

הגדרה

אוטומורפיזם הוא איזומורפיזם מחוג לעצמו.

דוגמה

אוטומורפיזם $\mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{2}]$ מוגדר ע"י $\sqrt{2} \mapsto -\sqrt{2}$. זה בעצם אומר שאין הבדל אלגברי בין $\sqrt{2}$ ל- $-\sqrt{2}$. אבל צריך להיזהר! זה נכון כשמתסכלים על $\mathbb{Q}[\sqrt{2}]$, אבל לא בהכרח אם מסתכלים על שדה יותר גדול - למשל ב- \mathbb{R} , $\sqrt{2}$ הוא ריבועי ו- $-\sqrt{2}$ אינו ריבועי. כלומר $\exists b \in \mathbb{R} b^2 = a$ נכון עבור $\sqrt{2}$ ולא עבור $-\sqrt{2}$.

הערה

אם $f : K \rightarrow R$ הוא הומומורפיזם $0 \neq$ של חוגים K שדה, אז f הוא חח"ע.

הוכחה

$$\ker f \triangleleft K \implies \ker f = 0$$

הגדרה

יהי F שדה. F -אלגברה קומוטטיבית הוא חוג שמכיל את F (הגדרה זמנית לצורך הקורס)
הומומורפיזם של F -אלגברות הוא הומומורפיזם של חוגים $\varphi : K \rightarrow R$ כאשר K, R שניהם F -אלגברות ו- $\forall \alpha \in F \varphi(\alpha) = \alpha$.

למה

אם K/F (שדה) הרחבה של F אז $[K : F] < \infty$ ו- $\varphi : K \rightarrow K$ הומומורפיזם של F -אלגברות אז φ אוטומורפיזם.

הוכחה

φ חח"ע לפי ההערה. לכן $\varphi(K) \subseteq K$ ו- $[\varphi(K) : F] = [K : F]$ (כי φ מעביר בסיס $\{b_1, \dots, b_n\}$ של K לבסיס $\{\varphi(b_1), \dots, \varphi(b_n)\}$ של $\varphi(K)$). לכן $\varphi(K) = K$ ו- $\varphi \leftarrow \varphi$ על φ איזומורפיזם.

מסקנה

קיבלנו "ספר בישול" לבנות אוטומורפיזמים של $K = F[a]$ כאשר $a \in K$ אלגברי מעל F . ניקח $f \in F[\lambda]$ הפולינום המינימלי של a מעל F . אי פריק (מדרגה) $[K : F]$

ניקח את השורשים a_1, \dots, a_n של f בתוך K . לכל אחד יש הומומורפיזם- F , ולכן אוטומורפיזם- F .

$$\sigma : K \rightarrow K \quad \sigma(a) = a_i$$

כלומר

$$\sigma\left(\sum \alpha_j a^j\right) = \sum \alpha_j a_i^j \quad \alpha_j \in F$$

כלומר $\text{Gal}(K/F) = m$ בדוגמא הזאת.

דוגמאות של אלגבראות

I. \mathbb{C}, \mathbb{R} הם \mathbb{Q} -אלגברות.

II. כל שדה עם מאפיין 0 הוא \mathbb{Q} אלגברה.

III. כל שדה עם מאפיין p הוא \mathbb{F}_p -אלגברה.

תזכורת

נתון חוג כלשהו R , נגדיר $\varphi : \mathbb{Z} \rightarrow R$ לפי $\varphi(n) = \underbrace{1 + 1 + 1 + \dots + 1}_{n \text{ times}} \in R$

$\ker \varphi \triangleleft \mathbb{Z}$, לכן $\ker \varphi = m\mathbb{Z}$ עבור איזשהו m .

הגדרה

$\text{char}(R) = m$ עבור R תחום שלמות. m הוא מספר ראשוני p . מש' נותר $\Leftrightarrow \mathbb{F}_p \cong \mathbb{Z}/\ker \varphi \hookrightarrow R$

המשך דוגמאות

IV. $F[\lambda]$ הוא F -אלגברה.

הגדרה

f מתון אם המקדם העליון הוא 1.

הערה: אם α המקדם העליון של f אז $\alpha^{-1}f$ פולינום מתוקן עם אותם שורשים.

$f \in F[x]$ מתוקן מתפצל אם $f = (\lambda - \alpha_1) \cdots (\lambda - \alpha_n)$ בתוך $f[\lambda]$.

הגדרה

E שדה פיצול של f מעל F אם f מתפצל בתוך E ו f אינו מתפצל בכל שדה L עבור $F \leq L < E$.
במילים אחרות, E שדה פיצול של $E = F[a_1, \dots, a_n]$ כאשר $f = (\lambda - a_1) \cdots (\lambda - a_n)$ ו $E = F[\lambda]$ בתוך E .

שאלות

I. האם אפשר לבנות שדה פיצול?

II. האם הוא יחיד עד F -איזומורפיזם?

פתרון ל I

ניקח g_1 גורם אי פריק של f . נגדיר $K_1 = F[\lambda]/F[\lambda]g_1$. הוא מכיל שורש $a_1 := \lambda + F[\lambda]g_1$.
בתוך $K_1[\lambda]$, $f = (\lambda - a_1)h_2$, $(h_2 \in K_1[\lambda])$
ממשיכים למצוא $K_2 \supset K_1$ עם שורש a_2 של h_1 , ונעשה n פעמים עד שמגיעים ל K_n . אז

$$K_n = F[a_1, \dots, a_n]$$

לכן K שדה פיצול של f .

דוגמה

E שדה הפיצול של F

$$\lambda^7 + 3\lambda^6 + 17\lambda^5 + 13\lambda^4 + 4\lambda^3 - 10002\lambda^2 + \lambda - 10$$

אולי $[E : F] = 7!$

I. אם $\deg f = 2$ אי פריק ב $F[\lambda]$ אז $[E : F] = 2$.

למשל \mathbb{C} שדה הפיצול של $\lambda^2 + 1$ מעל \mathbb{R} .

$\mathbb{Q}[\sqrt{2}]$ שדה הפיצול של $\lambda^2 - 2$ מעל \mathbb{Q} .

II. $f = \lambda^n - 1 = \prod_{i=1}^{n-1} (\lambda - p^i)$ כאשר p שורש n -פרימיטיבי של 1.

$$[E : F] = \deg p \iff E = F[p]$$

אם m ראשוני ו $F = \mathbb{Q}$ אז $[E : F] = n - 1 = \deg p$

III. $f = \lambda^n - p \in \mathbb{Q}[\lambda]$ כאשר p מספר ראשוני. $\sqrt[n]{p}$ שורש של f . לכן $\mathbb{Q}[\sqrt[n]{p}] \subseteq E$.
השורשים כולם הם $\rho^i \sqrt[n]{p}$, $0 \leq i < n$.

$$E = \mathbb{Q}[\rho, \sqrt[n]{p}], \rho = \frac{\rho \sqrt[n]{p}}{\sqrt[n]{p}} \in E$$

הערות

I. אם $f \mid g$ ו- f מתפצל אז g מתפצל.

הוכחה: $hg = f = (\lambda - a_1) \cdots (\lambda - a_n)$ לכך $g = (\lambda - a_{i_1}) \cdots (\lambda - a_{i_t})$ לאיזשהם i_1, \dots, i_t .

II. אם a שורש של f בתוך $E \supset K$ ו- E שדה פיצול של f מעל F אז $f = (\lambda - a_1)g \in F$ מעל K ו- E שדה פיצול של g מעל K .

III. אם $F \subset K \subset E$ ו- E שדה פיצול של f מעל E אז גם E שדה פיצול של f מעל K .

טענה (משפט)

נניח E_1, E_2 שדות פיצול של f מעל F . אז $E_1 \cong E_2$ כ- F -אלגברות.

משפט יותר כללי

אם $\varphi : F_1 \rightarrow F_2$ איזומורפיזם של שדות ו- $f = \sum_{i=0}^n \alpha_i \lambda^i \in F_1[\lambda]$ אז $f_\varphi = \sum \varphi(\alpha_i) \lambda^i \in F_2[\lambda]$ ו- E_1 שדה פיצול של f מעל F_1 ו- E_2 שדה פיצול של f_φ מעל F_2 אז $E_1 \cong E_2$ כ-אלגברות.

למה

נניח ש- f_φ מתפצל בתוך L_2 . שדה ההרחבה של F_2 ו- $F_1 \rightarrow F_2$ הומומורפיזם של שדות.

הוכחת הלמה

ניקח a_1 שורש של f . כלומר שורש של g , כאשר g גורם אי פריק של f . $g_\varphi \mid f_\varphi$ כי L_2 מתפצל בתוך L_2 ו- $f_\varphi = g_\varphi h_\varphi$ (אם $f = gh$ אז $f_\varphi = g_\varphi h_\varphi$). יש לו שורש b_1 . יש הומומורפיזם הצבה לגבי $\varphi : F[\lambda] \rightarrow L_2$ לפי $\lambda \mapsto b_1$ ו- $\sum \varphi(\alpha_i) b_1^i = \sum \alpha_i \lambda^i = 0$.

$$\ker \psi = \left\{ h = \sum \alpha_i \lambda^i \mid h_\varphi(b_1) = \sum \varphi(\alpha_i) b_1^i = 0 \right\}$$

אבל $g \in \ker \psi$ לפי בחירת b_1 . לכן יש הומומורפיזם $F[\lambda]/F[\lambda]g \rightarrow L_2$. כאשר $F[a_n] = F[\lambda]/F[\lambda]g \rightarrow L_2$ שורש של g . הוכחנו את הלמה ולכן את המשפט.

שאלה הבאה

נניח $L_1 = L_2 = E$ שדה הפיצול של f . אז כמה אוטומורפיזמים- F של E אפשר לקבל? $|\text{Gal}(E/F)| = ?$

¹ גם אם $\deg g = 1$ - אז g כבר מפוצל, וזה נחשב שהוא פולינום מתפצל.

נשים ♡: בהוכחה שלחנו a_1 שורש של g לתמונה $g = g_\varphi$ כי $\varphi = 1$. מספר הבחירות הוא מספר השורשים בתוך E (מס' הבחירות הוא $\deg g$, ויש שוויון אם אין שורש כפול של g).

בסיכום, מספר הבחירות \geq מכפלת הממדים של ההרחבות המינימליות בכל שלב, וזה שווה ל:

$$[E : K_{n-1}] [K_{n-1} : K_{n-2}] \cdots [K_2 : F] = [E : F]$$

מסקנה

נניח E שדה פיצול של פולינום f מעל שדה F . אז $|\text{Gal}(E/F)| \leq [E : F]$, ויש שוויון כאשר אין ל f שורש כפול ב E .