Charaktery a Gaussovy součty

Nechť $(G, \cdot)$ je komutativní grupa. Každý grupový homomorfismus

$$\chi : (G, \cdot) \to (\mathbb{C}, \cdot)$$

se nazývá *charakter* grupy G. Dále budeme uvažovat pouze konečné grupy G.

Charaktery tvoří také grupu, s násobením definovaným

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g) \cdot \chi_2(g).$$

Jednotkovým prvkem této grupy charakterů je identická jednička, kterou značíme ε a nazýváme *triviálním* charakterem.

Věta. Nechť je X grupa charakterů konečné komutativní grupy G. Pak

$$X \cong G.$$

Důkaz. Protože je G konečná, musejí se všechny její prvky zobrazovat na jednotkovou kružnici. Přesněji, prvek g se musí zobrazovat na r-tou odmocninu z 1, kde r je řád prvku g. Máme tedy

$$\chi(g) = \exp(2\pi i \frac{k}{r}),$$

pro nějaké $k \in \mathbb{Z}_r$.

Nechť $\{g_1, \ldots, g_m\}$ je nějaká minimální množina generátorů grupy G, kde prvek g_j má řád r_j. Pak

$$G \cong \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_m}$$

a charakter χ je jednoznačně určen volbou

$$(k_1, \ldots, k_m) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_m}$$

tak, že

$$\chi(g_j) = \exp\left(2\pi i \frac{k_j}{r_j}\right).$$

Je snadné ověřit, že zobrazení $\chi \mapsto (k_1, \ldots, k_m)$ dává požadovaný isomorfismus. □

Vzhledem k tomu, že se pohybujeme na jednotkové kružnici, platí

$$\chi^{-1}(g) = \chi(g)^{-1} = \overline{\chi(g)}.$$

Lemma. Pro libovolný netriviální charakter χ grupy G platí

$$(\diamond) \qquad \sum_{g \in G} \chi(g) = 0.$$

Pro triviální charakter ε platí

$$\sum_{g \in G} \varepsilon(g) = |G|.$$

Důkaz. Nechť je χ netriviální, a zvolme $h \in G$ tak, že $\chi(h) \neq 1$. Protože $g \mapsto hg$ je permutace grupy G, dostáváme

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

a tedy

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

Tvzení o triviálním charakteru je zřejmé. □

Podobný výsledek platí pokud fixujeme prvek grupy:

Lemma. Pro libovolný prvek $g \neq 1$ grupy G platí

$$(\diamond\diamond) \qquad \sum_{\chi \in X} \chi(g) = 0.$$

Platí

$$\sum_{\chi \in X} 1 = |G|.$$

Důkaz. Z výše uvedeného isomorfismu G a X plyne, že pro $g \neq 1$ existuje charakter γ splňující $\gamma(g) \neq 1$. Pak podobně jako v předchozím lemmatu dostáváme

$$\sum_{\chi \in X} \chi(g) = \sum_{\chi \in X} (\gamma \cdot \chi)(g) = \gamma(g) \sum_{\chi \in X} \chi(g),$$

a tedy

$$\sum_{\chi \in X} \chi(g) = 0.$$

Pro $g = 1$ tvrzení plyne z $|G| = |X|$. □

Nechť je nyní $G = \mathbb{Z}_n^*$. Pak mluvíme o *Gaussových charakterech* modulo n. *Gaussovým součtem* Gaussova charakteru χ modulo n je hodnota

$$g(\chi) := \sum_{k \in \mathbb{Z}_n^*} \chi(k)\, \omega_n^k,$$

kde

$$\omega_n = \exp\left(\frac{2\pi i}{n}\right)$$

je primitivní n-tá odmocnina z jedné.

Lemma. Pro netriviální Gaussův charakter χ modulo prvočíslo p platí

$$|g(\chi)| = \sqrt{p}.$$

Důkaz. Chceme ověřit, že $g(\chi) \cdot \overline{g(\chi)} = p$. Protože $\overline{\chi(\ell)} = \chi(\ell^{-1})$ a $\overline{\omega_p}^{\ell} = \omega_p^{-\ell}$, dostáváme

$$g(\chi) \cdot \overline{g(\chi)} = \left(\sum_{k \in \mathbb{Z}_p^*} \chi(k)\omega_p^k\right) \cdot \left(\sum_{\ell \in \mathbb{Z}_p^*} \chi(\ell^{-1})\omega_p^{-\ell}\right) = \sum_{k,\ell \in \mathbb{Z}_p^*} \chi(k\ell^{-1})\omega_p^{k-\ell}.$$

Hodnota $z = k\ell^{-1}$ probíhá celé $\mathbb{Z}_p^*$, přičemž pro zvolené z dostaneme $p-1$ sčítanců odpovídajících dvojicím $(z\ell, \ell)$. Vytkneme-li tedy $\chi(z)$ dostáváme

$$g(\chi) \cdot \overline{g(\chi)} = \sum_{z \in \mathbb{Z}_p^*} \left(\chi(z) \cdot \sum_{\ell \in \mathbb{Z}_p^*} \omega_p^{\ell(z-1)}\right).$$

Pro $z = 1$ dostáváme

$$1 \cdot \sum_{\ell \in \mathbb{Z}_p^*} \omega_p^0 = p - 1.$$

Pro $z \neq 1$ máme

$$\chi(z) \cdot \sum_{\ell \in \mathbb{Z}_p^*} (\omega_p^{z-1})^{\ell}.$$

Uvažme nyní charakter γ grupy $(\mathbb{Z}_p, +)$, nikoli tedy $(\mathbb{Z}_p^*, \cdot)$, daný vztahem $\gamma(1) = \omega_p^{z-1}$. Ze vztahu $(\diamond)$ máme

$$0 = \sum_{\ell \in \mathbb{Z}_p} \gamma(\ell) = 1 + \sum_{\ell \in \mathbb{Z}_p^*} \gamma(\ell).$$

Tedy

$$\sum_{\ell \in \mathbb{Z}_p^*} \omega_p^{\ell(z-1)} = -1.$$

Podobnou úvahou, tentokrát pro grupu $(\mathbb{Z}_p^*, \cdot)$, dostáváme

$$\sum_{\substack{z \in \mathbb{Z}_p^* \\ z \neq 1}} \chi(z) = -1.$$

Celkem tedy

$$g(\chi) \cdot \overline{g(\chi)} = (p-1) - \sum_{\substack{z \in \mathbb{Z}_p^* \\ z \neq 1}} \chi(z) = (p-1) + 1 = p.$$

□

Uvědomme si, že vlastnosti Legenderova symbolu dělají ze zobrazení

$$k \mapsto \left(\frac{k}{p}\right)$$

homomorfismus. Je to tedy charakter grupy $\mathbb{Z}_p^*$. Příslušný Gaussův součet

$$S := \sum_{k \in \mathbb{Z}_p^*} \left(\frac{k}{p}\right) \omega_p^k$$

se nazývá *kvadratický Gaussův součet* modulo p. Pro důkaz kvadratické reciprocity je důležitá následující vlastnost S.

Lemma.

$$S^2 = \left(\frac{-1}{p}\right) p.$$

Důkaz. Rozdělíme-li součet do dvojic podle komplexně sdružených čísel ω_p^k a ω_p^{-k}, dostáváme

$$S = \sum_{1 \leq k \leq \frac{p-1}{2}} \left(\frac{k}{p}\right) \left(\omega_p^k + \left(\frac{-1}{p}\right) \omega_p^{-k}\right).$$

Je-li $\left(\frac{-1}{p}\right) = 1$, vidíme, že S je reálné číslo

$$r := \sum_{1 \leq k \leq \frac{p-1}{2}} 2 \left(\frac{k}{p}\right) \mathrm{Re}(\omega_p^k).$$

Z předchozího lemmatu víme, že $|S| = \sqrt{p}$, takže $r = \pm\sqrt{p}$ a $S^2 = p = \left(\frac{-1}{p}\right) p$.

Pokud naopak $\left(\frac{-1}{p}\right) = -1$, dostáváme $S = i \cdot r'$, kde

$$r' = \sum_{1 \leq k \leq \frac{p-1}{2}} 2 \left(\frac{k}{p}\right) \mathrm{Im}(\omega_p^k)$$

a opět $r' = \pm\sqrt{p}$. Tedy i v tomto případě můžeme psát $S^2 = -p = \left(\frac{-1}{p}\right) p$.

□