אלגברה ב2

ארזים ©

21 במרץ 2017

1 חוגי פולינומים

הגדרה 1.1 יהי R חוג. נסמן בתור $R[x]$ את חוג הפולינומים מעל R במשתנה יחיד x.

$$R[x] = \left\{ \sum_{i=0}^{N} a_i x^i \mid a_i \in R \right\}$$

אם R אינו תחום שלמות, נאבד את התכונה שמעלת מכפלה היא סכום המעלות.

הגדרה 1.2 פולינום $f \in R[x]$ ייקרא <u>אי־פריק</u> אם $\deg f \geq 1$ ולכל פירוק $f = gh$ כאשר $g, h \in R[x]$ מתקיים $\deg(g) = 0$ או $\deg(h) = 0$.

מעתה נניח לפחות כי R תחום שלמות (אין מחלקי 0). כאשר בנוסף R הוא שדה, יש חלוקה עם שארית: לכל שני פולינומים $f, g \in R[x]$, כאשר $g \neq 0$, קיימים ויחידים $q, r \in R[x]$, כאשר $\deg r < \deg g$ וכן

$$f = qg + r$$

כעת, יהי F שדה. אזי $F[x]$ הוא <u>תחום ראשי</u> - כלומר תחום שלמות שבו כל אידאל הוא ראשי (נוצר על ידי איבר יחיד).

דוגמא כדוגמא נגדית, האידאל $\{2f(x) + xg(x) \mid f, g \in \mathbb{Z}[x]\} = (2, x)$ אינו ראשי בתוך $\mathbb{Z}[x]$.

נובע מתכונת הראשיות כי יש בחוג $F[x]$ פריקות יחידה: לכל פולינום f ממעלה שהיא לפחות 1 קיימים פולינומים אי פריקים $f_1, \ldots, f_k \in F[x]$ מתוקנים וסקלר $c \in F$ כך שמתקיים

$$f = c \cdot f_1 \cdot \cdots \cdot f_k$$

והפירוק הזה יחיד עד כדי שינוי סדר הגורמים.

דוגמא לתחום פריקות יחידה שאינו תחום ראשי:

$$\mathbb{C}[x, y] = \mathbb{C}[x][y]$$

האידאל (x, y) לא נוצר על ידי אף איבר. גם החוג $\mathbb{Z}[x]$ הוא תחום פריקות יחידה.

סיסמא שכדאי לשמור בראש:

"פירוק בחוג $\mathbb{Z}[x]$ שקול לפירוק בשדה $\mathbb{Q}[x]$".

תרגיל האם x^3-2x^2+5x-2 פריק? יש לציין באיזה חוג. נבדוק בחוגים $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$.

פתרון מעל שדה, בגלל שהפולינום ממעלה 3, אי פריקות שקולה לחוסר קיום שורשים. לפי קריטריון השורש הרציונאלי שראינו בהרצאה, $f\left(\frac{p}{q}\right)=0$ יגרור $p\mid -2, q\mid 1$, כלומר $\frac{p}{q}=\pm1,\pm2$. אם מציבים, רואים שאלה לא שורשים, ולכן מעל $\mathbb{Q}[x]$ - הפולינום אי פריק.
מעל $\mathbb{R}[x]$, משום שהפולינום ממעלה אי זוגית, קיים לו שורש ממשי. לכן הוא פריק.
בחוג $\mathbb{Z}[x]$, f אי פריק גם כן - פירוק בחוג $\mathbb{Z}[x]$ היה פירוק בחוג $\mathbb{Q}[x]$.

תרגיל האם x^4+1 פריק בחוג $\mathbb{R}[x],\mathbb{Q}[x]$?

פתרון מעל הממשיים, כל הפולינומים האי פריקים הם ממעלה 1 או 2. נראה זאת במקרה הפרטי שלנו: ניקח $\alpha=\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$, שהוא שורש של הפולינום. ברור כי גם $\overline{\alpha}=\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i$ הוא פתרון. כעת, מתקיים

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

וברור שפולינום זה מחלק את הפולינום שלנו, והוא במקדמים ממשיים. לכן הפולינום שלנו פריק מעל $\mathbb{R}$. בדומה $\beta=-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$ שורש, ונקבל דרכו את הגורם האי פריק

$$(x-\beta)\left(x-\overline{\beta}\right)=x^2+\sqrt{2}x+1$$

נקבל כי

$$x^4+1=\left(x^2-\sqrt{2}x+1\right)\left(x^2+\sqrt{2}x+1\right)$$

הפירוק מעל $\mathbb{R}$.
מעל $\mathbb{Q}$, נניח בשלילה שהיה פירוק למכפלת פולינומים מתוקנים (כי הפולינום המקורי מתוקן). נובע מיחידות הפירוק שזהו אותו פירוק שמצאנו לפני רגע, כי הוא פירוק גם מעל $\mathbb{R}$, אבל זו סתירה, כי $\sqrt{2}\notin\mathbb{Q}$.

משפט 1.3 (קריטריון איזנשטיין) יהי

$$f(x)=\sum_{i=0}^{n}a_ix^i$$

פולינום עם מקדמים שלמים, כך שקיים ראשוני p עבורו $p\mid a_i$ לכל $1\le i\le n-1$, $p\nmid a_n$ וכן $p^2\nmid a_0$. אזי f אי פריק בחוג $\mathbb{Z}[x]$ (ולכן גם בחוג $\mathbb{Q}[x]$).

דוגמא $3x^4+30x^2+10$ אי פריק, אם ניקח בקריטריון $p=2$, או $p=5$.

הערה 1.4 ההעתקה

$$f\left(x\right)\mapsto f\left(ax+b\right)$$

כאשר $a\in F^*$, $b\in F$ עבור F שדה, היא אוטומורפיזם של החוג $F\left[x\right]$ (איזומורפיזם מהחוג לעצמו).

לכן $f\left(x\right)$ אי פריק אם ורק אם $f\left(ax+b\right)$ אי פריק.

דוגמא הפולינום $x^4+x^3+x^2+x+1$ ניתן להוכיח אי פריקות על ידי בחירת $a=1,b=1$ וקריטריון איזנשטיין עם $p=5$. נשים לב שמתקיים

$$x^4+x^3+x^2+x+1=\frac{x^5-1}{x-1}$$

ובאותה צורה, כל פולינום מהצורה

$$\sum_{i=0}^{p-1}x^i$$

כאשר p ראשוני הוא אי פריק, מאותה בחירה, עם p בקריטריון איזנשטיין.