Лекция №8 «Характеры. Суммы Гаусса». Курс A-I

Кучерин Георгий Дмитриевич 619/2

28 октября 2025

Везде G - конечная абелева группа

Определение 1. *Характером* G *называется голом* $\chi : G \to \mathbb{C}^*$ (*то есть* $\chi-$ *функция* $\chi(gh) = \chi(g)\chi(h), \quad \chi(e) = 1$)

Лемма 1. *Множество характеров* G *является конечной абелевой группой*
$\square \quad |G| = K \Rightarrow g^K = e$
$\chi(g^K) = \chi(g)^K = 1$
$|\chi(g)| = 1 \quad (\chi : G \to U : \quad \{z : |z| = 1\})$
$\chi_0 : \quad \forall g \in G \quad \chi_0(g) = 1$
$(\chi_1, \chi_2)(g) = \chi_1(g)\underline{\chi_2(g)}$
$1 = |\chi(g)|^2 = \chi(g)\overline{\chi(g)}$
$\Rightarrow \chi^{-1} = \overline{\chi} \qquad \blacksquare$

Определение 2. $\widehat{G}$ *называется двойственной к* G

Примеры. *1)* $\psi(x) = e^{2\pi i \frac{x}{p}}, \quad x \in \mathbb{F}_p$
$\psi(x+y) = e^{2\pi i \frac{x}{p}} e^{2\pi i \frac{y}{p}}$
2)$\mathbb{F}_p^* \quad \chi(x) = (\frac{x}{p})-$*символ Лежандра (тоже характер мультипликативной группы)*

Определение 3. $\chi_0 \equiv 1$ *называется тривиальным главным,* $\chi \neq \chi_0$ *неглавным*

Лемма 2. *Если* G *- циклическая (конечная)* $|G| = n, \quad G = <g>$
$\forall \chi \in \widehat{G}$ *имеет вид* $: \quad \exists K : \quad 0 \leq k \leq n-1 \quad \chi_K(g^j) = e^{2\pi i \frac{Kj}{n}} \quad 0 \leq j \leq n-1$
$\chi = \chi_K \qquad \widehat{G} \cong G$
$\square g^n = e \quad \chi(g)^n = 1$
$\chi(g) = e^{2\pi i \frac{K}{n}} \quad 0 \leq K \leq n-1$
$\chi_K^n = \chi_0$
$\chi_K -$ *различны между собой*
$\chi_1(g^j) = e^{2\pi i \frac{j}{n}} -$ *образующ* $\widehat{G} \qquad \blacksquare$

Теорема 1. $\forall G -$ *конечн абелев группы* $\widehat{G} \cong G$
$\square$ (*набросок доказательства*) *факт из алгебры* :
$G \cong G_1 \cdots \times G_r, \quad$ *где* $G_i -$ *циклические,* $|G_i| = p^{a_i}$
$n = \prod_{i=1}^r p^{a_i} \quad \ldots \qquad \blacksquare$

Лемма 3. $H < G, \quad \forall\psi \quad \psi \in \widehat{H} \Rightarrow \exists\chi \in \widehat{G}: \quad \chi|_H = \psi$ *(то есть* $\forall h \in H$
$\chi(h) = \psi(h))$
$\square \quad a \in G \setminus H, \quad a \neq e$
$H_1 =< a, H >$
Пусть m *– порядок* $[a]$ *в* $G \setminus H$
$\forall g \in H: \quad g = a^j h \quad 0 \leq j \leq m-1 \quad h \in H$
$\psi(a^m) = \eta \in \mathbb{C}^*,$ *то есть возьмем* $\zeta: \quad \zeta^n = \eta$
$\psi_1(g) = \zeta^j \psi(h) \quad g' = a^K h'$
$\psi_1(gg') = \psi_1(a^{j+K}) =$
для случая $j + K < m$
$\psi_1(gg') = \psi_1(a^{j+K}) = \zeta^{j+K}\psi(h)\psi(h') = \psi_1(g)\psi_1(g')$
для случая $j + K > m$
$\psi_1(gg') = \psi_1(a^{j+K}) = \psi_1(a^{j+K-m}a^m hh') = \zeta^{j+K-m}\zeta^m\psi(h)\psi(h') = \psi_1(g)\psi_1(g')$
$G \setminus H_1 \ni a_2 \neq e \quad \ldots \quad \blacksquare$

Следствие. $\forall g \in G \setminus \{e\} \quad \exists\chi \in \widehat{G} \quad \chi(g) \neq 1$
$\square \quad H =< g > \quad \forall\psi \in \widehat{H} \quad \psi = \psi_K$
$\psi_K(g^j) = e^{2\pi i \frac{Kj}{n}} \quad \psi_1(g) = e^{2\pi i \frac{1}{n}} \neq 1 \qquad \blacksquare$

по лемме: $\exists\chi : \chi|_H = \psi_1$
χ – искомый характер

Теорема 2. *G - конечная абелева* $|G| = n$
$\sum_{g\in G} \chi(g) = \begin{cases} n, & \chi = \chi_0 \\ 0, & \chi \neq \chi_0 \end{cases}$
$\sum_{\chi\in \widehat{G}} \chi(g) = \begin{cases} n, & g = 0 \\ 0, & g \neq 0 \end{cases}$
$\square \quad 1) \quad \chi = \chi_0$ *– очевидно*
$\chi \neq \chi_0$
$\exists g_0 \neq e: \quad \chi(g_0) \neq 1$
$\chi(g_0)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(g_0 g) = \sum_{g\in G}\chi(g)$
$(1 - \chi(g_0))\sum_{g\in G}\chi(g) = 0$ *(первое* $\neq 0,$ *второе* $= 0)$
2) *доказывается по аналогии, только в этом случае двойственная картина*
$(g \in G$ *опред* $\widehat{g}: \quad \widehat{g} = \chi(g), \quad \widehat{g} \in \widehat{G}) \qquad \blacksquare$

Следствие.

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\,\overline{\psi(g)} = \begin{cases} 1, & \text{\textit{если} } \chi = \psi \\ 0, & \text{\textit{если} } \chi \neq \psi \end{cases}$$

Двойственное равенство

$$\frac{1}{|\widehat{G}|}\sum_{x\in \widehat{G}}\chi(g)\,\overline{\chi(h)} = \begin{cases} 1, & \text{если } g = h \\ 0, & \text{если } g \neq h \end{cases}$$

Характеры для $\mathrm{F}_q, \quad \mathbb{F}_q^*$
$\mathbb{F}_p \quad \psi(x) = e^{2\pi i \frac{x}{p}}$

Лемма 4. $\forall$ *аддитивн характер* ψ *группы* $\mathbb{F}_q$ *имеет вид:*
$\psi = \psi_\beta, \quad \psi_\beta(x) = e^{2\pi i \frac{Tr(\beta x)}{p}}$

$\square \quad \psi_\beta \in \widehat{\mathbb{F}_q}$
$\psi = \psi_1 \quad \exists x: \quad Tr \quad x \neq 0$
то есть ψ_1 – *неглавный*
$\psi_\alpha \neq \psi_\beta, \quad$ *если* $\alpha \neq \beta$
$\frac{\psi_\alpha(x)}{\psi_\beta(x)} = \psi(\alpha x - \beta x) \neq 1$
то есть q *различных характеров* ψ_α
$\Rightarrow \forall \psi \in \widehat{\mathbb{F}_q} \quad \exists \alpha : \psi = \psi_\alpha \quad \blacksquare$

Лемма 5. $F_q^* =< \eta >, \quad \forall \chi \in \widehat{\mathbb{F}_q^*}$ *имеет вид* $\chi = \chi_j$, *где* $\chi_j(\eta^K) = e^{2\pi i \frac{jK}{\eta - 1}}$
$\square$ *из леммы выше* $\blacksquare$

Лемма 6. $s\,|q-1, \quad \mathbb{F}_q^* =< \eta >$

$$1) \quad \sum_{\chi^s=\chi_0} \chi(a) = \begin{cases} s, & a \in (\mathbb{F}_q^*)^s \quad (\exists x : x^s = a) \\ 0, & a \notin (\mathbb{F}_q^*)^s \quad (\exists x : x^s = a) \\ 1, & a = 0 \end{cases}$$

$(\chi(0) = 0)$
2) *Если* $\chi^s = \chi_0 \quad (\chi \neq \chi_0)$
$\sum_{j=0}^{s-1} \chi(\eta^j) = 0$
$\square \quad G = \mathbb{F}_q^*, \quad H = (\mathbb{F}_q^*)^s = \{y \in \mathbb{F}_q : \quad y = x^s\}$
$|G| = q - 1$
$s|q-1. \quad \chi^s = \chi_0$
$\exists \chi_1 \in \widehat{G/H} : \quad \chi_1([a]) = \chi(a) \quad (\chi_1$ *индуцирует характер* $\chi)$
G/H – *циклическая*
$|G/H| = \frac{|\mathbb{F}_q^*|}{|(\mathbb{F}_q^*)^s|} = \frac{q-1}{(\frac{q-1}{s})} = s$
1) *если* $a \neq 0$

$$\sum_{\chi^s=\chi_0} \chi(a) = \sum_{\chi_1 \in \widehat{G/H}} \chi_1([a]) = \begin{cases} s, & [a] = a \\ 0, & \text{если } a \text{ не } \quad s - \text{той степени} \end{cases}$$

2) $G/H = \{1, \eta, \ldots, \eta^{s-1]}\} \sum_{j=0}^{s-1} \chi(\eta^j) = \sum_{g \in G/H} \chi(g) = 0 \quad \blacksquare$

Замечание. $F_q, \quad s = 2$
$\sum_{\chi^s=\chi_0} \chi(a) = 1 + (\frac{a}{p}) = N(x^2 = a)$ – *число решений уравнения*

Общий случай:
$\sum_{\chi^s=\chi_0} \chi(a) = N(x^s = a)$ (в следующий раз)

Суммы Гаусса

Определение 4. χ – *мультипликативный характер* $\mathbb{F}_p \quad (\chi \in \widehat{\mathbb{F}_p^*})$

$\mathrm{G}_a(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x) e^{2\pi i \frac{ax}{p}}$ – сумма Гаусса

Теорема 3. *Если* $\chi \neq \chi_0, \quad a \neq 0$
$(p|a), \quad$ *то тогда* $|G_a(x)| = \sqrt{p}$
$\square \quad F = \{f : \mathbb{F}_p \to \mathbb{C}\}$
$(f, g) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} f(x) \overline{g(x)}$
$\psi_a(x) = e^{2\pi i \frac{ax}{p}} \quad (\psi_a)$ – *ортонормированный базис* $a \in \mathbb{F}_p$

$\chi \in F \Rightarrow \chi = \sum_{a\in\mathbb{F}_p} \alpha_a\psi_a, \quad \alpha_a = (\chi, \psi_a) = \frac{1}{p}\sum_{c\in\mathbb{F}_p} \chi(x)e^{2\pi i\frac{ax}{p}} = \frac{1}{p}G_a(\chi)$
$\exists c \in \mathbb{F}_p^* : \quad \chi(c) \neq 1$
$\chi(xc^{-1}) = \chi(x)\chi(c^{-1}) = \sum_a \alpha_a\chi(c^{-1})\psi_a(x)$
$\chi(xc^{-1}) = \chi(x)\chi(c^{-1}) = \sum_a \alpha_a\psi_a(xc^{-1}) = \sum_{a\in\mathbb{F}_p} \alpha_a\psi_{ac^{-1}}(x) = [ac^{-1} = b] = \sum_{b\in\mathbb{F}_p} \alpha_{bc}\psi_b(x)$
$(\psi_a) - \textit{базис} \Rightarrow \alpha_a\chi(c^{-1}) = \alpha_{ac}$
$\alpha_a = \chi(c)\alpha_{ac}$
$\textit{Если} \quad \textit{при} \quad a = 1 : \quad |\alpha_1| = |\alpha_c|$
$\textit{при} \quad a = 0 : \quad \alpha_0 = \chi(c)\alpha_0 \quad (\chi c \neq 1) \Rightarrow \alpha_0 = 0$
$(\chi, \chi) = \frac{1}{p}\sum_{x\in\mathbb{F}_p} \chi(x)\overline{\chi(x)} = \frac{p-1}{p}$
$(\chi, \chi) = (\sum_{a\neq 0} \alpha_a\psi_a, \sum_{a\neq 0} \alpha_a\psi_a) = \sum_{a\neq 0} |\alpha_a|^2 = (p-1)|\alpha_1|^2$
$\Rightarrow |\alpha_c|^2 = |\alpha_1|^2 \quad (\textit{этот вывод мы сделали ранее}) \quad = \frac{1}{p} \quad |\alpha_c| = |\alpha_1| = \frac{1}{\sqrt{p}}$
$|\frac{1}{p}G_a(x)| = \frac{1}{\sqrt{p}} \Rightarrow |G_a(\chi)| = \sqrt{p} \qquad \blacksquare$

Замечание. $/G_a(\chi)|^2 = G_a(\chi)\overline{G_a(\chi)}$

Определение 5. *для* F_q *сумма Гаусса* $G(\chi, \psi) = \sum_{x\in\mathbb{F}_q} \chi(x)\psi(x)$
где χ, ψ *– мултиплик, аддитивн,* $\chi(0) = 0$

Теорема 4. *1)* $\chi \neq \chi_0, \quad \psi \neq \psi_0$
$|G(\chi, \psi)| = \sqrt{q}$
2) $G(\chi_0, \psi_0) = q - 1$
$G(\chi_0, \psi \neq \psi_0) = -1$
$G(\chi \neq \chi_0, \psi_0) = 0$
3) $G(\chi, \overline{\psi}) = \chi(-1)G(\chi, \psi)$

Теорема 5. $F_p^2 \quad \chi(\cdot) = (\frac{\cdot}{p})$
$$G_1(\chi) = \begin{cases} \sqrt{p}, & p \equiv 1(4) \\ i\sqrt{p}, & p \equiv 3(4) \end{cases}$$

Теорема 6. *(Соотношение Хассе Девинхорта)* $F_{q^s}/\mathbb{F}_q \quad N_{\mathbb{F}_{q^s}/\mathbb{F}_q}$
$Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}$
χ, ψ *– аддитивные характеры* $\mathbb{F}_q$
$\chi' = N_{\mathbb{F}_{q^s}/\mathbb{F}_q} \circ \chi$
$\psi' = Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q} \circ \psi$
$G(\chi', \psi') = (-1)^{s-1}G(\chi, \psi)^s$