

אלגברה ב2

© ארזים

4 באפריל 2017

1 שדות סופיים

הערה 1.1 לכל שדה סופי F קיים מספר ראשוני p (המציין או המאפיין של F) כך שמתקיים $\mathbb{F}_p \subseteq F$, לכן, $|F| = p^n$, כאשר $n > 0$.

משפט 1.2 לכל ראשוני p , ולכל $n > 0$ טבעי, קיים ויחיד שדה עם p^n איברים.

הוכחה: נתחיל מהוכחת היחידות. יהי F שדה עם p^n איברים. לפי ההערה, ההרחבה F/\mathbb{F}_p אלגברית, ולכן ניתן לשכן את F בתוך $\overline{\mathbb{F}_p}$, הסגור האלברי של \mathbb{F}_p . נניח עתה כי $F \subseteq \overline{\mathbb{F}_p}$. ניקח $x \in F^*$ ונבחין כי

$$\begin{aligned}x^{p^n-1} &= x^{|F^*|} = 1 \\x^{p^n} &= x\end{aligned}$$

והדבר האחרון מתקיים גם עבור 0, כלומר לכל $x \in F$. נסיק כי

$$F \subseteq \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$$

אבל ברור שקבוצה זו היא בעלת לכל היותר p^n איברים, ממשפט לגראנז' (יש לכל היותר d פתרונות לפולינום ממעלה d מעל שדה). לכן $F = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$, ועל כן הוא יחיד (עד כדי איזומורפיזם, כמובן).

נוכיח כעת קיום. נגדיר $\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$. ברור כי $0, 1 \in \mathbb{F}_{p^n}$. נראה סגירות לחיבור וכפל, ומסופיות ינבעו כל האקסיומות של שדה:

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} = x+y$$

ראינו עבור $n=1$, ניתן להוכיח באינדוקציה לכל n .

$$(xy)^{p^n} = x^{p^n} \cdot y^{p^n} = xy$$

נותר להראות כי יש p^n איברים בשדה. נגדיר $f(x) = x^{p^n} - x$. נשים לב כי מספיק להראות שבסגור האלגברי $\overline{\mathbb{F}_p}$, אין לפולינום f שורש כפול. די לראות כי אין שורשים משותפים של f, f' (נגזרת פורמלית).

$$f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$$

■ לכן אין שורשים משותפים, וסיימנו.

1.3 טענה

$$\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n} \iff k \mid n$$

הוכחה: נניח $k \mid n$. יהי $x \in \mathbb{F}_{p^k}$. אזי $x^{p^k} = x$. נעלה בחזקת p^k , ונקבל

$$x^{p^{2k}} = (x^{p^k})^{p^k} = x^{p^k} = x$$

וכך באינדוקציה $x^{p^{kl}} = x$ לכל l , בפרט עבור $l = \frac{n}{k}$. לכן $x \in \mathbb{F}_{p^n}$, ולכן $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n}$. בכיוון השני:

$$\mathbb{F}_p \xrightarrow{k} \mathbb{F}_{p^k} \xrightarrow{\frac{n}{k}} \mathbb{F}_{p^n}$$

(curved arrow from \mathbb{F}_p to \mathbb{F}_{p^n} labeled n)

■ לכן $n \mid k$.

1.4 טענה תהי A חבורה אבלית סופית, ויהי n השלם המינימלי עבורו $a^n = 1$ לכל $a \in A$. אזי קיים מסדר n .

הוכחה: לפי משפט המבנה:

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$$

■ כאשר $d_1 \mid \cdots \mid d_k$ שלמים. מתקיים $n = d_k$, ויש איבר מסדר d_k כנדרש.

1.5 משפט תת חבורה סופית של החבורה הכפלית של שדה הינה ציקלית.

הוכחה: תהי $A \subseteq F^*$ סופית, ויהי $x \in A$ האיבר שמובטח לנו מהטענה הקודמת. נסמן את סדרו n . אזי

$$A \subseteq \{\alpha \in F \mid \alpha^n = 1\}$$

■ לכן נקבל $|A| \leq n$. מאידך, $|\langle x \rangle| = n$, וכן $\langle x \rangle \subseteq A$, ולכן $A = \langle x \rangle$.

1.6 מסקנה

$$\mathbb{F}_{p^n}^* \cong \mathbb{Z}/(p^n - 1)\mathbb{Z}$$

1.7 מסקנה קיים $\alpha \in \overline{\mathbb{F}_p}$ כך שמתקיים $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$.

הוכחה: מהמשפט הקודם, קיים יוצר ציקלי של $\mathbb{F}_{p^n}^*$, שנסמנו α . ברור כי $\mathbb{F}_p[\alpha] \subseteq \mathbb{F}_{p^n}$, ומצד שני,

$$|\mathbb{F}_p[\alpha]| \geq (p^n - 1) + 1 = p^n$$

■

1.8 מסקנה לכל n , יש פולינום אי פריק ממעלה n .

הוכחה: יהי $\alpha \in \mathbb{F}_{p^n}$ המקיים $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^n}$. יהי $f = \text{irr}(\alpha, \mathbb{F}_p)$. אזי $\deg f = n$, והוא אי פריק, וסיימנו.

■

1.9 הגדרה נסמן

$$\pi_p(n) = |\{f \in \mathbb{F}_p[x] \mid f \text{ is a monic irreducible polynomial of degree } n\}|$$