

WB12

30/04/2012

הרצאה

הוכחנו כי בהינתן $p(x) \in F[x]$ אי-זריק, M מרחב וקטורי, $K \supset F$ הרחבה של F ו- $\alpha \in K$ ש- $p(\alpha) = 0$,
 הוכחנו אז כי $K = F[\alpha]$.
 הוכחנו זאת על ידי כך:

$$K = \frac{F[x]}{F[x]_{p(x)}}$$

$\varphi: F \hookrightarrow K$ — נבחר $\varphi(a) = a + F[x]_{p(x)}$
 — אברהם K נחשב כך:

$$\sum_{i=0}^n a_i x^i + F[x]_{p(x)} = \sum_{i=0}^{n-1} b_i x^i + F[x]_{p(x)} = \sum_{i=0}^{n-1} b_i (x + F[x]_{p(x)})^i$$

$$= \sum_{i=0}^{n-1} b_i \alpha^i$$

כאשר $p(\alpha) = 0$,
 F נכנסת ל- $K = F[\alpha]$

$a \in F, t \in K$

$$a \cdot t = \varphi(a) \cdot t$$

$$a = a \cdot 1_K = \varphi(a)$$

הרחבה

הרחבה $F \hookrightarrow K$ נקראת הרחבה פולינומית אם $K = F[\alpha]$ עבור אי-זריק $p(x) \in F[x]$.
 אם F היא שדה ו- α אי-זריק, אז $F[\alpha]$ היא הרחבה פולינומית של F .
 (הערה: F יכולה להיות גם שדה או שדה חסומים).

משפט: שדה F הוא אלמנטרי קיים.

יהי $f(x) \in F[x]$ פולינום.

אם $f(x)$ אינו מתפצל ב- F אז F הוא שדה.

הוכחה: באינדוקציה על $\deg(f(x))$.

בסיס: $n=1$ - F הוא שדה, כל פולינום מתפצל.

כאשר $f(x) = a(x-b)$, $F \ni a \neq 0$, F הוא שדה, $K=F$.

נניח $\deg(f(x)) \geq 2$.

יהי $f(x)$ פולינום מתפצל ב- F אז F הוא שדה.

אם $F \subset L$ שדה, אז F הוא שדה.

מחצית $\deg(f(x))$ היא מספר שלם α של $f(x)$.

פרק $f(x)$ הוא פולינום מתפצל ב- L כך:

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

באינדוקציה, כיון $\deg(g(x)) = \deg(f(x)) - 1$, יש שדה F של $g(x)$.

שדה F הוא שדה L .

נניח K הוא שדה של F ויש $\alpha_1, \alpha_2, \dots, \alpha_r$ שונים.

אם $\alpha_1, \alpha_2, \dots, \alpha_r$ הם שונים אז K הוא שדה.

אם $L = F[\alpha]$ אז $\alpha_1, \alpha_2, \dots, \alpha_r$ הם שונים.

אם K הוא שדה של F אז $\alpha_1, \alpha_2, \dots, \alpha_r$ הם שונים.

אם K הוא שדה של F אז $\alpha_1, \alpha_2, \dots, \alpha_r$ הם שונים.

משפט: נניח F_1, F_2 איזומורפיזם.

יהי $F_1 \rightarrow F_2$ איזומורפיזם.

יהי $f(x) \in F_1[x]$ פולינום מתפצל ב- F_1 .

אם $f(x)$ מתפצל ב- F_2 אז F_1 הוא שדה.

אם $f(x)$ מתפצל ב- F_2 אז F_1 הוא שדה.

אם F_1 הוא שדה אז F_2 הוא שדה.

אם F_1 הוא שדה אז F_2 הוא שדה.

יהי F_2 שדה, הוכחה, הוכחה, F_2 הוא שדה.

9.11' $\rho_{\text{rel}} = 0.5$, $\rho_{\text{rel}} = 0.5$ 10

$\sigma: K_1 \rightarrow K_2$
 $\sigma(u_1) = u_2$

כוכב:

$$\varphi: F_1[X] \rightarrow F_2[X]$$

7321

 $\therefore \text{ } ^{\circ}8$

$$\varphi\left(\sum_{j=1}^N a_j x^j\right) = \sum_{j=1}^N i(a_j) x^j$$

זמן אנונימיות. קר אנונימיות. זמן אנונימיות. זמן אנונימיות.

$$\psi(\sum_j a_j x^j \cdot \sum_l b_l x^l) = \psi(\sum_{s=0}^{M+R} (\sum_{j+l=s} a_j b_l) x^s) =$$

$$= \sum \left(\sum_i i(a_i) i(b_i) \right) x^5 = \left(\sum_i i(a_i) x^i \right) \left(\sum_i i(b_i) x^i \right)$$

- 4 תולדות, ח' ב' אבות א - תולדות:

$$\varphi^{-1}(\Sigma_{d_1} x^0) = \Sigma_{d_1}^{-1}(d_1) \times \mathbb{Q}$$

- כהל, 5 מעביר הלוח
- אי-סרז, זבולעם אי-סרז.
אי-סרז, בן-סרז: $\phi(p) = 1 - \phi(p)$ אי-סרז.

• e / m =

$$\varphi(F_1(x)p(x)) = F_2(x) \cdot i(p)(x)$$

4 פתח יחידות: 1000

$$i: \quad \frac{F_1[x]}{F_1[x]_{p(x)}} \xrightarrow{\sim} \frac{F_2[x]}{F_2[x]_{i(p)(x)}}$$

$$\sum \tilde{a}_j x^j + F_1(xp(x)) \mapsto \sum i(\tilde{a}) x^j + F_2(x) i(p)(x)$$

$$K_1 = F_1[u_1] \xrightarrow{S_1} F_1[x] / F_1[x]p(x) \xrightarrow{i_1} F_2[x] / F_2[x]i(p(x)) \xrightarrow{t_2} K_2 = F_2[u_2]$$

8

$$\sum_{j=1}^N a_j u_1^j \xrightarrow{S_1} \sum_{j=1}^N a_j x^j \in F_1[x]p(x) \xrightarrow{i_1} \sum_{j=1}^N i(a_j) x^j \in F_2[x]i(p(x))$$

$$\xrightarrow{t_2} \sum_{j=1}^N i(a_j) u_2^j$$

כבר, $u_1 \mapsto u_2$

וההיקף i $a_0 \mapsto i(a_0)$

לעיל נתקן שן F_1, F_2 איזומורפיים

והי' $F_1 \rightarrow F_2$ איזומורפיזם. הי' $[a] \in F_1$ סוף

הי' קבוצה L_1, L_2 הי' L_1 סוף L_2 סוף

הי' F_1 סוף F_2 סוף (f) סוף F_2 סוף

הי' (a) סוף (a) סוף (a) סוף F_1 סוף

הי' L_1 סוף L_2 סוף (a) סוף L_2 סוף

סוף (a) סוף (a) סוף (a) סוף

$L_1 \rightarrow L_2$ סוף (a) סוף (a) סוף (a) סוף

הי' (a) סוף (a) סוף (a) סוף (a) סוף

סוף (a) סוף (a) סוף (a) סוף (a) סוף

סוף (a) סוף (a) סוף (a) סוף (a) סוף

סוף (a) סוף (a) סוף (a) סוף (a) סוף

סוף (a) סוף (a) סוף (a) סוף (a) סוף

סוף (a) סוף (a) סוף (a) סוף (a) סוף

סוף (a) סוף (a) סוף (a) סוף (a) סוף

סוף (a) סוף (a) סוף (a) סוף (a) סוף

$$\tau(f)(x) = \tau(f)(x) = (1 - \tau(u,1)) \tau(g)(x) =$$

$$= (x - u_1) \tau(g)(x)$$

כיוון ש $1 - \tau(u,1) = \tau(g)(x)$ - רצוי בקצרה

יש פה שני טיפוסים של טיפוסים

$$G : L_1 \rightarrow L_2 \quad G : C \rightarrow C$$

מציג את שני הטיפוסים של הטיפוסים

(אנחנו יוצרים) של הטיפוסים של הטיפוסים

יש טיפוסים של הטיפוסים של הטיפוסים

הוא שני הטיפוסים של הטיפוסים

ובן ל L_2 שני הטיפוסים של הטיפוסים

אכן שני הטיפוסים של הטיפוסים

למשל

למשל

יש $F(x) = x^2$ פונקציה של הטיפוסים

יש F של הטיפוסים של הטיפוסים

יש F של הטיפוסים של הטיפוסים

יש F של הטיפוסים של הטיפוסים

יש F של הטיפוסים של הטיפוסים

למשל: איננו רוצים בזה של הטיפוסים

יש F של הטיפוסים של הטיפוסים

למשל

(1) יש F של הטיפוסים של הטיפוסים

(2) יש F של הטיפוסים של הטיפוסים

כבר מביא משהו של הטיפוסים

קובץ 10

(1) $\Leftarrow$ (2): נניח כי u הוא שבר פשוט $u \in F[x]$.

יהי $p(x) \in F[x]$ אי-פריק, $u \in K$.

הוא אדם של $p(x)$.

בשורה, נניח כי $p(x)$ אינו מתפצל לחלוטין u .

יהי L שדה פשוט של $p(x)$ ו- u .

ונבחר שדה $K \setminus L$ $v \in$.

אנו יוצגים כי יש איזומורפיזם $f: F \rightarrow$.

$$f: F[u] \xrightarrow{\sim} F[v]$$

$$f(u) = v$$

K הוא שדה פשוט של $f(x)$ ו- $f(u)$.

$K[v]$ הוא שדה פשוט של $f(x)$ ו- $f(u)$.

אם נחשב הקירובים, יש הרבה של f איזומורפיזם.

$$f: K \rightarrow K[v]$$

כיוון ש- f מרחיב את f , ו- f הוא איזומורפיזם $F \rightarrow$.

(אולי) הוא הפיכה $f: F \rightarrow$, שכן f פשוט.

הוא איזומורפיזם $F \rightarrow$.

$$[u: F] = [u(v): F] \quad \text{בפירוק}$$

$$[u(v): F] = [u(v): u] [u: F] \quad \text{אם}$$

$$[u(v): u] = 1 \quad \text{ואכן}$$

$$u \notin K \quad \text{כי}$$