

02.01.14

תורת גִּבְעָה וְתַּחֲנוּן

12 סדרת הנקודות ותבניות

הוכחההוכחה של מילוי קבוצת הנקודות $G_i \subset G_{i+1}$ ב- G .

$$1 = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_t = G$$

הוכחה של מילוי קבוצת הנקודות G_{i+1}/G_i ב- $G_i \times G_{i+1}$ ב- R^1 .הוכחה של מילוי קבוצת הנקודות K/F ב- \mathbb{A}^n $F = F_t \subset F_{t-1} \subset F_{t-2} \subset \dots \subset F_0 = K$ מילוי מושג של קבוצת הנקודות \Leftrightarrow מילוי $\text{Gal}(K/F)$.הוכחה של מילוי קבוצת הנקודות F_i/F_{i+1} ב- $F_i \times F_{i+1}$ ב- R^1 .הוכחההוכחה של מילוי קבוצת הנקודות G_{i+1} ב- $G_i \times G_{i+1}$ ב- R^1 .הוכחה של מילוי קבוצת הנקודות E/F ב- $E_i \times E_{i+1}$ ב- R^1 .

$$k = k^{(1)} \supset k^{(2)} \supset k^{(3)} \supset \dots \supset k^{(t)} = F \quad \Leftrightarrow \quad 1 = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_t = G_0$$

$$\text{Gal}(F_i/F_{i+1}) = G_{i+1}/G_i, \quad \forall i$$

הוכחה

$$n = [E:F], \quad E = F(\sqrt[n]{a}) \quad \text{מילוי } E/F$$

מילוי \Leftrightarrow מילוי E/F ב- $E_i \times E_{i+1}$, $f_i: E_i \rightarrow E$ ב- R^1 .הוכחה של מילוי קבוצת הנקודות $F(\alpha) \in F[\alpha]$ ב- F ב-הוכחה.הוכחה של מילוי K ב- R^1 .הוכחה של מילוי קבוצת הנקודות $G = \text{Gal}(K/F)$ ב- K/F ב-הוכחה.
מילוי $G \Leftrightarrow$ מילוי קבוצת הנקודות $\text{Gal}(F_i/F_{i+1})$ ב- $F_i \times F_{i+1}$ ב- R^1 .הוכחההוכחה של מילוי קבוצת הנקודות G ב- K \Leftrightarrow מילוי G .מילוי $=$ מילוי n , $n \geq r$ מילוי קבוצת הנקודות \mathbb{A}^r ב- \mathbb{A}^n .(� $\geq n$). $\ell \geq r$ מילוי קבוצת הנקודות \mathbb{A}^r ב-הוכחה. $\Leftrightarrow \ell \geq r$ מילוי קבוצת הנקודות \mathbb{A}^r ב- K .

↪

$$|F| = p^n$$

$\mathbb{Z}_p \subseteq F \Leftrightarrow p > 0 \text{ und } \int_{\mathbb{Z}_p}^0 \text{ ist ein } \mathbb{Z}_p\text{-Modul}$, $\mathbb{Z}_p \cong \mathbb{Z}^n$

↪

Ende

↪

$G \leq G'$: $\forall g \in G \exists g' \in G' \text{ mit } g = g' \cdot s_n$

$\forall g \in G \exists g' \in G' \text{ mit } g = g' \cdot s_n \Rightarrow g' = g \cdot s_n^{-1}$

? $\text{Gal}(K/\mathbb{Q}) = G$

$\forall g \in G \exists g' \in G' \text{ mit } g = g' \cdot s_n \Rightarrow g' = g \cdot s_n^{-1}$

Ende

$K(x_1, \dots, x_n) \subseteq K(x_1, \dots, x_n)$: $\forall i \in \{1, \dots, n\}$

$x_i \in K(x_1, \dots, x_n)$

$\forall i < j \exists \sigma \in S_n \text{ mit } \sigma(i) = j$

$\forall \sigma \in S_n \exists \sigma' \in S_n \text{ mit } \sigma' \circ \sigma = \text{id}$

$K(x_1, \dots, x_n) = K(x_{\sigma(1)}, \dots, x_{\sigma(n)})$

$\forall i \in \{1, \dots, n\}$

$\forall \sigma \in S_n \exists \sigma' \in S_n \text{ mit } \sigma' \circ \sigma = \text{id}$ \Leftrightarrow $\forall \sigma \in S_n \exists \sigma' \in S_n \text{ mit } \sigma' \circ \sigma = \text{id}$

$\forall \sigma \in S_n \exists \sigma' \in S_n \text{ mit } \sigma' \circ \sigma = \text{id}$ \Leftrightarrow $\forall \sigma \in S_n \exists \sigma' \in S_n \text{ mit } \sigma' \circ \sigma = \text{id}$

Ende

$\forall \sigma \in S_n \exists \sigma' \in S_n \text{ mit } \sigma' \circ \sigma = \text{id}$

$\forall \sigma \in S_n \exists \sigma' \in S_n \text{ mit } \sigma' \circ \sigma = \text{id}$ \Leftrightarrow $\forall \sigma \in S_n \exists \sigma' \in S_n \text{ mit } \sigma' \circ \sigma = \text{id}$

$\forall \sigma \in S_n \exists \sigma' \in S_n \text{ mit } \sigma' \circ \sigma = \text{id}$

↪

四

$\cdot p^n$ ביאר נזר נרע

$$K \text{ is } \mathbb{F}_p \text{ if } \exists x \in K \text{ such that } f(x) = 0 \Leftrightarrow \exists x \in K \text{ such that } x^{p^n} - x = 0$$

$$\{x \in K \mid x^{p^n} = x\}$$

לעומת (הנורווגית) מילויים נורווגיים נורווגית (הנורווגית)

[*(éle nens) són leu wiś, kó t mén, p ojścia wek b rat*]

$(x^{p^n} - x)$ lebt über \mathbb{F}_{p^n}

八月二日

Pⁿ 318,0 138 ke 103

$$\alpha^{(k-3)l} = \alpha^{p^n-1} = 1$$

, oždele ří

$$r \in \mathbb{K} \text{ with } \alpha^{p^n} = 2$$

$$\therefore \lambda - \lambda^{\infty} \approx \text{neglible} \quad k = 1$$

Siogn fe òil le wib

- PRACTICALLY 30 30 30,000 30

$$P^n \otimes_{\mathbb{Z}} \mathbb{Z}/p \text{ mod } = \mathbb{F} P^n : P^n$$

$$? \overline{F}_{p^n} \subseteq \overline{F}_{p^m} \quad \text{un : } \underline{\text{def}}$$

$$\text{nlm } \rho_{\mathbb{F}_p} : \mathbb{F}_{p^n} \text{ Lcan in } \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n} \leq \mathbb{F}_{p^n} \text{ RT}$$

$$(n = [\mathbb{F}_{p^n} : \mathbb{F}_p] \mid [\mathbb{F}_{p^m} : \mathbb{F}_p] = m) \quad)$$

$$\left(\frac{x^m - 1}{x^n - 1} = 1 + x + x^{2n} + \dots + x^{m-n} \right) \quad x^{m-1} \mid x^m - 1 \quad \text{since } n \mid m \quad n \geq 1$$

$$x^{p^n} - x \mid x^{p^m} - x \iff x^{p^n-1} \mid x^{p^m-1} - 1 \quad \text{由定理}$$

$$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$$

$$x^{p^n} - x^{p^m} \text{ is even } (\downarrow)$$

. $|F|=q$ (1) , ו/or F , F ck נו: אלגברה נורמלית

$$\cdot \phi(\alpha) = \alpha^q \quad \text{so} \quad \phi: k \rightarrow k \quad (2)$$

$\text{char } k = \text{char } F = p \Rightarrow q = p^n \rightarrow$ גזע ל' IND ס

$$\cdot \alpha = \beta \leftarrow \alpha - \beta = 0 \leftarrow (\alpha - \beta)^q = 0 \leftarrow \alpha^q - \beta^q = 0 \leftarrow \alpha^q = \beta^q \quad \text{מן } \phi$$

. תוליך פס) If ϕ SK מדו' ל' זר

$$\cdot \phi \in \text{Gal}(k/F), \underline{\alpha \in F} \text{ or } \alpha^q = \alpha \quad -\ell \quad (3)$$

$$\cdot |\text{Gal}(k/F)| = [k:F] = d \quad , |F| = q \quad , |k| = q^d \quad (4)$$

? $i \leq d$ ו/ז $\phi^i - \alpha$ גזע מודול גזע AND

$$|\alpha^{\phi^i}| \leq q^i < q^d \quad \Leftrightarrow \quad \alpha \mapsto \alpha^{q^i}$$

($\forall i < d$)

$\Rightarrow \phi$ גזע מדו' $\Leftrightarrow 0 < i < d$ So $\phi^i + 1 \Leftarrow$

$$\cdot d \in \text{ker Gal}(k/F)$$

$$\cdot \text{Gal}(k/F) = \langle \phi \rangle \quad \Leftarrow$$

. גזע מודול \cong מודול $\mathbb{F}_p[x]/\langle f \rangle$ - ℓ פונקציונליות

. n מודול k מודול \mathbb{F}_p ב- ℓ מודול \mathbb{F}_p

. n מודול \mathbb{F}_p מודול \mathbb{F}_p ב- ℓ מודול \mathbb{F}_p \Leftarrow

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/\langle f \rangle \quad \Leftarrow$$

(f מודול \mathbb{F}_p מודול \mathbb{F}_p מודול \mathbb{F}_p)

: מילון

$$\frac{x^4 - \lambda}{x^2} = \lambda(\lambda+1)(\lambda^2 + \lambda + 1)$$

. \mathbb{F}_2 מודול מודול מודול \mathbb{F}_4 מודול \mathbb{F}_4

$$\begin{array}{c} \text{מונומיאים} \\ x^2 \\ \hline x^2 \end{array} \left[\begin{array}{c} x^2 \\ x^2 + 1 \\ \hline x^2 + x \end{array} \right] = \begin{array}{c} (\lambda+1) \\ \text{מונומיאים} \\ \lambda+1 \end{array}$$

$$\text{מונומיאים} \leftarrow x^2 + \lambda + 1$$

$$\mathbb{F}_4 \cong \mathbb{F}_2[x]/\langle x^2 + \lambda + 1 \rangle$$

$$\mathbb{F}_8 \cong \mathbb{F}_2[x]/\langle x^3 + x^2 + 1 \rangle \quad : \mathbb{F}_8$$

$$\mathbb{F}_8 \cong \mathbb{F}_2[x]/\langle x^3 + x^2 + 1 \rangle$$