

1. יהי $f \in F[x]$ מונומיאל, $n = \deg(f)$.

יהי K שדה סגור ו- $f(x) \in F[x]$ פולינום.

$$[K:F] \leq n!$$

הוכחה: האינדוקציה על n .

בסיס: $n=1$ - אין מה להוכיח.

הנניס: נניח $f(x) \in F[x]$ פולינום.

יהי α שורש של $f(x)$.

$$F \subset F(\alpha) \subset K$$

$$g(x) \in F(\alpha)[x], \quad f(x) = (x-\alpha)g(x)$$

K הוא שדה סגור ו- $g(x)$ פולינום.

האינדוקציה:

$$[K:F(\alpha)] \leq (\deg g(x))! = (n-1)!$$

$$[F(\alpha):F] = \deg p(x) \leq \deg f(x) = n$$

$$[K:F] = [K:F(\alpha)][F(\alpha):F] \leq n! \quad \text{וק.$$

2. יהי p ראשוני. נניח $f(x) \in \mathbb{Q}[x]$ פולינום.

$$f(x) = x^{p-1} + x^{p-2} + \dots + x + 1$$

$$f(x) = \frac{x^p - 1}{x - 1}$$

אנחנו רוצים להראות כי $f(x)$ אינו מתפרק על $\mathbb{Q}$.

נניח $f(x) = (x-\alpha)g(x)$ על $\mathbb{Q}$.

$$\xi = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p} = e^{\frac{2\pi i}{p}}, \quad 1, \xi, \xi^2, \dots, \xi^{p-1}$$

השדה $\mathbb{Q}(\xi)$ הוא שדה הפיצול של $f(x)$.

כיוון ש- $f(x)$ אינו מתפרק על $\mathbb{Q}$, נקבל:

$$[\mathbb{Q}(\xi):\mathbb{Q}] = p-1$$

3. נמצא את כל הפתרונות של $x^5 - 2 = 0$ ב- $\mathbb{Q}$.

$$x^5 - 2 = (x - \sqrt[5]{2})(x - \sqrt[5]{2}\zeta)(x - \sqrt[5]{2}\zeta^2)(x - \sqrt[5]{2}\zeta^3)(x - \sqrt[5]{2}\zeta^4)$$

כאן

$$\zeta = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$$

כל הפתרונות = $\sqrt[5]{2} \zeta^k$ עבור $k=0,1,2,3,4$

- כאן $x^5 - 2$ אינו פירוק מלא (כי 2 אינו חזקה של 5)

הפירוק הקובץ כאן $x^5 - 2$ הוא שבר מנה 4 מ- $\mathbb{Q}$.

כיון ש-4, 5 זרים, נקבל:

$$[\mathbb{Q}(\sqrt[5]{2}, \zeta) : \mathbb{Q}] = 4 \cdot 5 = 20$$

4. נניח "קלאוס" :

$$\frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1 = 0$$

הצבה של $x^2 = t$ נותנת:

$$x^4 + x^3 + x^2 + x + 1 = 0 \Rightarrow t^2 + t + 1 + \frac{1}{t} + \frac{1}{t^2} = 0$$

$$(x^2 + 2 + \frac{1}{x}) + (x + \frac{1}{x}) - 1 = 0$$

$$(x + \frac{1}{x})^2 + (x + \frac{1}{x}) - 1 = 0$$

$$x + \frac{1}{x} = \frac{-1 \pm \sqrt{5}}{2} = \alpha, \quad \alpha^2 = \frac{3 \pm \sqrt{5}}{2}$$

$$x + \frac{1}{x} = \alpha, \quad x^2 - \alpha x + 1 = 0$$

$$x = \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2} = \frac{-1 \pm \sqrt{5}}{2} \pm \sqrt{\frac{3 \pm \sqrt{5}}{2} - 4}$$

$$e^{\frac{2\pi i}{5}} = \frac{-1 + \sqrt{5} + \sqrt{-10 + 2\sqrt{5}}}{4}$$

אם $\zeta = e^{\frac{2\pi i}{5}}$

$$\cos \frac{2\pi}{5} = \frac{\sqrt{5} - 1}{4}$$

הערות: נקבל

י"ה פ מספר ראשוני.

מסמן: $\mathbb{F}_{p^n}$ - הסדר הראשון (גודל ראשוני)
כא p^n איברים.

$$(\mathbb{Z}_p = \mathbb{F}_p)$$

$\mathbb{F}_{p^n}^*$ ציקל, כא $p^n - 1$ איברים.
:F-3

$x^2 + 3$ $\mathbb{F}_5$ הוא אי-פריק:

צ"ב $1, 2, \dots, 5^0$ ונסו.

י"ה α אינו $\mathbb{F}_5$ הפולינום $x^2 + 3$ פריק
:K

$$K = \mathbb{F}_5[\alpha] \cong \mathbb{F}_{25}$$

- נבדוק כי $-2 + \alpha$ הוא יוצר ציקל של $\mathbb{F}_{25}^*$:
 $\alpha^2 = 2, \alpha \in \mathbb{F}_{25}$

נראה $-2 + \alpha$ $\mathbb{F}_{25}$ (24) $\mathbb{F}_{25}^*$

ולכן הוא בקבוצה $\{1, 2, 4, 8, 3, 6, 12, 24\}$ $\alpha^2 = 2, \alpha^3 = 2\alpha$

$$(-2 + \alpha)^2 = 4 + 4\alpha + \alpha^2 = 6 - 4\alpha = 1 + \alpha \neq 1$$

$$(-2 + \alpha)^4 = (1 + \alpha)^2 = 1 + 2\alpha + \alpha^2 = 3 + 2\alpha \neq 1$$

$$\begin{aligned} (-2 + \alpha)^{12} &= (2\alpha - 2)^3 = 3(\alpha - 1)^3 = 3(\alpha^3 - 3\alpha^2 + 3\alpha - 1) = \\ &= 3(2\alpha - 6 + 3\alpha - 1) = -6 = -1 \end{aligned}$$

$$(-2 + \alpha)^{24} = (3 + 2\alpha)^2 = 9 + 12\alpha + 4\alpha^2 = -1 + 2\alpha + 3 = 2\alpha \neq 1$$