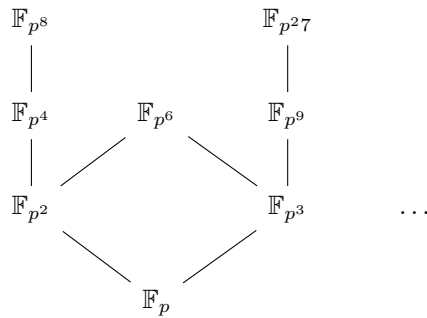


אלגברה ב2

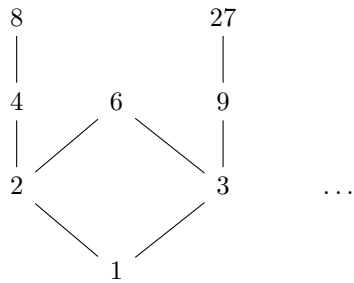
© ארזים

4 באפריל 2017

נבטונן בהרחבות הסופיות של \mathbb{F}_p :



זה מזכיר קצת פירוק של מספרים לראשוניים:



כמובן, איחוד על פני כל ההרחבות הסופיות של \mathbb{F}_p ייתן את הסגור האלגברי. נרצה לברר האם יש תת שדה $K \subsetneq \overline{\mathbb{F}_p}$ שדרגתו מעל \mathbb{F}_p אינסופית. התשובה היא שיש: ניקח

$$K = \bigcup_{m=0}^{\infty} \mathbb{F}_{p^{2^m}}$$

ונבחין שזהו שדה, שמעלתו גדולה יותר מאשר 2^m , לכל m . לכן היא אינסופית. אפשר לראות שהשדה \mathbb{F}_{p^3} אינו מוכל בתוך K , כי אם הייתה הכלה אז היה $0 < m \in \mathbb{N}$ עם $3 \mid 2^m$. בסתירה, $\mathbb{F}_{p^3} \subseteq \mathbb{F}_{p^{2^m}}$.

תרגיל הראו כי

$$p^k - 1 \mid p^m - 1 \iff k \mid m$$

פתרון אם $k \mid m$, אזי $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^m}$, ואז $\mathbb{F}_{p^k}^* \subseteq \mathbb{F}_{p^m}^*$, וממשפט לגראנז' מתקיים $p^k - 1 \mid p^m - 1$.
 בכיוון השני, אם $p^k - 1 \mid p^m - 1$, נראה כי $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^m}$ ונסיים. יהי $x \in \mathbb{F}_{p^k}$, $x \neq 0$.
 $|\mathbb{F}_{p^k}^*| \mid |\mathbb{F}_{p^m}^*| = p^m - 1$.

$$x^{p^k - 1} = 1$$

ולכן גם $x^{p^m - 1} = 0$, והרי שמתקיים $x \in \mathbb{F}_{p^m}$.

תרגיל הראו כי בשדה סופי, מכפלת כל האיברים ההפיכים היא -1 .

פתרון

$$\prod_{x \in F^*} x = \left(\prod_{x^{-1} \neq x \in F^*} x x^{-1} \right) \cdot 1 \cdot (-1) = -1$$

הגדרה 0.1 יהי R חוג. R נקרא סגור אלגברית אם לכל פולינום $f \in R[x]$ ממעלה לפחות 1 יש שורש בתוך R .

תרגיל הראו כי חוג סופי $R \neq 0$ אינו סגור אלגברית.

פתרון לפולינום הבא אין שורש:

$$f(x) = \left(\prod_{r \in R} (x - r) \right) + 1$$

תרגיל פרקו את $x^7 + x + 1$ מעל \mathbb{F}_7 ומצאו הרחבה קטנה ככל האפשר של \mathbb{F}_7 בה הפולינום מתפרק למכפלת גורמים לינאריים.

פתרון נציב $x + 3$:

$$(x + 3)^7 + x + 3 + 1 = x^7 + 3 + x + 3 + 1 = x^7 + x = x(x^6 + 1)$$

נמשיך לפרק:

$$\begin{aligned} x^6 + 1 &= (x^2)^3 - (-1) \\ T^3 - (-1) &= (T - 3)(T - 5)(T - 6) \\ x^6 + 1 &= (x^2 - 3)(x^2 - 5)(x^2 - 6) \end{aligned}$$

אם כן:

$$x^7 + x = x(x^2 - 3)(x^2 - 5)(x^2 - 6)$$

נציב בחזרה $x - 3$:

$$(x - 3)(x^2 + x + 6)(x^2 + x + 4)(x^2 + x + 3)$$

כעת, בשדה \mathbb{F}_{49} יש שורש של כל פולינום ריבועי או לינארי, ולכן בפרט את כל השורשים של הפולינום.

תרגיל הוכיחו כי $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10}$ אי פריק מעל \mathbb{F}_2 .

פתרון די להוכיח שאין גורם אי פריק ממעלה לכל היותר 5. נניח בשלילה שיש גורם כזה, וניקח שורש שלו $\alpha \in \overline{\mathbb{F}_2}$. מאפס גורם של הפולינום המקורי, ולכן גם אותו, כלומר $\alpha^{11} = 1$. ברור כי $\alpha \neq 1$, ולכן הוא מסדר 11. עם זאת, $\mathbb{F}_2(\alpha)$ הוא הרחבה סופית של \mathbb{F}_2 ממעלה לכל היותר 5, שגודלה חזקת שתיים - כלומר כמות ההפיכים בה היא אחת מבין $1, 3, 7, 15, 31$ - ואז 11 צריך לחלק את כמות ההפיכים, כי הוא סדר של איבר (משפט לגראנז'). 11 לא מחלק אף אחת מהאפשרויות, בסתירה.

תזכורת בהרצאה הגדרנו

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

בהרצאה הבאה נוכיח את העובדה הבאה:

$$\pi_p(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

כאשר μ מוגדרת כך: אם $t = p_1 \cdots p_k$ מכפלת ראשוניים שונים, אזי $\mu(t) = (-1)^k$. אחרת, $\mu(t) = 0$. נפשט מעט את הנוסחה:

$$\pi_p(n) = \frac{1}{n} (p^n \pm p^{\frac{n}{2}} \pm \dots) \sim \frac{p^n}{n}$$

אנחנו מתכוונים לומר:

$$\lim_{n \rightarrow \infty} \frac{\pi_p(n)}{\frac{p^n}{n}} = 1$$

זה מזכיר לנו את משפט המספרים הראשוניים:

$$\pi(x) \sim \frac{x}{\log x}$$

אם נציב $x = p^n$, נקבל

$$\pi(p^n) \sim \frac{p^n}{\log p^n} = \frac{1}{\log p} \frac{p^n}{n}$$