

אלגברה ב' 2 – תרגול 3

07.03.11

פולינומים סימטריים

A חוג חילופי עם יחידה, $R = A[x_1, \dots, x_n]$, $f(x_1, \dots, x_n) \in R$ ייקרא סימטרי אם $f(x_1, \dots, x_n) = f(\sigma(x_1), \dots, \sigma(x_n))$.
לדוגמא הפולינומים הסימטריים היסודיים:

$$S_k = \sum_{i_1 < \dots < i_k} \prod_{j=1}^k x_{i_j} \quad 1 \leq k \leq n$$

סכומי החזקות: $P_k = \sum_{i=1}^n x_i^k$ ל- $k \geq 1$, $P_0 = n$. למשל $P_1 = S_1$.

$$S_1^2 = \left(\sum_{i=1}^n x_i\right)^2 = \sum_{i=1}^n x_i^2 + 2 \sum_{i < j} x_i x_j = P_2 + 2S_2$$

הגדרה. יהי $f \in F[x]$ ויהי $F \subseteq K$ שדה ההרחבה כך ש- $x_1, \dots, x_n \in K$ הם כל השורשים של f עם ריבוי $(K$ מוכל בסגור האלגברי של $F)$.

$$D(f) = \prod_{i < j} (x_i - x_j)^2$$

הדיסקרימיננט של f .

ההגדרה טובה: $D(f)$ הוא פולינום סימטרי ב- $x_1, \dots, x_n$, לכן ניתן להצגה ע"י $S_1, \dots, S_n$, אלה מופיעים כמקדמים של f ולכן נמצאים ב- F . זה לא תלוי בשדה ההרחבה K .
נגדיר

$$\Delta = \det \begin{pmatrix} 1 & \dots & 1 \\ x_1 & \dots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \dots & x_n^{n-1} \end{pmatrix} = (-1)^{\frac{n(n-1)}{2}} \prod_{i < j} (x_i - x_j)$$

$$\Delta^2 = \det \begin{pmatrix} 1 & \dots & x_1^{n-1} \\ \vdots & & \vdots \\ 1 & \dots & x_n^{n-1} \end{pmatrix} \cdot \det \begin{pmatrix} 1 & \dots & 1 \\ x_1 & \dots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \dots & x_n^{n-1} \end{pmatrix} = \det \begin{pmatrix} P_0 & P_1 & P_2 & \dots & P_{n-1} \\ P_1 & P_2 & & & P_n \\ P_2 & & & & \\ \vdots & & & & \\ P_{n-1} & P_n & & & P_{2n-2} \end{pmatrix}$$

הרחבה של שדות

תהי $K \subset L$ הרחבה של שדות. $[L : K] = \dim_K L$.

דוגמא. $[\mathbb{R} : \mathbb{Q}] = \infty$ כי אחרת יש בסיס $x_1, \dots, x_n \in \mathbb{R}$ בסיס - $\mathbb{Q}$ ולכל $r \in \mathbb{R}$ יש כתביה יחידה $\sum_{i=1}^n a_i x_i$ ($a_i \in \mathbb{Q}$) ולכן $|\mathbb{R}| = |\mathbb{Q}^n| = \aleph_0$ בסתירה.

שאלה. יהי F שדה סופי. אז $|F| = p^n$ עבור p ראשוני.

תשובה. F סופי לכן $p = \text{char } F < \infty$ וראינו בשיעור ש- p ראשוני וש- $\mathbb{Z}_p \subset F$, לכן, $|F| = p^n$ שדה הרחבה סופית (כי השדה סופי) של $\mathbb{Z}_p$ כלומר $[F : \mathbb{Z}_p] = n$ לאיזשהו n ואז $|F| = p^n$.

דוגמא. בניה של שדה בן 9 איברים. ניקח את $\mathbb{Z}_3$, הפולינום $x^2 - 2$ מעל $\mathbb{Z}_3$ (כי אין לו שורש ב- $\mathbb{Z}_3$). אי אפשר לקחת את $\sqrt{2}$ כממשי כי ממשיים הם לא שדה הרחבה של $\mathbb{Z}_3$. בכל זאת, יש שדה $K \subseteq \mathbb{Z}_3$ כך שיש ב- K שורש ל- $x^2 - 1$ נסמן אותו ב- $\sqrt{2}$. נגדיר: $F = \text{span}_{\mathbb{Z}_3}\{1, \sqrt{2}\}$. איברי F הם מהצורה $a \cdot 1 + b \cdot \sqrt{2}$ עבור $a, b \in \mathbb{Z}_3$.

$$a \cdot 1 + b \cdot \sqrt{2} \Leftrightarrow a = b = 0$$

$\Rightarrow$: אם $b = 0$ אז ברור ש- $a = 0$ ואם $b \neq 0$ $\frac{a}{b} \in \mathbb{Z}_3$ $\sqrt{2} = -\frac{a}{b}$ בסתירה. לכן $1, \sqrt{2}$ הם בסיס - $\mathbb{Z}_3$ של F . נגדיר כפל: $(a \cdot 1 + b \cdot \sqrt{2})(c \cdot 1 + d \cdot \sqrt{2}) = (ac + 2bd) \cdot 1 + (ad + bc) \cdot \sqrt{2}$. ההגדרה בסדר כי זה בסיס. תחת החיבור והכפל הנ"ל חוג חיפולי עם יחידה, תחום. לזוג $(a, b) \neq (0, 0)$ $(a \cdot 1 + b \cdot \sqrt{2})^{-1} = \frac{a-b\sqrt{2}}{a^2-2b^2}$ כי $1 = \frac{a \cdot 1 + b \cdot \sqrt{2}}{a^2-2b^2} (a \cdot 1 + b \cdot \sqrt{2})$ צריך לבדוק שהמכנה לא התאפס) לכן $[F : \mathbb{Z}_3] = 2$ וזו שדה ואז $[F : \mathbb{Z}_3] = 2$ לכן $|F| = 9$.

הערה. מראש $\mathbb{Z}_3 \subset K$ אפשר לחשוב על F כתת-קבוצה של K ואז החיבור והכפל מוגדרים לפי K (זה החיבור והכפל ב- K).

שאלה. תארו את השדה המינימלי המכיל את $\mathbb{Q}$ ואת $\sqrt{\rho}$ עבור $\rho \in \mathbb{Q}$ כך ש- $\sqrt{\rho} \in \mathbb{Q}$.

תשובה. $\sqrt{\rho} \in F, \mathbb{Q} \subset F$, לכן $\{\text{סכומים סופיים} : a_1 + a_2\sqrt{\rho} + a_3\sqrt{\rho}^2 + \dots : a_i \in \mathbb{Q}\}$
 $\{a + b\sqrt{\rho} : a, b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{\rho}] \subset F$
אבל $\mathbb{Q}[\sqrt{2}]$ הוא כבר שדה ואז $F = \mathbb{Q}[\sqrt{\rho}]$.
מדוע זה שדה?
 $a + b\sqrt{\rho} = 0 \Leftrightarrow a = b = 0$ (אם $b \neq 0$ אז $\sqrt{\rho} = -\frac{b}{a} \in \mathbb{Q}$ בסתירה). לכן $\sqrt{\rho} \notin \mathbb{Q}$
בסיס של $\mathbb{Q}[\sqrt{\rho}]$ מעל $\mathbb{Q}$.
 $[\mathbb{Q}[\sqrt{\rho}], \mathbb{Q}] = 2$

$$\frac{1}{a + b\sqrt{\rho}} = \frac{1}{a + b\sqrt{\rho}} \frac{a - b\sqrt{\rho}}{a - b\sqrt{\rho}} = \frac{a - b\sqrt{\rho}}{a^2 - b^2\rho}$$

ובגלל שקיים הפוך זה שדה.