ ומעל $\mathbb{C}$