

10/3/08

תכנון

כתיבה רגילה השיעור הקודם

$$\det \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \det A \det B$$

כאלוהי צורה סופר לרוביות ועוד משהו צריך להוסיף

$$\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det A \det B$$

$$\det \begin{pmatrix} A_1 & & * \\ & \ddots & \\ 0 & & A_k \end{pmatrix} = \prod_{i=1}^k \det A_i$$

שדה סופי

משפט: G שדה סופי מסוים מספר $p > 0$ הוא p^n איברי

משפט: G שדה F $\text{char}(F) = 0$ וכל $\text{char}(F) = p$

זיקלי

השדה \mathbb{Z}_p שדה p האיברי

$$p \cdot \mathbb{Z} = \{ \dots, -p, 0, p, 2p, \dots \}$$

$$\mathbb{Z}_p = \{ [i] \mid i = 0, \dots, p-1 \} \quad [i] = i + p\mathbb{Z}$$

$$i + p\mathbb{Z} = \{ i-p, i, i+p, i+2p, \dots \}$$

$$[k] + [l] = [j]$$

(יש להוסיף) $k+l = j+pm$

$$0 \leq j \leq p-1$$

$$[k] \cdot [l] = [k \cdot l]$$

(רוביות) קבוצתו של החוקי והכל שיתבנה מקומם של רוביות

יש הפסד יש צד

$\text{char}(F) = p, x \in F, G$

$$m \cdot x = \begin{cases} \overbrace{x + \dots + x}^{m \text{ פעמים}} & m > 0 \\ \underbrace{(-x) + \dots + (-x)}_{|m|} & m < 0 \\ 0 & m = 0 \end{cases}$$

יש $\text{char} F = p$ כל \mathbb{Z}_p

$\forall x \in F \quad px = 0$ (1)

יש $n = p \cdot m$ כל $nx = 0$ כל \mathbb{Z}_p (2)

מפתח

השאלה

$1 + \dots + 1 = 0$ e C בגי מנימלי. $m = \text{char}(F)$

$\text{char} F = 0$ אם לא קיים m כזה של מציבים

$\text{char} F = p > 0$ אחרת

$\forall x, y \in F : (x+y)^p = x^p + y^p$

פתרון: $(x+y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}$

אם נראה של $k=1, \dots, p-1$ $\binom{p}{k}$ מתחלק ב- p (מחלק של p נקרא

אם $m = p \cdot m'$ אז p מתחלק ב- m ; כיון שמתקיים

$\forall x \in F : m \cdot x = (p \cdot m') \cdot x = p(m'x) = 0$ ($m'x \in F$ e כיון e

$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1) \cdot \dots \cdot (p-k+1)}{k!}$

p מחלק את המונה, אבל p לא מחלק את המכנה (אכן p מחלק

את המנה) \square
 $(x+y)^{p^r} = x^{p^r} + y^{p^r}$ מתקיים

הוכחה באינדוקציה על r

דוגמה: \mathbb{Z}_5 -
 $[3]^5 = ([2] + [1])^5 = [2]^5 + [1]^5 = [1]^5 + [1]^5 + [1]^5 = [3]$

תוצאה: $x \in \mathbb{Z}_p$ מתקיים $x^p = x$

(השאלה: \mathbb{Z}^p בחלוקה p היא \mathbb{Z})

"מ"מ \mathbb{Z}_p

תוצאה: פתרון של מערכת המשוואות הבאה:

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 2 & 1 & 5 & 1 \\ 3 & 5 & 4 & 0 \end{array} \right)$$

\mathbb{Z}_5 \mathbb{F}_5 (א)

\mathbb{Z}_7 \mathbb{F}_7 (ב)

פירוק לזוגות

$$Z_5 \begin{array}{c|ccc|c} 1 & 2 & 3 & 4 & 0 \\ \hline 1 & 3 & 2 & 4 & x \end{array}$$

$$Z_7 \begin{array}{c|cccc|c} 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ \hline 1 & 4 & 5 & 2 & 3 & 6 & x \end{array}$$

$$Z_8 \begin{array}{c|cccc|c} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \\ \hline 1 & x & 3 & x & 5 & x & 7 & x \end{array}$$

Z_8 זוגות של 6 ו- 7 אינם זוגיים

Z_5 זוגות (10)

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 2 & 1 & 5 & 1 \\ 3 & 5 & 4 & 0 \end{array} \right) \begin{array}{l} R_2 \leftarrow R_2 - 2R_1 \\ R_3 \leftarrow R_3 - 3R_1 \end{array} \rightarrow \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 4 & 3 & 4 \\ 0 & 2 & 1 & 2 \end{array} \right) \begin{array}{l} R_2 \leftarrow \frac{1}{4}R_2 \end{array}$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 2 & 1 & 2 \end{array} \right) \begin{array}{l} R_1 \leftarrow R_1 - R_2 \\ R_3 \leftarrow R_3 - 2R_2 \end{array} \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 4 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 2 & 0 \end{array} \right) \begin{array}{l} R_1 \leftarrow R_1 - 4R_3 \\ R_2 \leftarrow R_2 - 2R_3 \end{array}$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array} \right) \begin{array}{l} \text{זוגות} \\ \text{זוגות} \end{array}$$