

1) (2) במסלול סיום:

באופן כללי, נניח שיש לנו תחום -

$$t: G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

$$t(\sigma) = l + n\mathbb{Z} \quad (l \text{ זוגי})$$

$$\sigma(\zeta) = \zeta^l \quad \text{אם } l \text{ זוגי}$$

2) נניח כי עבור $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ נקבע

3) נניח: אם $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

$$\sigma(\zeta) = \zeta^l$$

3) נניח: אם $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

אם $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

$$\sigma(\zeta) = \zeta^l \quad \sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$$

$$\sigma(\zeta) = \zeta^l \quad \sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$$

$$\sigma(\zeta) = \zeta^l \quad \sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$$

4) נניח כי $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

5) נניח כי $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

6) נניח כי $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

$$\sigma(\zeta) = \zeta^l$$

7) נניח כי $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

$$\langle \zeta^l \rangle = \mu_n(\mathbb{C})$$

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^l)$$

8) נניח כי $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

$$\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$$

9) נניח כי $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

10) נניח כי $\sigma \in G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ אז $\sigma(\zeta) = \zeta^l$ כאשר l זוגי.

לול $\mathbb{Q}$ $\mathbb{E}$ $\mathbb{F}$ $\mathbb{F}^p$ בגאומטריה

במילוי, (ניח): $(\omega, f + \omega)$

כיון $\mathbb{E}$ $\mathbb{F} \mid x^n - 1$

נקרא $\mathbb{F} \mid x^n - 1$

כצבור $\mathbb{Z}[x]$ הוא תחום פריק יחיד

לפני $\mathbb{Z}$ $\mathbb{Z}[x]$ איננו אינדיבידואליזציה של $\mathbb{Z}$

כבר איננו יכולים להגיד כי $\mathbb{Z}$ הוא פריק, משום

לכן, איננו יכולים להגיד כי $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

אין צורך להוכיח את הטענה הזו, אלא להשתמש בה

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

אין צורך להוכיח את הטענה הזו, אלא להשתמש בה

כיון $\mathbb{E}$ $\mathbb{F} \mid x^n - 1$

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

הוא פריק, כלומר $\mathbb{Z}$ הוא פריק

לול

ענין: F שיהי מברקטוויסט'ה q (זאגן). ויהי

p. 25 n

$K = F(\zeta)$, $F \subseteq K$ — נורמלית: $\zeta^2 = -1$ ולכן $K = F(\sqrt{-1})$.

-! ז שורש מו' נ' ט' ב' ו' א' | שורש ה' , ח' ט' ז' ב' -

הצגה: כי F היא הצגה $(F-S)$ החדה

$F_p \subset F$ גרען דאן נישט, F_p איז ~~א~~

$$K = F(\mathbb{F}_p(\zeta))$$

ז"ל - $F_p \supset F_p(\zeta_p)$ הכתובת היא, כי $\zeta_p \in F_p$

$$G_{K/F} = G_{F(\mathbb{F}_p\{\zeta\})/F} \cong G_{\mathbb{F}_p\{\zeta\}/F \cap \mathbb{F}_p\{\zeta\}}$$

האברהם

החברות
~~החברות~~ - כל"ס $F_p(y), F_p(z) \cap F$ - ע"י

התאריך 17/12/2019

שאלה: ה' F , n זכר , F לך Co'ק' F

במקרה זה $K \neq F$ וזהו המקרה הראשון.

המשפט של פאלי

$$\mu_n = \mu_n(\bar{F}) \subset F, \quad n \geq 0, \quad n \in \mathbb{N}$$

e. פ'פ'ק, פ'ר'ב נ נ נ נ נ כ'נ כ'נF ג'כ

$$K = F(a) \quad \text{---} \quad a^n \in F \quad \text{---} \quad \therefore a \in K$$

$K = F(\sqrt[n]{b})$ $a = \sqrt[n]{b}$ $a^n = b \in F$ F ist ein rest

$$a^n = b \in F - \{0\} \Rightarrow K = F(a) \text{ is a field}$$

$$X^n - b = X^n - a^n = \prod_{\zeta \in \mu_n} (X - \zeta a)$$

אם $\mathcal{F}$ הוא סדרה של פונקציות f_n על X ו- f פונקציה על X כך ש-

הפונקציה U הפסדית: X^n וכן KDF המחרטת.

ברור כי $\sigma \in G_{K/F}$ קבץ $\sigma(a)$, שכן a זרע F .

$\text{pr}(a^n = b \Rightarrow \sigma(a^n) = \sigma(b) = b \Rightarrow \sigma(a)^n = b) \quad \chi^n = b \in \mathbb{Q}$

$$X^n - b, [K:F] = n \text{ and } \forall \sigma \in \text{Gal}(K/F), \sigma(a) = \zeta a$$

$X^2 - b$ הוא הפולינום האי-פריימיטיבי של $\sqrt{b}$ ב- F .
 נכונות: $\sigma \in \text{Aut}(F)$ אם ורק אם $\sigma(\sqrt{b}) = \pm \sqrt{b}$.
 נניח $\sigma \in \text{Aut}(F)$ ונניח $\sigma(\sqrt{b}) = \zeta \sqrt{b}$ עבור $\zeta \in F$.
 אז $\sigma^2(\sqrt{b}) = \sigma(\zeta \sqrt{b}) = \zeta \sigma(\sqrt{b}) = \zeta^2 \sqrt{b}$.
 מכאן $\sigma^2 = \text{id}$ ולכן $\sigma \in G_{K/F}$.
 הפוך: אם $\sigma \in G_{K/F}$ אז $\sigma(\sqrt{b}) = \pm \sqrt{b}$.

$$G_{K/F} = \{ \sigma_\zeta \mid \zeta \in \mu_n \}$$

נניח $\sigma \in G_{K/F}$ ונניח $\sigma(\sqrt{b}) = \zeta \sqrt{b}$.
 אז $\sigma^2(\sqrt{b}) = \sigma(\zeta \sqrt{b}) = \zeta \sigma(\sqrt{b}) = \zeta^2 \sqrt{b}$.
 מכאן $\sigma^2 = \text{id}$ ולכן $\sigma \in G_{K/F}$.

$$\sigma_{\zeta_1 \zeta_2}(a) = \zeta_1 \cdot \zeta_2 \cdot a = \zeta_1 (\zeta_2 a) = \sigma_{\zeta_1}(\sigma_{\zeta_2}(a))$$

$$G_{K/F} \cong \mu_n = \{ \zeta \mid \zeta^n = 1 \}$$

נניח $K = F(\sqrt[n]{a})$ ונניח $\sigma \in G_{K/F}$. אז $\sigma(\sqrt[n]{a}) = \zeta \sqrt[n]{a}$ עבור $\zeta \in \mu_n$.
 אז $\sigma^n(\sqrt[n]{a}) = \zeta^n \sqrt[n]{a} = \sqrt[n]{a}$ ולכן $\sigma^n = \text{id}$.

$$G_{K/F} = \{ \text{id}_K, \sigma, \sigma^2, \dots, \sigma^{n-1} \}$$

נניח $\sigma \in G_{K/F}$ ונניח $\sigma(\sqrt[n]{a}) = \zeta \sqrt[n]{a}$. אז $\sigma^n(\sqrt[n]{a}) = \sqrt[n]{a}$.
 נניח $t \in K$ ונניח $t = \sum_{i=0}^{n-1} \zeta^i \sigma^i(\sqrt[n]{a})$.

$$\text{id}_K + \zeta \sigma + \zeta^2 \sigma^2 + \dots + \zeta^{n-1} \sigma^{n-1} \neq 0$$

$$0 \neq a \stackrel{\text{מכאן}}{=} t + \zeta \sigma(t) + \zeta^2 \sigma^2(t) + \dots + \zeta^{n-1} \sigma^{n-1}(t)$$

$$\sigma(a) = \sigma(t) + \zeta \sigma^2(t) + \zeta^2 \sigma^3(t) + \dots + \zeta^{n-1} \sigma^n(t)$$

$$= \zeta^{-1} (t + \zeta \sigma(t) + \zeta^2 \sigma^2(t) + \dots + \zeta^{n-1} \sigma^{n-1}(t)) = \zeta^{-1} a$$

$x^2 + bx + c = 0 \quad (1) \quad : \quad \frac{1}{\sqrt{b^2 - 4ac}}$
 $\mathbb{Q} \subset \mathbb{Q}(b, c) \subset \mathbb{Q}(b, c, \sqrt{b^2 - 4ac})$
 $\uparrow$
 $"\mathbb{C}_0"$

$x^3 + px + q = 0 \quad \text{p.e. (2)}$
 $\mathbb{Q}(p, q) \subset \mathbb{Q}(p, q, \zeta_3) \subset \mathbb{Q}(p, q, \zeta_3, \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}) \subset$
 $\mathbb{Q}(p, q, \zeta_3, \sqrt{D}) \subset \mathbb{Q}(p, q, \zeta_3, \sqrt{D}, \sqrt[3]{\frac{q}{2} + \sqrt{D}}) \subset$
 $\mathbb{Q}(p, q, \zeta_3, \sqrt{D}, \sqrt[3]{\frac{q}{2} - \sqrt{D}})$
 $\uparrow$
 $\frac{1}{2} + i\frac{\sqrt{3}}{2}$