

1. Bevezetés

A következő félévben tervezem karakterösszegek használatát arra vonatkozólag, hogy a diszkrét logaritmus, más néven index mennyire jól közelíthető (esetleg többváltozós) polinomfüggvénnyel. Ezért idén a diszkrét logaritmus tanulmányozása mellett a karakterösszegekben is elmélyedtem. Tehát az egyéni kutatómunka 2 tantárgy keretein belül főleg a karakterekkel foglalkoztam. Az összefoglaló során a tételeket és állításokat bizonyítások nélkül fogom ismertetni.

2. Karakterek

Az additív és multiplikatív karakterek bevezetéséhez először ismertetem a csoport karakterek fogalmát, és néhány tulajdonságát. Emellett szükség lesz még a karakterek jellemzéséhez egy fontos számelméleti függvényre, amely a következő:

2.1. Definíció. Legyen $e(\alpha) = e^{2\pi i \alpha}$, és legyen $e_m(\alpha) = e^{2\pi i \frac{\alpha}{m}} = e(\frac{\alpha}{m})$.

Itt $e(\alpha)$ csak α törtrésztől függ, és $e(\alpha)$ periodikus, 1 periódushosszal. Ez könnyen látható, az $f : \mathbb{R} \rightarrow \mathbb{C}$, $f(t) = e^{it} = \cos t + i \sin t$ vizsgálatával, amely periodikus, és periódushossza 2π .

2.1. Csoport karakterek

A csoport karaktereket csak véges Ábel csoportokra fogom bevezetni. Általános csoportok karakterére nem lesz szükségem a diszkrét logaritmus későbbi vizsgálata során, így azokat nem ismertetem. Két fontos eset: $G_1 = \langle \mathbb{Z}_m, + \rangle$, és $G_2 = \langle \mathbb{Z}_m^*, \times \rangle$, ahol G_1 a $\text{mod } m$ maradékosztályok additív csoportja, és G_2 a $\mathbb{Z}_m$ redukált maradékosztályainak multiplikatív csoportja. Előbbi esetben a csoport karakter additív karakter, míg az utóbbiban multiplikatív karakter.

2.2. Definíció. Legyen G véges Ábel csoport. Ekkor $\chi : G \rightarrow \mathbb{C}$ csoport karakter G -n, ha teljesíti az alábbiakat:

1. χ nem azonosan nulla G -n
2. $\forall g_i, g_j \in G : \chi(g_i g_j) = \chi(g_i) \chi(g_j)$

A következő 3 állítás a karakter definíciójának a következménye.

2.3. Állítás. *Legyen χ karakter G -n, és legyen G egységeleme u . Ekkor*

1. $\chi(u) = 1$
2. $\forall g \in G : (\chi(g))^{|G|} = 1$

2.4. Állítás. 1. *Legyen $\chi_0 : G \rightarrow \mathbb{C}$ olyan, hogy $\forall g \in G : \chi_0(g) = 1$. Ekkor χ_0 egy karakter G -n, melyet triviális karakternek vagy főkarakternek hívunk.*

2. *Legyen χ karakter G -n, ekkor χ konjugáltja is karakter G -n, és a következő módon értelmezzük: $\bar{\chi} : G \rightarrow \mathbb{C}$, ahol $\forall g \in G : \bar{\chi}(g) = \overline{\chi(g)}$. Ezt nevezzük konjugált karakternek.*

3. *Két karakter szorzata is karakter: legyenek χ_1, χ_2 karakterek G -n. Ekkor a $\chi(g) := \chi_1(g) \chi_2(g) \forall g \in G$ módon definiált χ is karakter G -n.*

4. *Legyen $G = G_1 \times G_2$. Ekkor χ karakter G -n $\Leftrightarrow$ ha létezik χ_1 karakter G_1 -en és χ_2 karakter G_2 -n, melyekre $\forall g = g_1 g_2 \in G : \chi(g) = \chi_1(g_1) \chi_2(g_2)$. A fordított irány szintén triviális.*

Megjegyzés. Legyen G véges Ábel csoport. Ekkor a G -n értelmezett karakterek csoportot alkotnak a szorzásra nézve. Az egység a triviális karakter, és egy karakter inverze a karakter konjugáltjával egyezik meg.

2.5. Állítás. 1. *Legyen $G = C_n = \{g\}_n$ n -edrendű ciklikus csoport. Ekkor χ karakter G -n $\Leftrightarrow$ ha $\exists a \in \{0, 1, \dots, n-1\} : \chi(g^k) = e(k \frac{a}{n}) \forall k \in \mathbb{Z}$.*

2. *Legyen $G = C_{n_1} \times C_{n_2} \times \dots \times C_{n_r}$, ahol C_{n_i} n_i -rendű ciklikus ($i = 1, 2, \dots, r$). Ekkor a G -n értelmezett χ karakterek explicit alakja: $\chi(g_1^{k_1}) \dots g_r^{k_r} = e(k_1 \frac{a_1}{n_1} + \dots + k_r \frac{a_r}{n_r})$, ahol $a_i \in \{0, 1, \dots, n_i-1\}$, $i = 1, 2, \dots, r$. Ha itt $a_i = 0 \forall i$, akkor $\chi = \chi_0$.*

3. *A G -n definiált különböző karakterek száma $|G|$.*

A következő állítás az eddigi állítások, és a karakterek alapdefiníciójának a következménye.

2.6. Állítás. 1. Legyen G egy véges Ábel csoport, és legyen χ G egy karaktere. Ekkor

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{ha } \chi = \chi_0, \\ 0 & \text{ha } \chi \neq \chi_0. \end{cases}$$

2. $\forall g \in G :$

$$\sum_{\chi} \chi(g) = \begin{cases} |G| & \text{ha } g = 1, \\ 0 & \text{ha } g \neq 1. \end{cases}$$

2.7. Tétel. Legyen G egy véges Ábel csoport, valamint $g, g_1, g_2, \dots, g_t \in G$, ahol lehet két g_i azonos is. Ekkor

$$|\{i : 1 \leq i \leq t, g_i = g\}| = \frac{1}{|G|} \sum_{\chi} \bar{\chi}(g) \sum_{i=1}^t \chi(g_i).$$

2.2. Additív karakterek

Rögzítsünk egy m és k egész számot. Ekkor a korábbiak szerint $\mathbb{Z}_m$ -en egy χ karakter leírható az alábbi módon:

$$\chi(k) = e\left(k \frac{a}{m}\right),$$

ahol $a \in \{0, 1, \dots, m-1\}$. Itt valójában k alatt a k által reprezentált maradékosztályt értjük, melyet jelölhetünk $\bar{k}$ -val, és az alábbi módon definiáljuk:

$$\bar{k} = \{g \in \mathbb{Z} : g \equiv k \pmod{m}\}.$$

Az előző fejezetben ismertetett 2.3, 2.4, 2.5, 2.6 állítások mind kimondhatók az additív karakterekre is.

2.8. Definíció. Legyen $A \subset \mathbb{Z}$ véges. Ekkor

$$f(t) = \sum_{a \in A} e(at)$$

az A halmaz generátorfüggvénye, vagy más néven Fourier transzformáltja.

Megjegyzés. Látható, hogy a korábban bevezetett $e(\alpha)$ függvény valóban egy fontos számelméleti függvény. Segítségével definiáljuk egy halmaz Fourier transzformáltját. Az $e(\frac{n}{m})$ érték csak az $n \pmod m$ értéktől függ, és így rögzített k és m mellett az $e(a\frac{k}{m})$ csak az $a \pmod m$ értéktől függ.

2.9. Tétel. Legyen $A \subset \mathbb{Z}$ véges, $r \in \mathbb{Z}$ és $m \in \mathbb{N}$. Ekkor

$$|\{a : a \in A, a \equiv r \pmod m\}| = \frac{1}{m} \sum_{k=0}^{m-1} e(-\frac{rk}{m}) f(\frac{k}{m}) = \sum_{k=0}^{m-1} e(-\frac{rk}{m}) \sum_{a \in A} e(\frac{ak}{m}).$$

2.3. Multiplikatív karakterek

A multiplikatív karaktereket, az additív karakterekhez hasonlóan a csoport karakterek segítségével definiálhatjuk. Egy multiplikatív karakteren egy csoport karakter speciális módon vett kiterjesztését értjük. Azonban csoport karakterek használata nélkül is tudjuk definiálni őket.

2.10. Definíció. Legyen $m \in \mathbb{N}$. Egy $\chi(n) : \mathbb{Z} \rightarrow \mathbb{C}$ függvényt multiplikatív karakternek nevezünk, ha létezik olyan $\mathbb{Z}_m^*$ -en definiált χ_1 csoport karakter, melyre

$$\chi(n) = \begin{cases} \chi_1(n), & \text{ha } (n, m) = 1 \\ 0, & \text{egyébként.} \end{cases}$$

2.11. Definíció. Legyen $m \in \mathbb{N}$. Egy $\chi(n) : \mathbb{Z} \rightarrow \mathbb{C}$ függvényt multiplikatív karakternek nevezünk, ha teljesíti az alábbiakat:

1. $\chi(n)$ nem azonosan nulla
2. $\forall u, v \in \mathbb{Z} : \chi(uv) = \chi(u)\chi(v)$
3. $u, v \in \mathbb{Z} : u \equiv v \pmod m \Rightarrow \chi(u) = \chi(v)$
4. $(n, m) > 1$ esetén $\chi(n) = 0$.

Megjegyzés. A két definíció ekvivalens.

Az additív karaktereknél láttuk, hogy mivel a csoport karakterekből származtatjuk őket, így az azokra kimondott állításokat ki lehet mondani az additív karakterekre is. Ugyanilyen érvelés mellett kapjuk a multiplikatív karakter alaptulajdonságait. Legyen $m \in \mathbb{N}$ és $\chi(n) : \mathbb{Z} \rightarrow \mathbb{C}$ egy multiplikatív karakter. Ekkor

1. $\chi(1) = 1$.
2. Ha $(a, m) = 1$, akkor $\chi(a)$ $\varphi(m)$ -edik egységgyök.
3. A főkaraktert a következő módon definiáljuk multiplikatív karakterek esetén:

$$\chi_0(a) = \begin{cases} 1 & \text{ha } (a, m) = 1 \\ 0 & \text{ha } (a, m) > 1. \end{cases}$$

4. Ha χ karakter, akkor annak konjugáltja is karakter, és $\overline{\chi}(a) = \overline{\chi(a)} = \chi(a^{-1})$.
5. Ha χ_1 és χ_2 karakterek, akkor azok szorzata is karakter, és $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$.
6. A $\text{mod } m$ karakterek száma $\varphi(m) = |\mathbb{Z}_m^*|$.

7.

$$\sum_{a=1}^m \chi(a) = \begin{cases} \varphi(m) & \text{ha } \chi = \chi_0, \\ 0 & \text{ha } \chi \neq \chi_0. \end{cases}$$

8.

$$\sum_{\chi \text{ mod } m} \chi(a) = \begin{cases} \varphi(m) & \text{ha } a = 1, \\ 0 & \text{ha } a \neq 1. \end{cases}$$

2.12. Tétel. Legyen $a, n_1, \dots, n_t \in \mathbb{Z}$, $m \in \mathbb{N}$ és $(a, m) = 1$. Ekkor

$$|\{i : 1 \leq i \leq t, a \equiv n_i \pmod{m}\}| = \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi}(a) \sum_{i=1}^t \chi(n_i).$$

Hivatkozások

- [1] K. Gyarmati, A. Sárközy: *Exponenciális és karakterösszegek* <https://gyarmatikati.web.elte.hu/jegyzet/expossz.pdf>
- [2] K. Conrad: *Characters of Finite Abelian Groups* <https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf>