

שיעור 1

ספר: A course in arithmetic
J. P. Serre

פרק טו: גשטalt דינאמיקה

בנקטיות של תבניות חלופיות סופיות

בשורה: G - תבנית חלופית סופית, בנקטיות של G
 $\chi: G \rightarrow \mathbb{C}^*$ הוא איזומורפיזם
 $\chi(ab) = \chi(a)\chi(b)$

למנה

① נניח כי $|G| = n$, אז $\chi(G) \subseteq \mu_n$ (תבניות μ_n)
 $\mu_n = \{e^{\frac{2\pi i k}{n}} \mid k \in \mathbb{Z}\}$ שורשי היחידה מסדר n .

② קבוצת הבנקטיות של G היא תבנית גיחס לכל סתם-קבוצה:
 $(\chi_1 \chi_2)(a) = \chi_1(a) \chi_2(a)$
 תבנית זו משמשת כי $\hat{G} =$ התבנית הדואלית של G .

הוכחה

③ לכל $a \in G$ $a^n = 1$ ולכן $\chi(a^n) = \chi(1) = 1$
 $\Rightarrow \chi(a)^n = 1$
 ולכן $\chi(a) \in \mu_n$.

② $\chi_1 \chi_2$ הוא כרך

$$(\chi_1 \chi_2)(ab) = \chi_1(ab) \chi_2(ab) = \chi_1(a) \chi_1(b) \chi_2(a) \chi_2(b) \\ = (\chi_1 \chi_2)(a) (\chi_1 \chi_2)(b)$$

לפי הניחוי: $\chi_0 \equiv 1$

$$\chi^{-1}(a) = \chi(a^{-1}) \quad \text{לפי הניחוי}$$

דוגמה

G גורם ציקלי מסדר n , $G = \langle a \rangle$

כרך χ של G נקבע ביחידות $\chi(a) = e^{\frac{2\pi k i}{n}}$: $\chi(a)$: $0 \leq k \leq n-1$

$$\chi(a^j) = e^{\frac{2\pi k i j}{n}} \quad \text{לפי}$$

המשפט

ההמראה $\chi \mapsto \chi(a)$ היא איזומורפיזם של גורמים

$$(\hat{G} \cong \mu_n \text{ (כחול)}) \quad \hat{G} \cong G \quad \text{(לפי)} \quad \hat{G} \cong \mu_n$$

הוכחה

$$f(\chi_1 \chi_2) = (\chi_1 \chi_2)(a) = \chi_1(a) \chi_2(a) = f(\chi_1) f(\chi_2)$$

$$\text{לפי } f: \chi(a) = 1 \text{ ולפי } f: \chi(a) = 1 \\ \forall j \quad \chi(a^j) = \chi(a)^j = 1$$

$$\Rightarrow \chi = 1$$

$$w = e^{\frac{2\pi i k}{n}}, \quad w \in \mu_n \quad \text{for } f$$

$$\chi: G \rightarrow \mathbb{C}^* \quad \text{for}$$

$$\chi(a^j) = w^j$$

$$\chi(a) = w \quad \text{for}$$

G is a group, $H \leq G$ is a subgroup. χ is a character of G . $\chi|_H$ is a character of H .

$$p: \hat{G} \rightarrow \hat{H}$$

$$p(\chi) = \chi|_H$$

p is a surjective homomorphism.

$$p(\chi_1 \chi_2) = (\chi_1 \chi_2)|_H = \chi_1|_H \chi_2|_H = p(\chi_1) p(\chi_2)$$

$$\ker(p) = \{ \chi \in \hat{G} \mid \chi|_H = 1 \} = \{ \chi \in \hat{G} \mid \forall h \in H, \chi(h) = 1 \}$$

for

$$G/H \quad \text{for } \chi \in \ker(p)$$

$$\bar{\chi}(gH) = \chi(g)$$

G/H is a group, η is a character of G/H . χ is a character of G .

$$\chi(g) = \eta(gH)$$

$\ker p$ is a subgroup of $\hat{G}$.

$$\ker p = \widehat{G/H}$$

למה

φ חזר, כלומר φ מרכזי H שכן φ מרכזי G .

כוכב

באמצעות $[G:H]$ ש

לפי $[G:H] = 1$ אז $H = G$ ואין מה לדבר.

נניח $[G:H] > 1$, נבחר איברי $x \in G \setminus H$.
 יהי n המספר הקטן ביותר כך ש: $x^n \in H$.
 אז: $n = o(xH)$

יהי $\chi \in \hat{H}$, נסמן $t = \chi(x^n)$. נבחר איברי $h \in H$ ונקרא לו w .

נסמן $H' = \langle H, x \rangle$ - המכונה המצומצמת ביותר
 וזו, x , איברי H' איננו בקו.

$$h \cdot x^j, j \in \mathbb{Z}, h \in H$$

$$\chi: H' \rightarrow \mathbb{C}^*$$

$$\chi'(h \cdot x^j) = \chi(h) w^j$$

χ' מוגדר היטב.

$$h_1 x^{j_1} = h_2 x^{j_2} \quad \text{אז}$$

$$\Rightarrow x^{j_1 - j_2} = h_1^{-1} h_2 \in H$$

$$\int \chi(h) dh = 0 \quad \text{אם } j_1 \neq j_2$$

$$(\alpha \in \mathbb{Z}) \quad j_1 = j_2 + \alpha n \quad \text{כאשר}$$

$$\begin{aligned} \chi(h_2) \omega^{j_1} &= \chi(h_2) \omega^{j_2 + \alpha n} = \chi(h_2) (\omega^n)^\alpha \omega^{j_2} = \chi(h_2) t^\alpha \omega^{j_2} = \\ &= \chi(h_2) \chi(x^n) \omega^{j_2} = \chi(h_2) \chi(x^{j_1 - j_2}) \omega^{j_2} = \chi(h_2) \chi(h_2^{-1} h_2) \omega^{j_2} \\ &= \chi(h_2) \omega^{j_2} \end{aligned}$$

$$\Rightarrow \chi(h_2) \omega^{j_1} = \chi(h_2) \omega^{j_2}$$

$$: H' \text{ על } \gamma \text{ כי } \chi'$$

$$\begin{aligned} \chi'((h_2 x^{j_1})(h_2 x^{j_2})) &= \chi'(h_2 h_2) \omega^{j_1 + j_2} = \chi(h_2) \chi(h_2) \omega^{j_1} \omega^{j_2} \\ &= \chi'(h_2 x^{j_1}) \chi'(h_2 x^{j_2}) \end{aligned}$$

$$\text{אם } [G: H'] < [G: H], \quad H' \neq H \quad \text{כאן } \chi' \text{ אינו } \chi \text{ על } \gamma$$

$$\{1\} \rightarrow \widehat{G_H} \xrightarrow{\alpha} \widehat{G} \xrightarrow{\beta} \widehat{H} \rightarrow \{1\}$$

$$\text{אם } \alpha \text{ אינו מונומורפיזם}$$

$$\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}$$

$$\text{אם } \alpha$$

$$\alpha: \widehat{G_1 \times G_2} \rightarrow \widehat{G_1} \times \widehat{G_2} \quad \text{אם } \alpha$$

$$\alpha(\chi) = (\chi_1, \chi_2)$$

$$\chi_1(g_1) = \chi(1, g_1), \quad \chi_2(g_2) = \chi(g_2, 1) \quad \text{אם } \alpha$$

α הומומורפיזם:

$$\alpha(\chi\chi') = ((\chi\chi')_1, (\chi\chi')_2) = (\chi_1\chi'_1, \chi_2\chi'_2) = (\chi_1, \chi_2)(\chi'_1, \chi'_2) = \alpha(\chi)\alpha(\chi')$$

α הה"א: אם $\alpha(\chi) = (1, 1)$ אז:

$$\chi(g_1, g_2) = \chi(g_1, 1) \cdot \chi(1, g_2) = \chi_1(g_1) \chi_2(g_2) = 1$$

$$\Rightarrow \chi = 1$$

α הר:

אם $\eta \in \hat{G}_1, \xi \in \hat{G}_2$, נגדיו:

$$\chi(g_1, g_2) = \eta(g_1) \xi(g_2)$$

ואז נקרא $\alpha(\chi) = (\eta, \xi)$, $G_1 \times G_2$

$$(\chi = \eta \otimes \xi \text{ אינדיקטור מסתנה})$$

מסקנה:

$$\hat{G} \cong G$$

הוכחה:

ידיע כי G אוטומורפיזם למכנה ישרה של גבוהה ציקליות.

$$\hat{G} \cong \widehat{G_1 \times \dots \times G_n} \cong \hat{G}_1 \times \dots \times \hat{G}_n \cong G_1 \times \dots \times G_n \cong G$$

הערה: האיזומורפיזם $\hat{G} \cong G$ ידוע "קלאסי", כי הוא כיוון ההפך.
 של וצורה $a_1, \dots, a_n \in G$ כך של: $G = \langle a_1, \dots, a_n \rangle$.
 יש משמעות ב: $e^{2\pi i \frac{\cdot}{n}} \mapsto a_j$

נכון

$$\hat{G} \cong G$$

כאן יש "הומומורפיזם" ε

$$\varepsilon: G \rightarrow \hat{G} \quad ; \quad \text{הומומורפיזם}$$

$$(\varepsilon(g))(x) = \chi(g)$$

$\varepsilon(g)$ הוא כינוי ל- $\hat{G}$

$$\begin{aligned} (\varepsilon(g))(x_1 x_2) &= \chi(x_1 x_2) = \chi(x_1) \chi(x_2) = \varepsilon(g)(x_1) \varepsilon(g)(x_2) \\ &= (\varepsilon(g))(x_1) \cdot (\varepsilon(g))(x_2) \end{aligned}$$

ε הוא הומומורפיזם:

$$\begin{aligned} \varepsilon(g_1 g_2)(x) &= \chi(g_1 g_2) = \chi(g_1) \chi(g_2) = \\ &= (\varepsilon(g_1))(x) (\varepsilon(g_2))(x) = (\varepsilon(g_1) \varepsilon(g_2))(x) \end{aligned}$$

ε חזק:

$$(\varepsilon(g))(x) = 1 \quad \forall x \in \hat{G} \quad \text{אם } \varepsilon(g) = 1 \quad \text{כלומר } \chi(g) = 1$$

$$\Rightarrow \chi(g) = 1 \quad \forall x \in \hat{G}$$

אם $g \neq 1$, אז $\chi(g) \neq 1$ כלומר $\varepsilon(g) \neq 1$

$$\hat{H} \cong \mu_n \quad \text{אם } H \text{ סגור וחסום}$$

כלומר $\chi(g) \neq 1$ לכל $g \in \hat{H}$ ו- $\chi(g) = 1$ לכל $g \notin \hat{H}$

$$\chi(g) \neq 1 \quad \text{אם } (x) \in G$$

לפי ε חזק

$$|\hat{G}| = |G| \quad \text{כלומר } \varepsilon \text{ חזק}$$

$$S(G) = \{f: G \rightarrow \mathbb{C}\} \simeq \mathbb{C}^n$$

$(f_1, f_2)(g) = f_1(g) + f_2(g)$ (הכנסה נוקדית) C כוון וקטורי
 $(\lambda f)(g) = \lambda(f(g))$ כפל סקלרי

$$\dim_{\mathbb{C}} S(G) = |G|$$

$$G = \{g_1, \dots, g_n\}$$

$$f \mapsto (f(g_1), \dots, f(g_n))$$

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)}$$

המכנה הנירמול מסתדר

טענה

$\hat{G}$ היא קבוצת הוויכוחים של $S(G)$.

כל $\chi_1, \chi_2 \in \hat{G}$ הם

$$\frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = \delta_{\chi_1, \chi_2}$$

הוכחה

$$(*) \quad \sum_{g \in G} \chi(g) = \begin{cases} 0 & \chi \neq 1 \\ |G| & \chi = 1 \end{cases} \quad \chi \in \hat{G}$$

נניח כי $\chi \in \hat{G}$

נניח כי $\chi \neq 1$, נבחר $x \in G$ כך ש $\chi(x) \neq 1$

$$\chi(x) \left(\sum_{g \in G} \chi(g) \right) = \sum_{g \in G} \chi(x) \chi(g) = \sum_{g \in G} \chi(xg) =$$

$\sum_{h \in G} \chi(h) = \sum_{g \in G} \chi(g)$

$\chi(xg) \sim \chi(h)$ כי $h = xg$ וכל $h \in G$ יכול להיכתב בצורה הזו

$$\overset{0}{\neq} (\chi(x) - 1) \left(\sum_{g \in G} \chi(g) \right) = 0 \quad \text{לפי}$$

$$\Rightarrow \sum_{g \in G} \chi(g) = 0$$

$$\chi_2(g) = \overline{\chi_2(g)} \quad \text{כי } |\chi_2(g)| = 1 \quad \text{לפי}$$

$$\Rightarrow \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = \sum_{g \in G} (\chi_1 \chi_2^{-1})(g) = |G| \delta_{\chi_1, \chi_2}$$

לפי

$$\frac{1}{|G|} \sum_{x \in G} \chi(g_1 g_2^{-1}) = \delta_{g_1, g_2} \quad g_1, g_2 \in G \quad \text{לפי}$$

$$\hat{G} \text{ חיבור } (*) \quad \text{לפי}$$

$$\frac{1}{|\hat{G}|} \sum_{\chi \in \hat{G}} \alpha(\chi) = \delta_{\alpha, 1}$$

$$g \in G, \quad \alpha = \varepsilon(g) \quad \text{לפי}$$

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \varepsilon(g)(\chi) = \delta_{\varepsilon(g), 1}$$

$$\Rightarrow \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(g) = \delta_{g, 1} \quad (\text{לפי } \varepsilon)$$

$$g = g_1 g_2^{-1} \quad \text{לפי}$$

$$|\mathbb{Z}_m^*| = \phi(m), \quad G = \mathbb{Z}_m^* \quad \text{קבוצה}$$

$$(\text{לפי } p_1, \dots, p_n) \quad m = p_1^{k_1} \dots p_n^{k_n} \quad \Rightarrow \quad \text{לפי}$$

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_n^{k_n}}$$

$$r + m\mathbb{Z} \xrightarrow{f} (r + p_1^{k_1}\mathbb{Z}, \dots, r + p_n^{k_n}\mathbb{Z})$$

ה'י' צמצום מרחב - הומומורפיזם ההפיכה הקבוצה

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{p_1^{k_1}}^* \times \dots \times \mathbb{Z}_{p_n^{k_n}}^*$$

f מוגדר היטב

f הומומורפיזם של חבורות (חזית)

f חזית $\Leftrightarrow$ $\ker f$ חבורה - חזית

לפי $(1 \leq j \leq n)$ $x_j \in \hat{\mathbb{Z}}_{p_j^{k_j}}$

$$\chi(r + m\mathbb{Z}) = \chi_1(r + p_1^{k_1}\mathbb{Z}) \cdot \dots \cdot \chi_n(r + p_n^{k_n}\mathbb{Z})$$

מחרוזת ביקטורי כללי של $\mathbb{Z}_m^*$ (קבוצת המספרים הקטנים יותר מ-m וחסרי גורמים משותפים עם m)

דוגמה

בבילי של $\mathbb{Z}_m^*$ יקרה גם ביקטור מורחב מ

$\mathbb{Z}_{p^k}^*$ ביקטור - כחור, כחור (חזית)
(יוצר ביקטור קטן שיהיה חבורה מורחבת p^k)

דוגמה

בתורו המספרים מובנים כי הם g הוא שיהיה חבורה

מורחב p כך $g \not\equiv 1 \pmod{p^2}$ $g^{p-1} \not\equiv 1 \pmod{p^2}$
אם g הוא שיהיה חבורה מורחבת p חזית $1 \leq k$

$$p=5 \quad 2 \text{ הוא שיהיה חבורה מורחב } 5 \quad \phi(5)=4 \quad 2^2 \equiv -1 \pmod{5}$$

$$2^4 \equiv 16 \not\equiv 1 \pmod{25}$$

לפי 2 הוא שיהיה חבורה מורחבת 5^k לכן k

$$\mathbb{Z}_{5^k}^* = \langle 2 \rangle, \quad \phi(5^k) = 4 \cdot 5^{k-1}$$

כדי ש $\mathbb{Z}_{5^k}^*$ יהיה ציקלי

$$\chi_p(2) = e^{\frac{2\pi i \cdot 1}{4 \cdot 5^{k-1}}}$$

$$\chi_p(2^j + 5^k \mathbb{Z}) = e^{\frac{2\pi i \cdot j}{4 \cdot 5^{k-1}}}$$

מכאן נובע

$$\text{ל } \mathbb{Z}_p^* \quad |\mathbb{Z}_p^*| = p-1 \quad \text{ע"פ } p \geq 3$$

2. χ_p הוא חבורת יחידים מודולו p

$$\left(\begin{array}{l} \chi_p^2 = 1 \\ \chi_p \neq 1 \end{array} \right) \quad \chi_p \text{ הוא כונומי יחיד } \chi_p \text{ מודולו } p, \quad \mathbb{Z}_p^* \cong \hat{\mathbb{Z}}_p^*$$

$$\chi_p \cdot \chi_p : x \mapsto \chi_p(x)^2 = \chi_p(x^2)$$

לכן χ_p נמצא בכונומי יחידים

$$\mathbb{Z}_p^* / (\mathbb{Z}_p^*)^2 \rightarrow \text{חבורת מודולו } 2$$

הפרקטיקה היא לכתוב את היחידים של חבורה זו

$$(\mathbb{Z}_p^*)^2 \mapsto 1$$

$$\mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2 \mapsto -1$$

$$\text{Legendre} \quad \chi_p(x) = \left(\frac{x}{p} \right) \equiv x^{\frac{p-1}{2}} \pmod{p}$$

נניח כי m הוא אי-זוגי. נגדיר χ_m על ידי:

$$\mathbb{Z} \ni n \mapsto \left(\frac{n}{m} \right) = \prod_{i=1}^r \left(\frac{n}{p_i} \right)^{k_i}$$

$$p_1^{k_1} \dots p_r^{k_r}$$

קבוצת המספרים מובנית $\mathbb{Z}_{2^k}^*$ היא תת-קבוצה של $\mathbb{Z}_{2^k}$ כאשר $k \geq 3$.
מובנית לפי h ו- 5 .

$$(3 \leq k \text{ זוגי}) \quad n^{2^{k-2}} \equiv 1 \pmod{2^k}$$

וכן מובנית 5 ו- 2^{k-2} (מובנית 2^k)
(מובנית בזיוק 2^k) $5^{2^{k-2}} \equiv 1 + 2^{k-1} \pmod{2^k}$ לפי $2^{k-2} \mid a(5)$

ומכאן:

$$\mathbb{Z}_{2^k}^* = \left\{ 5^j + 2^k \mathbb{Z} \right\}_{j=1}^{2^{k-2}} \cup \left\{ -5^j + 2^k \mathbb{Z} \right\}_{j=1}^{2^{k-2}}$$

לכל j מובנית 5^j ו- -5^j מובנית 2^k

$$\Rightarrow \mathbb{Z}_{2^k}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$$

Gen

י"א a חופשי מריבועים, $m \equiv 4 \pmod{a}$, m זוגי
כל קיים בתוך מובנית m עם המבנה:

$$\chi_a(p) = \left(\frac{a}{p} \right)$$

$\chi_p^2 = 1$; $m-1$ זוגי p ראשוני
~~לכל $a \neq 1$ ש- $\chi_a \neq 1$~~

הוכחה

המובנית n של n זוגי, $m-1$ זוגי, $n = p_1^{k_1} \dots p_r^{k_r}$
לכל $p_j \nmid m$ ראשוני שונה מ- n ש- χ_a זוגי

$$\chi_a(n) = \prod_{j=1}^r \chi_a(p_j)^{k_j} = \prod_{j=1}^r \left(\frac{a}{p_j} \right)^{k_j} = \left(\frac{a}{n} \right)$$

$$\chi_a(h) = \chi_a((m-1)h) = \left(\frac{a}{(m-1)n} \right)$$

[illegible]

תלמוד: יום ה' ט"ז, ח' ט"ז, ז' ט"ז, ו' ט"ז.
מקום זה מן התורה

$$\left(\frac{a}{n}\right) = (-1)^{\frac{1}{2}(a-1)(n-1)} \left(\frac{n}{a}\right)$$

$\int_0^1 \frac{1}{x} dx = \ln 1 - \ln 0 = 0 - (-\infty) = \infty$

$$\chi_a(h) = (-1)^{\frac{a-1}{2}} (a-1)(n-1) \left(\frac{n}{a} \right)$$

in 1812 1675 1815

167 ~~167~~ $h \mapsto \binom{n}{h}$ 2178 120