

יש המבולגן בקלות עם המערכת הריבית $V(x_0, \dots, x_{n-1})$ ויש המבולגן עם המערכת הריבית $V(x_0, \dots, x_{n-1})$

$\det V(x_0, \dots, x_{n-1}) = \prod_{j < k} (x_k - x_j) \neq 0$

כלומר יש מערכת של x_0, \dots, x_{n-1} שבה $\det V \neq 0$

הערה:

המערכת $x_0, \dots, x_{n-1} \in F$ היא מערכת של $F_n[X]$ ויש לה מערכת של F .

הערה:

המערכת (y_0, \dots, y_{n-1}) היא מערכת של $F_n[X]$ ויש לה מערכת של F .

$a(x) \rightarrow (y_0, \dots, y_{n-1})$ ארבעה

$\tilde{a}(x) \rightarrow (y_0, \dots, y_{n-1})$ ארבעה

(x_0, \dots, x_{n-1}) מערכת של F ויש לה מערכת של $F_n[X]$

$a(x) + \tilde{a}(x) \rightarrow (y_0 + \tilde{y}_0, \dots, y_{n-1} + \tilde{y}_{n-1})$

$\tilde{a}(x) \rightarrow (y_0, \dots, y_{n-1})$

יש מערכת של F ויש לה מערכת של $F_n[X]$

הערה:

יש מערכת של F ויש לה מערכת של $F_n[X]$

$\deg a(x) + \deg \tilde{a}(x) < n$

יש מערכת של F ויש לה מערכת של $F_n[X]$

$\log_2 2^n = 2^{\log_2 2^n} = 2^n$

יש מערכת של F ויש לה מערכת של $F_n[X]$

המערכת $a(x) \in F_n[X]$ היא מערכת של F

$a(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$

יש מערכת של F ויש לה מערכת של $F_n[X]$

יש מערכת של F ויש לה מערכת של $F_n[X]$

$y_k = a(x_k) \quad (0 \leq k \leq n-1)$

יש מערכת של F ויש לה מערכת של $F_n[X]$

יש מערכת של F ויש לה מערכת של $F_n[X]$

יש מערכת של F ויש לה מערכת של $F_n[X]$

$\psi((a_0, \dots, a_{n-1})) := (y_0, \dots, y_{n-1})$

$y_k = \sum_{j=0}^{n-1} a_j x_k^j \quad (0 \leq k \leq n-1)$

יש מערכת של F ויש לה מערכת של $F_n[X]$

הערה:

יש מערכת של F ויש לה מערכת של $F_n[X]$

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

יש מערכת של F ויש לה מערכת של $F_n[X]$

$\dim \ker \psi + \dim \text{im } \psi = n$

יש מערכת של F ויש לה מערכת של $F_n[X]$