# NYILATKOZAT

**Név:** Pataki Vilmos Ivó

**ELTE Természettudományi Kar, szak:** Matematika Bsc

**NEPTUN azonosító:** HINHKY

**Szakdolgozat címe:**
Parkettázás véges Abel csoportokon és Fourier analízis

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2021. 05. 28.

Pataki Vilmos

*a hallgató aláírása*

# Parkettázás véges Abel csoportokon és Fourier analízis

Diplomamunka

Írta: Pataki Vilmos Ivó

Matematikus szak

Témavezető:

Somlai Gábor, egyetemi adjunktus
Algebra és Számelmélet Tanszék
Eötvös Loránd Tudományegyetem, Természettudományi Kar

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2021

# Tartalomjegyzék

# Köszönetnyilvánítás

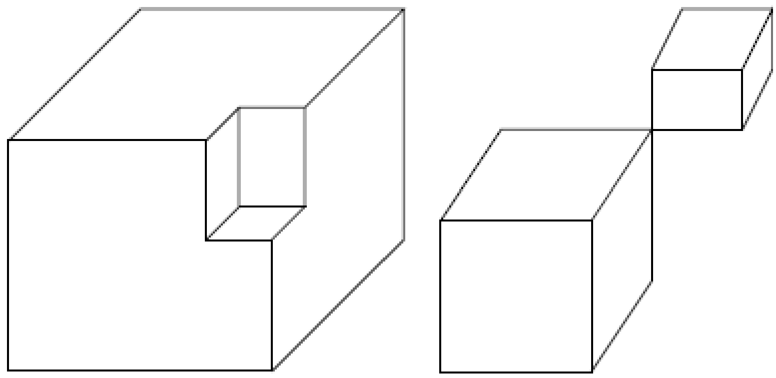
Elsősorban szeretnék köszönetet mondani témavezetőmnek, Somlai Gábornak, a rendszeres, jó hangulatú konzultációkért, hogy mindig türelmesen válaszolt kérdéseimre, és megosztotta velem az 3. fejezet ötletét. Köszönöm továbbá szüleimnek a sok éves támogatást, illetve páromnak és kisfiamnak, hogy lelkileg támogattak a dolgozat megírásában.

# Bevezetés

Ebben a részben megpróbálunk rámutatni, miért fontos a parkettázások megértése véges Abel csoportokon, különös tekintettel a véges ciklikus csoportokon, továbbá ismertetjük a Fuglede sejtést.

Tekintsük az egész számok egy $A$ véges részhalmazát. A parkettázás egy teljesen természetes definíció: $A$-t elég sokszor eltolva minden egész számot le tudunk fedni a halmazzal pontosan egyszer. A végtelen eltoló halmazt jelöljük $B$-vel. Először Hajós bizonyította be [8]-ban, hogy $B$ megválasztható úgy is, hogy $B$ periodikus legyen, azaz valamilyen $n$-re az $a \mapsto n + a$ hozzárendelés bijekció $B$-ből $B$-be. Ekkor persze $B$ $C + \mathbb{Z}/n\mathbb{Z}$ alakba írható valamilyen véges $C$ halmazra. Belátható, hogy ekkor $A + C$ halmaz teljes maradékrendszert alkot modulo $n$. Ebből pedig az következik, hogy elég megértenünk a véges ciklikus csoportokon a parkettázásokat, ahhoz hogy megértsük $\mathbb{Z}$-n.

A parkettázás definíciója kiterjeszthető $\mathbb{R}^n$-re. Itt persze nem fog minket zavarni, ha néhány pontot egyszer sem, vagy esetleg többször fedünk le, tehát nullmértékű halmazotól eltekintve kell lefednünk mindent. Azt is megköveteljük, hogy az eredeti halmaz ne legyen túl pici, vagyis pozitív Lebesgue mértékű legyen. Egyszerűbb geometria alakzatokról szemléletesen könnyen látszik, hogy parkettáznak-e vagy sem: egy kocka és egy hatszög parkettáz, a kör és a háromszög nem. Meglepő, hogy például az ábrán szereplő két alakzat is parkettáz (a képeken csak a 3 dimenziós eset szerepel, de 2-re és nagyobbakra is igaz). Az elsőt úgy kapjuk, hogy tetszőleges téglatest sarkából kivágunk valamekkora téglatestet, a másodikat pedig úgy, hogy két (különböző) téglatestet sarkaiknál egymáshoz ragasztunk. Ezt [13]-ban bizonyították



Forrás: [15]

be és a Fourier analízis eszközeit alkalmazták.

Bent Fuglede [7]-ban $\mathbb{R}^n$-re bevezette a spektralitás fogalmát. $\Omega \subset \mathbb{R}^n$ pozitív Lebesgue mértékű halmaz spektrális, ha van olyan $\Lambda$, hogy a $e^{2\pi i x \cdot \lambda}, \lambda \in \Lambda$ hatványfüggvények ortogonális bázist alkotnak $L^2(\Omega)$ Hilbert téren. Megmutatta, hogy például egy háromszög spektrális. Fuglede sejtése a következő volt: $\mathbb{R}^n$ a spektrális és parkettázó halmazok ugyanazok. Több éven keresztül próbálták az általános esetben belátni a sejtést, de csak speciális feltételek mellett születtek eredmények ([9], [10], [14], [24]). Végül 2004-ben Terence Tao [23] bebizonyította, hogy a sejtés nem igaz 5 és annál magasabb dimenzióban:

ellenpéldákat generált $\mathbb{Z}_2^{12}, \mathbb{Z}_3^5$ csoportokban, utóbbit felemelte $\mathbb{Z}^5$ 5 dimenziós rácsra, majd $\mathbb{R}^5$-re (az eljárás hasonló a magasabb dimenziós esetben). Mind a három esetben, olyan halmazokat kapott, melyek spektrálisak, de nem parkettáznak. Megjegyezzük, hogy az így nyert ellenpéldák geometriailag viszonylag egyszerűek: véges sok $[0,1)^5$ kocka $\mathbb{Z}^5$ rácspontokba eltoltjainak uniója. Kiderült, hogy ha a diszkrét esetet vizsgáljuk, abból fontos megállapításokat kaphatunk a folytonosra. Azóta megcáfolták mindkét irányt 3 és annál magasabb dimenzióban ([15] section 4). Ez persze nem jelenti, hogy ha az alakzatunk elég szép, akkor ne lenne rá igaz az állítás. Például Nir Lev és Matolcsi Máté belátták, hogy $n$ dimenziós konvex tartományokra igaz a sejtés [16].

1 és 2 dimenzióban se bizonyítani, se cáfolni nem tudták a sejtést. 1 dimenzióban viszont megmutatkozik a Fuglede sejtés jelentősége véges ciklikus csoportokon. Ugyanis, ha igaz, hogy minden parkettázó halmaz spektrális $\mathbb{Z}_n$-ben, minden $n$-re, abból egyből következik, hogy ugyanez az irány igaz $\mathbb{R}$-re is. Illetve ha bármelyik irányra találunk ellenpéldát valamilyen $\mathbb{Z}_n$-ben, akkor ez az irány nem lesz igaz $\mathbb{R}$-ben sem.

A spektralitást (értelemszerű módosításokkal) ugyanúgy lehet értelmezni véges Abel csoporton, mint a valós esetben. Magának a fogalomnak ekkor lineáris algebrai jelentése van: a spektrális halmazok és spektrumuk leírhatók, mint a csoport, úgynevezett karaktertáblájának részmátrixai. Az is ki fog derülni, hogy ezek komplex Hadamard mátrixok, azaz olyan mátrixok melyeknek koordinátái egységhosszúak és sorai ortogonálisak.

1998-ban [3]-ban Ethan Coven és Aaron Meyerowitz a körosztási polinomokkal egy elégséges feltételt adtak parkettázásra $\mathbb{Z}_n$ ciklikus csoportokon (és ezzel együtt $\mathbb{Z}$-n is), viszont megoldatlan kérdés maradt (mai napig), hogy a feltétel szükséges-e. Bebizonyították, hogy ha $n$-nek legfeljebb két különböző prímosztója van, akkor a fordított irány is igaz. Továbbá megfigyelték, hogy ha $n$ négyzetmentes, akkor $\mathbb{Z}_n$ parkettázásai "szépek", geometriai jelentés adható nekik: minden parketta $\mathbb{Z}_n$ alkalmas $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \mathbb{Z}_{p_d}$ felírásával $\{(x, y_x) : x \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \mathbb{Z}_{p_m} m \leq d\}$ alakba írható. Ezt csak később, [22] blog egy kommentjében, illetve [20]-ben bizonyították. Később az is kiderült, hogy a feltételekből következik a véges csoport spektralitása [25].

A dolgozat a következőképpen épül fel. Az 1. fejezetben a parkettázás és spektralitás alapvető tulajdonságaival foglalkozunk, felidézzük a körosztási polinomok néhány tulajdonságát, illetve felépítjük a szükséges mennyiségű reprezentációelméletet és véges Fourier analízist. A 2. fejezetben belátjuk a Coven-Meyerowitz sejtést illetve, hogy mi köze a spektralitáshoz, továbbá ismertetjük a Fuglede sejtést. A 3. és 4. fejezetben célunk hogy belássuk a Fuglede sejtést $\mathbb{Z}_{p^2}, \mathbb{Z}_{pq}$ és $\mathbb{Z}_p^2$ csoportokra, ahol $p, q$ különböző prímek. Az utolsó fejezetben pedig belátjuk, hogy $\mathbb{Z}_p^d$-ben nem igaz a sejtés ($p$ prím), ha $d = 5$, alkalmas feltételekkel $d = 4$. A dolgozatban véges Abel csoportokkal fogunk foglalkozni, de mint említettük a parkettázás és a Fuglede sejtés $\mathbb{Z}$ és $\mathbb{R}^n$ esetében is fontosak, így ezekről a függelékben ejtünk néhány szót.

# 1. fejezet

# Előismeretek

Jelölések:

- $(G, +)$ tetszőleges véges Abel csoportot.
- $L(G)$ fogja jelenteni az összes $f : G \mapsto \mathbb{C}$ függvényt.
- Tetszőleges $S \subset G$ halmazra $\mathbb{1}_S$ jelöli $S$ indikátorfüggvényét, azaz $\mathbb{1}_S(s) = 1$, ha $s \in S$, 0 egyébként.
- Tetszőleges $g \in G$ elemre bevezetjük a $\delta_g := \mathbb{1}_{\{g\}}$ jelölést.
- $A, B$ halmazokra $A + B$ a $\{a + b : a \in A,\ b \in B\}$ halmazt jelöli.

Ebben a fejezetben az alapvető ismereteken megyünk végig.

## 1.1. Konvolúció és parkettázás

**1.1.1. Definíció.** Legyen $f, h \in L(G)$. Ekkor a

$$(f * h)(t) := \sum_{g \in G} f(t - g)h(g)$$

függvényt $f$ és $h$ konvolúciójának hívjuk.

**1.1.2. Állítás.** Legyenek $f, h, g \in L(G)$ tetszőlegesek. A konvolúcióra teljesülnek a következők:

1. $f * g = g * f$
2. $(f * g) * h = f * (g * h)$
3. $\delta_0 * f = f$
4. $(f + g) * h = f * h + g * h$
5. $\delta_{s_1} * \delta_{s_2} = \delta_{s_1 + s_2} \quad s_1,\ s_2 \in G$

*Bizonyítás.* Csak 5. látjuk be a többi hasonlóan megy.

$$(\delta_{s_1} * \delta_{s_2})(t) = \sum_{g \in G} \delta_{s_1}(t - g)\delta_{s_2}(g)$$

Ez 1, ha $g = s_2$ és $s_1 = t - g = t - s_2$, azaz $t = s_1 + s_2$ valamilyen $g$-re, egyébként 0. □

**1.1.3. Következmény.** $(L(G), +, *)$ algebra $\mathbb{C}$ fölött izomorf a $\mathbb{C}[G]$ csoportalgebrával.

*Bizonyítás.* Vegyük észre, hogy tetszőleges $f \in L(G)$ előáll, mint

$$\sum_{g \in G} f(g)\delta_g$$

Ezek után már nyilvánvaló, hogy a

$$\theta : L(G) \mapsto \mathbb{C}[G] \qquad \theta(\sum_{g \in G} f(g)\delta_g) = \sum_{g \in G} f(g)x^g$$

leképezés izomorfizmus. □

**1.1.4. Állítás.** $L(G)$ vektortér $\mathbb{C}$ felett és a

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

művelet pedig skaláris szorzás.

**1.1.5. Definíció.** $A \subset G$ parkettázza $G$-t, ha létezik $B$ halmaz, hogy minden $G$-beli elem egyértelműen előáll, mint egy $A$-beli és egy $B$-beli összege. Jelölése: $A \oplus B = G$.

**1.1.6. Példa.** Legyen $H$ részcsoportja $G$-nek. Ha minden $H$ szerinti mellékosztályból kiveszünk egy reprezentánst és ezek halmazát $F$-el jelöljük, akkor $H \oplus F = G$.

**1.1.7. Állítás.** Legyen $A,\ B \subset G$. $A \oplus B = G$ akkor és csak akkor, ha $\mathbb{1}_A * \mathbb{1}_B = \mathbb{1}_G$.

*Bizonyítás.*

$$(\mathbb{1}_A * \mathbb{1}_B)(t) = \sum_{g \in G} \mathbb{1}_A(t-g)\mathbb{1}_B(g)$$

Ez pontosan akkor 1, ha egyértelműen létezik $g \in G$, amelyre $t - g \in A$ és $g \in B$. Ez minden $t$-re igaz, ami pont az előző definíció. □

**1.1.8. Állítás.** $A \oplus B = G$, akkor és csak akkor ha $(A + \{g\}) \oplus (B + \{h\}) = G$

*Bizonyítás.*

$$A \oplus B = G \Longleftrightarrow (A \oplus B) \oplus g = G \Longleftrightarrow (A \oplus g) \oplus B = G$$

□

Ez alapján, ha $A \oplus B = G$, akkor tetszőleges $g_1$ és $g_2$ elemre feltehetjük $g_1 \in A$ és $g_2 \in B$. Egyszerű számolás mutatja a következőt:

**1.1.9. Állítás.** Ha $A \oplus B = G$, akkor $|A||B| = |G|$.

**1.1.10. Példa.** Legyen $G = \mathbb{Z}_p$, $p$ prím. Az előző állítás alapján, ha $A \oplus B = G$, akkor $|A||B| = p$, tehát csak a $G \oplus g = G$ alakú parkettázások léteznek.

**1.1.11. Példa.** Most nézünk egy példát arra is, amikor $A$ és $B$ sem részcsoport, vagy mellékosztály. Legyen $G = \mathbb{Z}_2 \times \mathbb{Z}_6$. Legyen $A = \{(0,0),\ (0,1),\ (0,2)\}$ és $B = \{(0,0),\ (1,1),\ (0,3),\ (1,4)\}$. Ezek parkettáznak, de egyik se részcsoport. Ugyanakkor vegyük észre, hogy $A$ kicserélhető a $\{(0,0),\ (0,2),\ (0,4)\}$ részcsoportra.

## 1.2. Körosztási polinomok

Ebben a szekcióban belátjuk a körosztási polinomok néhány fontosabb, de talán kevésbé ismert tulajdonságát, amit a későbbiek során fel fogunk használni. Az $n$-edik körosztási polinomot $\Phi_n(x)$ jelöjük, definíciója pedig

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \xi_i)$$

ahol $\xi_1, \xi_2, \ldots \xi_{\varphi(n)}$ az összes primitív $n$-edik egységgyök. Belátható, hogy $\Phi_n(x)$ irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ fölött, és mindig egész együtthatósak. Idézzük fel a következő jól ismert képletet:

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Ebből azonnal következik, hogy $p$ prímre $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$. Ismeretes továbbá az is, hogy $p^\alpha$ prímhatványra $\Phi_{p^\alpha}(x) = \Phi_p(x^{p^{\alpha-1}})$.

**1.2.1. Állítás.** Bármely $k$-ra az összes $k$-adik egységgyök összege 0. Ha $k$ prím és $\sum_{i=0}^{k-1} a_i \xi_i = 0$ ($a_i \in \mathbb{Q}$), akkor $a_i = a_j$ minden $i, j$-re.

*Bizonyítás.* Legyen $\xi_k$ $k$-adik primitív egységgyök. Arra van szükségünk, hogy $\sum_{i=0}^{k-1} \xi_k^i = 0$. Mivel

$$\prod_{\substack{d|k \\ d>1}} \Phi_d(\xi_k) = \sum_{i=0}^{k-1} \xi_k^i$$

Így a $\Phi_k(\xi_k)$ tag miatt a fönti szorzat 0, tehát az összeg is.

Rátérünk a második részre. Tegyük fel, hogy $k$ prím és hogy az állítás hamis, tehát nem egyezik meg az összes $a_i$. Az első rész alapján igaz

$$\sum_{i=0}^{k-1} a_i \xi_k^i = \sum_{i=0}^{k-1} a_i \xi_k^i - \sum_{i=0}^{k-1} a_{k-1} \xi_k^i = \sum_{i=0}^{k-2} (a_i - a_{k-1}) \xi_k^i = 0$$

Ez egy legfeljebb $k-2$ fokú, nem azonosan 0 polinom kiértékelve $\xi_k$. Mivel az eredmény 0 és $\Phi_k(x)$ irrdecubilis $\mathbb{Q}$ fölött, így ellentmondást kaptunk. $\square$

**1.2.2. Állítás.** Ha $s$ és $t$ relatív prímek, akkor $\Phi_s(x^t) = \prod \Phi_{rs}(x)$, ahol $r$ végigfut $t$ összes osztóján.

*Bizonyítás.* Legyen $p \mid t$ prím. Ekkor $p$ nem osztja $s$-et. $z$ pontosan akkor gyöke $\Phi_s(x^p)$-nek, ha $z^p$ egy $s$-edik primitív egységgyök, vagyis ha $z = e^{\frac{2\pi i k}{ps}}$ $(s, k) = 1$ alakú. Vagyis $\Phi_s((x^{t/p})^p) = \Phi_{ps}(x^{t/p}) \Phi_s(x^{t/p})$. Ezt ismételve $t$ összes prímosztójára kapjuk az állítást. $\square$

**1.2.3. Állítás.**

$$\Phi_s(1) = \begin{cases} 0 \text{ ha } s = 1 \\ p \text{ ha } s \text{ a } p \text{ prímnek egy hatványa} \\ 1 \text{ egyébként} \end{cases}$$

*Bizonyítás.* Ha $s = 1$, akkor triviális. Láttuk, hogy $p$ prímre $\Phi_p = 1 + x + \ldots + x^{p-1}$ és $\Phi_p(x^{p^{\alpha-1}}) = \Phi_{p^\alpha}(x)$. Ebből következik az állítás, ha $s = p^\alpha$ prímhatványra.

Most legyen $s$ összetett, és tegyük fel, hogy minden $s$-nél kissebb pozitív egészre igaz az állítás. Továbbá használjuk fel, hogy

$$\prod_{d|s, d\neq 1} \Phi_d(x) = 1 + x + x^2 + \ldots + x^{n-1}$$

Behelyettesítve 1-et azt kapjuk, hogy $\Phi_s(1) = 1$, hiszen az indukcióból következik, hogy az összetett osztókra 1 az értéke a körosztási polinomnak, prímhatványokra pedig már tudjuk. $\square$

## 1.3. Reprezentációk és Fourier transzformált

Ebben a szekcióban felépítjük a szükséges csoportreprezentáció-elméletet. Magának az általános elméletnek már a bevezetése se férne bele ebbe a dolgozatba. Viszont nekünk csak a véges Abel csoportok reprezentációjára lesz szükségünk, azon belül is az 1 dimenziósakra. Bevezetjük a diszkrét Fourier transzformáltat is, és ismertetjük néhány fontos tulajdonságát. A szekció [21] alapján lett feldolgozva.

**1.3.1. Definíció.** Legyen $G$ véges Abel csoport. Egy $\chi : G \mapsto \mathbb{C}^*$ csoporthomomorfizmust, reprezentációnak, irreducibilis reprezentációnak, irreducibilis karakternek, vagy csak egyszerűen karakternek nevezzük. Ha $\chi$ értékkészlete $\{1\}$, akkor $\chi$-t triviális reprezentációnak nevezzük.

Általános reprezentációelméletben a fenti elnevezések mind más dolgot jelentenénk, de jelen esetünkben ezek mind egybeesnek.

**1.3.2. Tétel.** *$G$ véges Abel csoport irreducibilis karaktereinek halmaza $G$-vel izomorf csoport (a művelet a függvények szorzása). Ezt $G$ duálisának is hívjuk, jelölése $\hat{G}$.*

*Bizonyítás.* Legyen $|G| = N$. Az nyilvánvaló, hogy $\hat{G}$ csoport. A véges Abel csoportok alaptétele szerint $G = \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_d^{\alpha_d}}$, ahol $p_i$ prím és $\alpha_i$ pozitív egész. Legyen $a_i$ az az elem, ahol az $i$-edik koordinátában $\mathbb{Z}_{p_i^{\alpha_i}}$-nek egy generátoreleme van, a többiben pedig 0. $o(a_i) = p_i^{\alpha_i}$, tehát egy homomorfizmusnál a képe $p_i^{\alpha_i}$-adik egységgyök. Ebből következően, legfeljebb $\prod_{i=1}^{d} p_i^{\alpha_i} = N$ különböző reprezentáció lehetséges.

Most megadunk egy $\theta : G \mapsto \hat{G}$ injektív homomorfizmust. Legyen $a = (a_1, a_2, \ldots, a_d) \in G$ és

$$\theta(a)(x) = \theta(a)(x_1, x_2, \ldots x_d) = \prod_{i=1}^{d} e^{\frac{2\pi i a_i x_i}{p_i^{\alpha_i}}}$$

ahol az $a_i x_i$ szorzatokat modulo $p_i^{\alpha_i}$ tekintjük Ez könnyen ellenőrizhetően homomorfizmus.

Most belátjuk, hogy $\theta$ injektív. Legyen két $G$-beli elem $a = (a_1, a_2, \ldots a_n)$ és $b = (b_1, b_2, \ldots b_n)$, továbbá $x = (x_1, 0, \ldots, 0)$, ahol $(x_1, p_1^{\alpha_1}) = 1$. Ha $\theta(a) = \theta(b)$, akkor $a_1 x_1 \equiv b_1 x_1 \pmod{p_1^{\alpha_1}}$, ami ekvivalens $a_1 \equiv b_1 \pmod{p_1^{\alpha_1}}$ kongruenciával. Ezt az összes koordinátára megcsinálva kapjuk, hogy $a = b$. Mivel $|\hat{G}| \le |G|$, így $\theta$ bijekció is. □

Innentől kezdve $\hat{G}$ elemeit indexelhetjük $G$ elemeivel.

**1.3.3. Definíció.** Legyen $G = \{0 = g_0, g_1, g_2, \ldots, g_{n-1}\}$. Ekkor $\hat{G} = \{\chi_{g_0}, \chi_{g_1}, \chi_{g_2}, \ldots, \chi_{g_{n-1}}\}$. Azt az $A \in \mathbb{C}^{n \times n}$ mátrixot, ahol az $i$-edik sor $j$-edik oszlopában $\chi_{g_i}(g_j)$ áll, a $G$ csoport karaktertáblájának nevezzük.

**1.3.4. Példa.** Kiszámítjuk $G = \mathbb{Z}_4$ karaktertábláját. $\chi_g(x) = e^{\frac{2\pi i g \cdot x}{4}}$, ahol a szorzást (mod 4) tekintjük.

$$\mathbb{A} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i 1\cdot 1}{4}} & e^{\frac{2\pi i 1\cdot 2}{4}} & e^{\frac{2\pi i 1\cdot 3}{4}} \\ 1 & e^{\frac{2\pi i 2\cdot 1}{4}} & e^{\frac{2\pi i 2\cdot 2}{4}} & e^{\frac{2\pi i 2\cdot 3}{4}} \\ 1 & e^{\frac{2\pi i 3\cdot 1}{4}} & e^{\frac{2\pi i 3\cdot 2}{4}} & e^{\frac{2\pi i 3\cdot 3}{4}} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Figyeljük meg, hogy $\mathbb{A}\mathbb{A}^* = 4I$. Itt $I$ az identitás mátrix, és $\mathbb{A}^*$ pedig $\mathbb{A}$ transzponáltjának konjugáltja. Később látni fogjuk, hogy ez a tulajdonság minden karaktertáblára igaz.

**1.3.5. Definíció.** Vegyünk egy $f \in L(G)$ függvényt. Az

$$\hat{f} : \hat{G} \mapsto \mathbb{C} \qquad \hat{f}(\chi) = \sum_{g \in G} f(g)\overline{\chi(g)}$$

függvényt $f$ Fourier transzformáltjának hívjuk.

**1.3.6. Tétel.** $\hat{G}$ bázis $L(G)$-ben és tetszőleges $f \in L(G)$-re

$$f = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi$$

A fenti egyenletet Fourier inverziós formulának is szokták hívni.

*Bizonyítás.* Már láttuk, hogy $\dim L(G) = |G| = |\hat{G}| = n$. Be fogjuk látni, hogy a reprezentációk merőlegesek egymásra. Tehát vegyünk $\chi_a$ és $\chi_b$ különböző karaktert. Arra van szükségünk, hogy $\langle \chi_a, \chi_b \rangle = \sum_{g \in G} \chi_{a-b}(g) = 0$. Mivel $\chi_{a-b}$ nem a triviális karakter, így alkalmas $h$-t választva $\chi_{a-b}(h) \neq 1$. Szorozzuk meg a skalárszorzatot $\chi_{a-b}(h)$-val. Kihasználva hogy $\chi_{a-b}$ homomorfizmus, könnyen látható, hogy

$$\chi_{a-b}(h) \sum_{g \in G} \chi_{a-b}(g) = \sum_{g \in G} \chi_{a-b}(g)$$

Ha a szumma nem nulla szám lenne, akkor $\chi_{a-b}(h) = 1$, ami nem lehet. Tehát szumma értéke 0.

Az állítás második fele az alábbi átalakításból következik:

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi = \sum_{\chi \in \hat{G}} \left( \frac{1}{|G|} \sum_{g \in G} f(g)\overline{\chi(g)} \right) \chi = \sum_{\chi \in \hat{G}} \langle f, \chi \rangle \chi = f$$

□

Jelöljük $\mathcal{F}$-el azt az operátort, ami $f$-hez $\hat{f}$-et rendeli.

**1.3.7. Következmény.** $\mathcal{F}$ egy invertálható lineáris leképezés $L(G)$ és $L(\hat{G})$ között.

*Bizonyítás.* Tetszőleges $f_1, f_2 \in L(G)$ függvényekre, és $c_1, c_2$ konstansokra

$$\mathcal{F}(c_1 f_1 + c_2 f_2)(\chi) = \sum_{g \in G} (c_1 f_1(g) + c_2 f_2(g))\overline{\chi(g)} =$$
$$= c_1 \sum_{g \in G} f_1(g)\overline{\chi(g)} + c_2 \sum_{g \in G} f_2(g)\overline{\chi(g)} = c_1 \mathcal{F}(f_1)(\chi) + c_2 \mathcal{F}(f_2)(\chi)$$

vagyis lineáris a leképezés. Az előző tételben pont azt mutattuk meg $\mathcal{F}$ képterében minden elemnek létezik inverze, vagyis injektív a leképezés. Mivel $dim L(G) = dim L(\hat{G})$, így ez egy lineáris izomorfizmus.

□

**1.3.8. Tétel.** Legyen $f, h \in L(G)$. Ekkor

$$\widehat{f * h} = \widehat{f} \cdot \widehat{h}$$

*Bizonyítás.*

$$\widehat{f * h}(\chi) = \sum_{g_1 \in G} (f * h)(g_1)\overline{\chi(g_1)} = \sum_{g_1 \in G} \left( \sum_{g_2 \in G} f(g_1 - g_2)h(g_2) \right) \overline{\chi(g_1)} =$$
$$= \sum_{g_2 \in G} \sum_{g_1 \in G} f(g_1 - g_2)h(g_2)\overline{\chi(g_1)} = \sum_{g_2 \in G} \sum_{g_3 \in G} f(g_3)h(g_2)\overline{\chi(g_2 + g_3)} =$$
$$= \sum_{g_2 \in G} \sum_{g_3 \in G} f(g_3)h(g_2)\overline{\chi(g_2)}\,\overline{\chi(g_3)}) = \sum_{g_2 \in G} f(g_3)\overline{\chi(g_2)} \sum_{g_3 \in G} h(g_2)\overline{\chi(g_3)}) = \widehat{f}(\chi) \cdot \widehat{h}(\chi)$$

A 4. egyenlőségbe a $g_1 - g_2 = g_3$ helyettesítést végeztük el, majd kihasználtuk, hogy $\chi$ homomorfizmus. □

## 1.4. Spektralitás

A szekció [12] alapján lett feldolgozva.

**1.4.1. Definíció.** Legyen $S$ részhalmaza $G$-nek. Azt mondjuk, hogy $S$ spektrális, ha létezik olyan $T \subset G$ halmaz, hogy a $\{\chi_t \mid t \in T\}$ karakterek halmaza ortogonális bázisa $L(S)$-nek, azaz

$$\sum_{s\in S} \chi_{t_1}\overline{\chi_{t_2}(s)} = \sum_{s\in S} \chi_{t_1-t_2}(s) = 0$$

minden $t_1,\ t_2 \in T$, és minden $f : S \mapsto \mathbb{C}$ függvényre egyértelműen léteznek $a_i, 0 \leq i \leq |T|$ elemek, melyre

$$f = \sum_{t\in T} a_i\chi_i,\ \ a_i \in \mathbb{C}$$

Ekkor $T$-t $S$ spektrumának hívjuk, illetve azt mondjuk, hogy $(S, T)$ spektrális pár.

**1.4.2. Megjegyzés.** A folytonos esetben fontos, hogy az $L^2(\mathbb{R}^n)$ négyzetesen integrálható függvények terén dolgozzunk, mivel csak itt van skalárszorzás. A diszkrét esetben bármilyen függvényt ki tudunk "négyzetesen integrálni", így $L(G) = L^2(G)$.

**1.4.3. Példa.** Legyen $G = \mathbb{Z}_p$, $p$ prím és $(S, T)$ spektrális pár. Ekkor

$$\sum_{s\in S} \chi_{t_1-t_2}(s) = \sum_{s\in S} e^{\frac{2\pi i(t_1-t_2)s}{p}} = 0$$

A szumma csak akkor lehet 0, ha $(t_1 - t_2)s \bmod p$ befutja a $0, 1, \ldots p - 1$ számokat. Tehát $|S| = |G|$, így $S = G$, ami természetesen spektrális, spektruma önmaga. A másik lehetőség, hogy az összeg üres, vagyis $T = \{g\}$, és ez egy 1 elemű halmaznak lehet a spektruma, és nyilván ezek is spektrális párt alkotnak. Tehát a spektrális párok: $(G, G)$ és ({g}, {h}) teszőleges $g,\ h$ elemekre. Vegyük észre, hogy pont ugyanezek a halmazok voltak a parkettázó halmazok, vagyis $\mathbb{Z}_p$-ben egy halmaz pontosan akkor spektrális, ha parkettáz.

**1.4.4. Állítás.** Ha $(S, T)$ spektrális pár, akkor $|S| = |T|$.

*Bizonyítás.* Definíció alapján $|T| = \dim L(S)$. Ugyanakkor $\{\delta_s \mid s \in S\}$ halmaz is egy lineárisan független generátorrendszere $L(S)$-nek. □

**1.4.5. Megjegyzés.** Az előbbi állítás bizonyítását továbbgondolva az is kiderül, hogy ha be akarjuk látni, hogy $(S, T)$ spektrális pár, és tudjuk, hogy $|S| = |T|$, akkor elég az ortogonalitást ellenőrizni.

**1.4.6. Állítás.** $(S, T)$ akkor és csak akkor spektrális pár, ha $(T, S)$ is az.

*Bizonyítás.* Az előző fejezetben láttuk, hogy $G$ izomorf $\hat{G}$-vel és konstruáltunk is egy izomorfizmust. Ebből a leképezésből következik, hogy $\chi_s(t) = \chi_t(s)$ $s \in S,\ t \in T$ esetén. Ebből pedig következik az állítás. □

**1.4.7. Állítás.** Legyen $(S, T)$ spektrális pár. Ekkor $(S+g_1, T+g_2)$ is spektrális pár, minden $g_1,\ g_2 \in G$-re.

*Bizonyítás.* Először azt bizonyítjuk, hogy $(S, T + g)$ spektrális pár. A két halmaz elemszáma ugyanannyi és

$$\sum_{s\in S} \chi_{t_1+g-t_2-g}(s) = \sum_{s\in S} \chi_{t_1-t_2}(s) = 0$$

így készen vagyunk.

Ha $(S + g, T)$ spektrális pár, akkor is megegyeznek a halmazok méretei és

$$\sum_{s\in S} \chi_{t_1-t_2}(s+g) = \sum_{s\in S} \chi_{t_1-t_2}(s)\chi_{t_1-t_2}(g) = \chi_{t_1-t_2}(g)\sum_{s\in S} \chi_{t_1-t_2}(s) = 0$$

hiszen $\chi_{t_1-t_2}$ homomorfizmus, így készen vagyunk. □

**1.4.8. Példa.** Legyen $H$ részcsoportja $G$-nek. Ekkor $(H, H)$ spektrális pár. Elemszámaik megegyeznek. Tetszőleges $\chi$ reprezentációra $\chi(H)$ részcsoportja $\mathbb{C}^*$-nak, vagyis az összes $k$-adik egységgyök valamilyen $k$-ra. Láttuk, hogy ezek összege mindig 0, amivel készen vagyunk.

Az előző állítás azt mondja, hogy a $H$ szerinti mellékosztályok is spektrálisak, és spektrumnak tetszőleges $H$ szerinti mellékosztály lehet.

**1.4.9. Állítás.** Legyen $S \subset H \leq G$. Ekkor $S$ pontosan akkor spektrális $H$-ban, ha spektrális $G$-ben.

*Bizonyítás.* Tegyük fel, hogy $S$ spektrális $H$-ban, spektruma $T$. Mivel $T$ $H$-n értelmezett reprezentációkból áll, így ki kell terjeszteni $\hat{H}$ karaktereit $\hat{G}$-re. Legyen $\phi : \hat{G} \mapsto \hat{H}$ a megszorítás. Meg szeretnénk mutatni, hogy a leképezés szürjektív. $\chi \in \ker \phi$ pontosan, akkor ha $\chi(h) = 1$ miden $h \in H$, ami pontosan akkor következik be, ha $\chi$ konstans $H$ mellékosztályain. Ez fordítva is igaz, $G/H$ karakteréhez hozzá tudunk rendelni olyan $\chi \in \hat{G}$ karaktert, mely 1-et ad $H$-n. Így létezik egy bijekció $\ker \phi$ és $G/H$ karakterei között, speciálisan ugyanannyi elemük van. Alkalmazva $\phi$-re a homomorfizmus tételt azt kapjuk, hogy $\hat{G}/\ker \phi$ izomorf $\operatorname{Im} \phi$-vel. Mivel $|\ker \phi| = |G|/|H|$, így $|\operatorname{Im} \phi| = |H|$, vagyis $\phi$ szürjektív.

Ha $S$ spektrális $G$-ben, akkor spektruma $\hat{G}$-beli reprezentációkból áll. Ezeket megszorítva $H$-ra az ortogonalitás megőrződik, így készen vagyunk.

$\square$

# 2. fejezet

# Sejtések

A fejezet [20], [22], [3], [25] alapján lett feldolgozva.

## 2.1. A Coven-Meyerowitz sejtés

**2.1.1. Definíció.** Legyen $A \subset \mathbb{Z}_N$ multihalmaz. Ekkor az

$$A(x) = \sum_{a \in A} m_a x^a$$

polinomot az $A$ multihalmaz generátorpolinomjának hívjuk, ahol $m_a$ az $a$ elem súlya.

Két generátorpolinomot összeadva nyilvánvaló, hogy generátorpolinomot fogunk kapni. Viszont a szorzásnál a hatványok kiléphetnek a $\{0, 1, 2, \dots, N-1\}$ halmazból. Ezért egy ilyen műveletet elvégezve egyszerűsítünk, vagyis a keletkezett polinomot mod $x^N - 1$ fogjuk tekinteni. A következő néhány tulajdonságot könnyen be lehet látni:

**2.1.2. Állítás.** Ha $A, B \subset \mathbb{Z}_N$ multihalmazok, $k \in \mathbb{Z}_N$, akkor

1. $A + B$ generátorpolinomja $A(x)B(x) \pmod{x^N - 1}$
2. $kA$ generátorpolinomja $\{k\}(x)A(x) = A(x^k) \pmod{x^N - 1}$
3. $A \cup B$ generátorpolinomja $A(x) + B(x)$
4. $A(1)$ az $A$ multihalmaz mérete

Alapvető fontosságú a parkettázások és körosztási polinomok közötti kapcsolat.

**2.1.3. Állítás.** Legyen $A,\ B \subset \mathbb{Z}_N$ multihalmazok. A következő 3 kijelentés ekvivalens:

1. $A \oplus B = \mathbb{Z}_N$
2. $A(x)B(x) = 1 + x + x^2 + \cdots + x^{N-1} \pmod{x^N - 1}$
3. $N = A(1)B(1)$ és $N$ minden 1-nél nagyobb $t$ osztójára teljesül, hogy $\Phi_t(x)$ osztja $A(x)$-et vagy $B(x)$-et.

Továbbá, ha teljesül valamelyik feltétel, akkor $A$ és $B$ is halmazok és $A(1)B(1) = N$.

*Bizonyítás.* Mivel $\mathbb{Z}[x]/(x^n - 1)$ faktorizálás azt jelenti, hogy a polinomok kitevőit mod $n$ vesszük, így 1. és 2. ekvivalenciája nyilvánvaló.

Tegyük fel 2-t. A

$$x^n - 1 = (x-1)(1 + x + x^2 + \cdots + x^{N-1}) = \prod_{d|N} \Phi_d(x)$$

képlet miatt

$$(x-1)A(x)B(x) \equiv 0 \pmod{x^N - 1}$$

Ebből következik, hogy ha $d \mid N$ és $d > 1$, akkor $\Phi_d(x)$ osztja $A(x)$-t vagy $B(x)$-t. Továbbá

$$A(x)B(x) - 1 - x - x^2 - \ldots - x^{N-1} = P(x)(x^N - 1)$$

valamilyen $P(x)$ polinomra, amiből következik, hogy $A(1)B(1) = N$.

A visszafele irány ugyanígy következik a képletből. □

**2.1.4. Definíció.** $S_A$-val fogjuk jelölni, azon $s$ prímhatványok halmazát, amelyekre $s \mid N$ és $\Phi_s(x)$ osztja $A(x)$-et. A következő két feltételt szokás Coven-Meyerowitz feltételnek is hívni.

(T1) $A(1) = \prod_{s \in S_A} \Phi_s(1)$

(T2) Ha $s_1, s_2, \ldots s_m \in S_A$ és $(s_i, s_j) = 1,\ i \neq j$, akkor $\Phi_{s_1 \ldots s_m} | A(x)$

[3]-ben felvetették a következő két sejtést.

**2.1.5. Sejtés.** Legyen $N$ négyzetmentes. Ekkor $A$ akkor és csak akkor parkettázza $\mathbb{Z}_N$-t, ha létezik $B$ részcsoport, hogy $A$ éppen $B$ mellékosztályainak egy reprezentánsrendszere.

**2.1.6. Sejtés.** $A$ akkor és csak akkor parkettázza $\mathbb{Z}_N$-t, ha teljesül ra T(1) és T(2).

Az első sejtés feltétele nyilván elégséges: $B$-t választva $A \oplus B = \mathbb{Z}_N$ parkettát kapunk. A szükségességet néhány évvel később függetlenül megoldották [22]-ben és [20]-ben. Felvetődik a kérdés, hogy mi történik az általános esettel, vagyis ha nem követeljük meg $N$ négyzetmentességét. Ekkor azonban már kevés elemszámú csoportoknál is elromlik a feltétel. Ugyanis legyen $N = p^2$, ahol $p$ prím, és legyen $A$ az egyetlen nemtriviális részcsoport.

A második sejtésben egyik irány se triviális, de [3]-ben bebizonyították, hogy a feltétel elégséges. Bebizonyítjuk, hogy a parkettázásból következik (T1), viszont a következő példa mutatja, hogy ez az egy feltétel nem elégséges. Legyen $A(x) = x^7 + x^6 + x^4 + x^3 + x + 1 = (x+1)(x^6 + x^3 + 1) = \Phi_2(x)\Phi_3(x)$. $A(1) = \prod_{s \in S_A} \Phi_s(1)$, azaz T(1) teljesül. Viszont $\{0, 1, 3, 4, 6, 7\}$ nem parkettázza $\mathbb{Z}_{12}$-t.

**2.1.7. Tétel.** Tegyük fel, hogy $A \oplus B = \mathbb{Z}_n$. Jelölje $P$ $n$ összes prímhatvány osztójának halmazát. Ekkor az alábbiak teljesülnek.

1. $A$-ra és $B$-re teljesül T(1).
2. $S_A$ és $S_B$ diszjunkt uniója $P$, vagyis $S_A \dot{\bigcup} S_B = P$.

*Bizonyítás.* Nyilván $S_A \bigcup S_B \subset P$. Továbbá tudjuk, hogy $n$ minden $1 < t$ osztójára $\Phi_t(x)$ osztja $A(x)$-et vagy $B(x)$-et, emiatt $P \subset S_A \bigcup S_B$.

3.1.4 lemma alapján

$$A(x) = R(x) \prod_{s \in S_A} \Phi_s(x) \quad B(x) = Q(x) \prod_{s \in S_B} \Phi_s(x)$$

valamilyen $R(x), Q(x) \in \mathbb{Z}[x]$ polinomokra, így teljesül $A(1) \geq \prod_{s \in S_A} \Phi_s(1)$ és $B(1) \geq \prod_{s \in S_B} \Phi_s(1)$. Szintén a lemma alapján $A(1)B(1)$, így

$$A(1)B(1) \geq \prod_{s \in S_A} \Phi_s(1) \prod_{s \in S_B} \Phi_s(1) \geq \prod_{r \in R} \Phi_r(1) = n.$$

Itt felhasználtuk 1.2.3 állítást. A lemma miatt $A(1)B(1) = n$, így mindenhol egyenlőség van, ami csak úgy lehet, hogy $S_A \dot{\bigcup} S_B = P$. Ebből és az egyenlőtlenségekből pedig T(1) is következik. □

Az első sejtés bizonyításához szükségünk lesz két lemmára.

**2.1.8. Lemma** (Tijdeman)**.** Legyen $A \oplus B = \mathbb{Z}_n$. Ha $p$ prím és $(p, |A|) = 1$, akkor $pA$ halmaz és $pA \oplus B = \mathbb{Z}_n$.

*Bizonyítás.* Alkalmazva, hogy $pA$ generátorpolinomja $A(x^p)$ és 2.1.3 állítást, elég azt leelenőrizni, hogy

$$A(x^p)B(x) = 1 + x + x^2 + \ldots + x^{N-1} \pmod{x^N - 1}$$

Az $A(x), A'(x) \in \mathbb{Z}[x]$ polinomokra vezessük be a következő két jelölést:

$$A(x) \equiv A'(x) \pmod{p}$$

ha redukálva az együtthatókat modulo $p$ a polinomok megegyeznek,

$$A(x) \equiv A'(x) \pmod{x^N - 1,\ p}$$

ha a kitevőket modulo $N$, majd az együtthatókat modulo $p$ redukálva a polinomok megegyeznek. Jelöljük $C(x)$-el $1 + x + x^2 + \ldots + x^{N-1}$ polinomot.

Ezekkel az új jelölésekkel először vegyük észre, hogy $A(x^p) \equiv (A(x))^p \pmod{p}$. Továbbá

$$A(x^p)B(x) = A(x)^{p-1}A(x)B(x) \equiv A(x)^{p-1}C(x) \equiv G(x) \pmod{x^N - 1}$$
$$A(x)^{p-1}C(x) \equiv A(1)^{p-1}C(x) \equiv C(x) \pmod{x^N - 1,\ p}$$

Tehát a szorzatból $G(x)$ polinom lett mod $x^N - 1$, majd az együtthatókat is egyszerűsítve $C(x)$. Az utolsó előtti kongruenciánál azt használtuk ki, hogy $C(x) \equiv x^i C(x)$, az utolsóban pedig a kis-fermat tételt alkalmaztuk.

$A(x^p)B(x)$ együtthatói nemnegatívak és összegük $A(1)B(1) = C(1) = N$. Miután a kitevőket modulo $p$ redukáltuk, az együtthatók összege nem változik, amikor pedig az együtthatókat redukáltuk mod $p$ az összegükből $p$ egy többszörösét levontuk. De láttuk, hogy az összeg nem változott vagyis $G(x) = C(x)$, amivel készen vagyunk. □

**2.1.9. Állítás.** Legyen $p$ prím, $A \subset \mathbb{Z}_N$ halmaz. Ha $\Phi_p(x) \mid A(x)$, akkor $|A_{i \bmod p}| = |A_{j \bmod p}|$ minden $i, j$-re, ahol $A_{i \bmod p} = \{a \in A : a \equiv i \pmod{p}\}$.

*Bizonyítás.* Nyilvánvalóan teljesül

$$A(x) = \sum_{i=0}^{p-1} |A_{i \bmod p}| x^i \pmod{x^p - 1}$$

A feltétel miatt $A(x) = G(x)\Phi_p(x)$. Mivel $x^i \Phi_p(x) \equiv \Phi_p(x) \pmod{x^p - 1}$, így

$$A(x) = G(x)\Phi_p(x) = G(1)\Phi_p(x) \pmod{x^p - 1}$$

Vagyis $|A_{i \bmod p}| = G(1)$ minden $i$-re. □

Most pedig belátjuk mindkét sejtést négyzetmentes ciklikus csoportra.

**2.1.10. Tétel.** Legyen $A \subset \mathbb{Z}_N$, ahol $N = p_1p_2 \dots p_n$ négyzetmentes. A következő öt kijelentés ekvivalens:

1. Létezik $B \subset \mathbb{Z}_N$, hogy $A \oplus B = \mathbb{Z}_N$.
2. $A(x)$-re teljesül (T1) és (T2).
3. Létezik $H$ részcsoport, hogy $A$ $H$ mellékosztályainak egy reprezentánsrendszere.
4. $A = \{(x, y_x) : x \in \mathbb{Z}_q\}$, ahol $q = q_1q_2 \cdots q_m \mid N$ és minden $x$-re $y_x \in \mathbb{Z}_{N/q}$.
5. $A(x) \equiv 1 + x + x^2 + \dots + x^{m-1} \pmod{x^m - 1}$, ahol $m \mid N$.

*Bizonyítás.* 3. és 4. ekvivalenciája nyilvánvaló a véges Abel csoportok alaptételéből. 3. és 5. ekvivalenciája pedig onnan látszik, hogy minden $H$ részcsoport $\mathbb{Z}_m, m \mid N$ alakú.

**3 $\implies$ 1 eset.** Könnyen ellenőrizhető, hogy $A \oplus H = \mathbb{Z}_N$.

**2 $\implies$ 5 eset.** Legyen $S$ $S_A$-beli elemek legkissebb közös többszöröse. T(2) miatt

$$A(x) = P(x) \prod_{\substack{1<d \\ d|S}} \Phi_d(x) = P(x)(1 + x + x^2 + \dots + x^{S-1})$$

1.2.3 állításból következik, hogy $\prod_{\substack{1< \\ d|S}} \Phi_d(1) = S$. T(1) miatt pedig $P(1) = 1$. Mivel $x^i(1 + x + x^2 + \dots + x^{S-1}) \equiv (1 + x + x^2 + \dots + x^{S-1}) \pmod{x^S - 1}$, így

$$A(x) \equiv P(1)(1 + x + x^2 + \dots + x^{S-1}) \equiv (1 + x + x^2 + \dots + x^{S-1}) \pmod{x^S - 1}$$

amivel készen vagyunk.

**1 $\implies$ 2 eset.** Már láttuk, hogy T(1) teljesül továbbá, hogy $S_A$ és $S_B$ diszjunktak. Ha

$$A(x) = P(x) \prod_{s \in S_A} \Phi_s(x), \quad B(x) = Q(x) \prod_{s \in S_B} \Phi_s(x)$$

akkor, 1.2.3 állítás miatt

$$A(x)B(x) = P(x)Q(x) \prod_{s \in S_B \bigcup S_A} \Phi_s(x) \equiv \prod_{\substack{1<s \\ s|N}} \Phi_d(x) \pmod{x^N - 1}$$

amiből következik, hogy $\Phi_s(x)$ osztja $P(x)$-et vagy $Q(x)$-et, ha $s \mid N$.

Be kell még látnunk, hogy teljesül (T2). Ehhez elég lenne azt látni, hogy

$$A(x) = 1 + x + \dots + x^{s_A - 1} \pmod{x^{s_A} - 1}$$

ahol $s_A$ az összes $S_A$-beli elem szorzata. Vegyünk egy $S_B$-beli $p$ prímet. Tijdeman lemma alapján $pA \oplus B = \mathbb{Z}_n$. Legyen $B_0 = B_{0 \bmod p}$, láttuk, hogy ekkor $|B_0| = |B|/p$. Emiatt $pA \oplus B_0 = p\mathbb{Z}_{N/p}$. Vagyis $A \oplus B_0 = \mathbb{Z}_{N/p}$.

Minden $S_B$-beli prímre ezt végigcsinálva kapjuk, hogy $A \oplus 0 = \mathbb{Z}_{s_A}$, vagyis

$$A(x) \equiv 1 + x + x^2 + \dots x^{s_A - 1} \pmod{x^{s_A} - 1}.$$

□

Ahogy azt már említettük igaz a következő tétel.

**2.1.11. Tétel.** Legyen $A \subset \mathbb{Z}_N$. Ha $A$-ra igaz T(1) és T(2), akkor $A$ parketttáz.

*Bizonyítás.* Megkonstruáljuk a $B$ halmazt, melyre $A \oplus B = \mathbb{Z}_N$. Legyen $S$ az $S_A$-beli elemek legkissebb közös többszöröse és legyen $D$ halmaz a következő:

$$\{p^\alpha : p \text{ prím}, \ p^\alpha \notin S_A, \ p^\alpha \mid S\}$$

Továbbá $s(p)$ legyen $S$-nek a legnagyobb $p$ hatvány osztója. Legyen $B(x) = \prod_{p^\alpha \in D} \Phi_{p^\alpha}(x^{\frac{S}{s(p)}})$.

1.2.3 állítás alapján $A(1)B(1) = S$. Most vegyük $S$-nek egy $t = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$ osztóját. Meg kell mutatni, hogy $A(x)$-et vagy $B(x)$-et osztja. Ha $p_i^{t_i} \in S_A$ minden $i$-re, akkor T(2) miatt $\Phi_t(x) \mid A(x)$. Ha például $p_1^{s_1} \notin S_A$, akkor $\Phi_{p_1^{t_1}}(x^{\frac{S}{s(p_1)}}) \mid B(x)$, továbbá $p_1^{t_1} \mid \frac{S}{s(p_1)}$, így 1.2.2 állítás alapján $\Phi_t(x) = \Phi_{\frac{t}{p_1^{t_1}} p_1^{t_1}}(x) \mid \Phi_{p_1^{t_1}}(x^{\frac{S}{s(p_1)}}) \mid B(x)$.

Továbbá vegyük észre, hogy $B(x)$ egy multihalmaz generátorpolinomja, hiszen a prímrendű körosztási polinomok együtthatói nullák és egyek, és mivel 2.1.3 állítás teljesül, így $B$ szükségszerűen halmaz. Tehát megkaptuk, hogy $A \oplus B = \mathbb{Z}_S \subset \mathbb{Z}_N$. $\square$

**2.1.12. Példa.** Döntsük el, hogy a $A = \{0, 2, 3, 4, 6\}$ halmaz parkettázza-e $\mathbb{Z}_{30}$-at! Irreducibilisek szorzatára bontva a generátorpolinomot azt kapjuk, hogy $A(x) = \Phi_5(x)\Phi_6(x)$. $A(1) = \Phi(1)$ tehát T(1) teljesül, továbbá $S_A = \{5\}$, így T(2) is. A tételt alkalmazva kapjuk, hogy $A$ parkettáz. A bizonyítás során alkalmazott technikával a kiegészítő $B$ halmazt is megkaphatjuk: $B(x) = \Phi_2(x^{15})\Phi_3(x^{10}) = x^{35} + x^{25} + x^{20} + x^{15} + x^{10} + 1$. Vagyis $B = \{35, 25, 20, 15, 10, 0\} = \langle 25 \rangle$.

## 2.2. Fuglede sejtés

Ahogy azt a bevezetőben említettük a spektralitás és a parkettázás kapcsolatának kérdése nem csoportok vagy az egésze struktúráján merült fel először, hanem $\mathbb{R}^n$.

**2.2.1. Definíció.** Legyen $\Omega \in \mathbb{R}^n$ Lebesgue mérhető halmaz pozitív, véges mértékkel. Azt mondjuk, hogy a $\Omega$ halmaz spektrális, ha létezik $\Lambda \in \mathbb{R}^n$ , hogy a $\{e^{2\pi i \langle x, \lambda \rangle}\}_{\lambda \in \Lambda}$ halmaz ortogonális bázisa $L^2(\Omega)$-nak.

**2.2.2. Definíció.** $\Omega \in \mathbb{R}^n$ parkettázza $\mathbb{R}^n$-t, ha létezik $\Lambda$, hogy majdnem minden $\mathbb{R}^n$-beli pont egyértelműen előáll, mint $\lambda + \omega$ $\lambda \in \Lambda, \omega \in \Omega$ összeg.

**2.2.3. Sejtés** (Fuglede)**.** $\mathbb{R}^n$ pozitív Lebesgue mértékű részhalmaza pontosan akkor spektrális, ha parkettáz. $G$ véges Abel csoport egy részhalmaza pontosan, akkor spektrális, ha parkettáz.

Bevezetünk néhány jelölést. Legyen $G = \mathbb{R}, \mathbb{Z}$ vagy véges Abel csoport. $(S \implies T)(G)$ jelentse azt, hogy $G$ minden spektrális részhalmaza parkettáz, $(T \implies S)(G)$ pedig értelemszerűen a fordított irányt. $(S \implies T)(\mathbb{Z}_N)_\infty$ pedig jelentse azt, hogy $\mathbb{Z}_N$ spektrális részhalmazai parkettáznak minden $N$-re, $(T \implies S)(\mathbb{Z}_N)_\infty$ pedig a megfordítást minden $N$-re. A következő tétel rámutat a folytonos és diszkrét Fuglede sejtés közötti kapcsolatra. A következő eredmény [4]-ben van összefoglalva.

**2.2.4. Tétel.**

$$(T \implies S)(\mathbb{R}) \iff (T \implies S)(\mathbb{Z}) \iff (T \implies S)(\mathbb{Z}_N)_\infty$$

$$(S \implies T)(\mathbb{R}) \implies (S \implies T)(\mathbb{Z}) \implies (S \implies T)(\mathbb{Z}_N)_\infty$$

Az első fejezetben láttuk, hogy ha egy halmazt eltolunk, akkor az nem változtat sem a parkettázó, sem a spektrális tulajdonságán. Így ha a Fuglede sejtést szeretnénk egy adott csoportra bizonyítani, feltehetjük tetszőleges elemről, hogy a halmaznak eleme, vagy azt hogy nem. A következő összefoglalás megtalálható [11]-ben. A $(S \not\Longrightarrow T)(G)$ jelölés, ahol $G$ véges Abel csoport, azt fogja jelenteni, hogy létezik $G$-ben spektrális halmaz, amely nem parkettáz. Ugyanígy $(T \not\Longrightarrow S)(G)$. $(T \iff S)(G)$ pedig jelentse azt, hogy $G$-re igaz a Fuglede sejtés.

**2.2.5. Tétel.** Igaz a következő néhány állítás:

1. $(S \not\Longrightarrow T)(\mathbb{Z}_p^d)$, ha $d \geq 4$ és $p$ páratlan prím.
2. $(S \not\Longrightarrow T)(\mathbb{Z}_2^d)$, ha $d \geq 10$.
3. $(S \not\Longrightarrow T)(\mathbb{Z}_8^3)$.
4. $(T \not\Longrightarrow S)(\mathbb{Z}_{24}^3)$.
5. $(T \implies S)(\mathbb{Z}_p^d)$, ha $p$ prím és $d \leq 3$.
6. $(S \implies T)(\mathbb{Z}_p^d)$, ha $p$ prím és $d \leq 2$ vagy $d = 3$ és $p \leq 7$ prím.
7. $(T \iff S)(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ és $(T \iff S)(\mathbb{Z}_p \times \mathbb{Z}_{pq})$, ahol $p \neq q$ prímek.
8. $(T \implies S)(\mathbb{Z}_n)$, ahol $n$ négyzetmentes, $n = p^m q^n$ vagy $n = p^m d$ tetszőleges $d$ négyzetmentes számra.
9. $(T \iff S)(\mathbb{Z}_n)$, ahol $n = p^n, p^n q, p^n q^2, pqr, p^2 qr$, ahol $p, q, r$ különböző prímek.

## 2.3. Kapcsolat

Ebben a szekcióban a Coven-Meyerowitz feltételek és a spektralitás közötti kapcsolattal foglalkozunk, speciálisan bebizonyítjuk, hogy az elsőből következik a második.

**2.3.1. Lemma.** Legyen $b = \sum_{i=1}^{n} \frac{k_i}{s_i}$, ahol $(k_i, s_i) = (s_i, s_j) = 1$ minden $i \neq j$ indexre. Ekkor $\Phi_s(e^{2\pi i b}) = 0$, ahol $s = s_1 \dots s_n$.

*Bizonyítás.* Azt kell ellenőrizni, hogy közös nevezőre hozás után nem lehet $b$-t egyszerűsíteni. Tehát írjuk fel $b$-t a következőképpen:

$$b = \frac{k}{s}, \; s = s_1 \dots s_n, \; k = \frac{k_1 s}{s_1} + \dots + \frac{k_1 s}{s_n}$$

Indirekte tegyük fel, hogy létezik $p$ mely osztja $k$-t és $s$-et. Ekkor valamelyik $s_i$-t is osztja, legyen ez $s_1$. Ekkor $p \mid k - \frac{k_1 s}{s_1}$, hiszen a jobboldalt, ha definíció szerint felírjuk, akkor mindegyik összeadandót osztja $s_1$. Ezekből következik, hogy $p \mid \frac{k_1 s}{s_1}$. Mivel $s_i$-k páronként relatív prímek, így $p \mid k_1$. De ekkor $p \mid (s_1, k_1)$, ami feltevésünk szerint nem lehet.

□

**2.3.2. Tétel.** Legyen $A \subset \mathbb{Z}_N = G$. Tegyük fel, hogy teljesülnek a Coven-Meyerowitz feltételek. Ekkor $A$ spektrális.

*Bizonyítás.* Legyen $|A| = N = p_1^{\alpha_1} \dots p_m^{\alpha_m}$. Álljon $B$ halmaz a következő elemekből:

$$\sum_{s \in S_A} \frac{k_s}{s}$$

ahol $k_s$ befutja $\{0, 1, 2, \dots p-1\}$ halmazt, ha $s = p^\alpha$ alakú. Vegyük észre, hogy ekkor $e^{2\pi i b x}, b \in B$ alakú függvények éppen $\hat{G}$ karakterei. Azt fogjuk belátni, hogy $A$ spektruma $B$.

Vegyünk egy $b, b' \in B$ elemeket. Ezekről be kell látnunk, hogy

$$A(e^{2\pi i(b-b')}) = \sum_{a \in A} e^{2\pi i(b-b')a} = 0$$

Hozzuk $b-b'$ különbséget, minél egyszerűbb alakra. Azokat a tagokat, amiknek nevezőjébe ugyanannak a prímnek a hatványa szerepel hozzuk közös nevezőre. Így $b-b'$

$$\sum_{i=1}^{m} \frac{k_i}{p_i^{\beta_i}}$$

alakba írható, ahol $\beta_i$ az a legnagyobb kitevő, amire még $p_i^{\beta_i} \in S_B$ és az eredeti szummában hozzá tartozó számláló nem 0 volt. Közös nevezőre hozva és alkalmazva a kínai maradéktételt látható, hogy ez pontosan akkor 0, ha tagonként 0. Nézzük a szummának egy tagját:

$$\sum_{j=1}^{l} \frac{v_j}{p_i^{\beta_j}} = \frac{\sum_{j=1}^{l} v_j p_i^{\beta_l - \beta_j}}{p_i^{\beta_j}}$$

ahol $v_j \in \{-p_i+1, -p_i+2, \ldots, p_i-1\}$. A számlálóról látható hogy relatív prím $p_i$-hez. Az előző lemma alapján $\Phi_s(e^{2\pi i(b-b')}) = 0$, ahol $s = \prod_{i \in I} p_i^{\beta_i}$. Mivel $p_i^{\beta_i} \in S_A$, így (T2) miatt $\Phi_s(x) \mid A(x)$, tehát $e^{2\pi i(b-b')}$ gyöke $A(x)$-nek. A fenti felírásból továbbá az is látszik, hogy pontosan, akkor 0, ha $p_i^{\beta_j}$ nevezőjű tag 0. Ezzel azt is megmutattuk, hogy $B$ eredeti felírásában minden elem különböző.

Még be kell látnunk, hogy $|B| = |A|$. (T1) alapján $|A| = A(1) = \prod_{s \in S_A} \Phi_s(1)$. Az 1.2.3 lemma miatt ez azt jelenti, hogy $S_A$-ban pontosan $\alpha_i$ darab $p_i$ hatvány van. Vagyis $|B| = N$.

$\square$

# 3. fejezet

# Spektralitásból Parkettázás

## 3.1. Gyenge Parkettázás

Ez a fejezet Somlai Gábor, Kiss Gergely és Matolcsi Máté ötlete alapján készült.

A fejezet célja az lesz hogy megmutassuk néhány csoportra, hogy ha egy részhalmaza spektrális, akkor parkettáz. A módszer alapjául a következő tétel fog szolgálni, melyet [16]-ban bizonyítottak (ott folytonos esetre):

**3.1.1. Tétel.** Legyen $G$ véges Abel csoport és $S \subseteq G$ spektrális. Ekkor létezik $T : G \to \mathbb{R}$ függvény melyre igazak az alábbiak:

1. $T(0) = 1$
2. $\mathbb{1}_S * T = \mathbb{1}_G$
3. $T \geq 0$

*Bizonyítás.* Legyen $S$ spektruma $\Lambda$.

$$\mathbb{1}_S * T = \mathbb{1}_G \iff \widehat{\mathbb{1}}_S \cdot \widehat{T} = \widehat{\mathbb{1}}_G = |G|\delta_{\chi_0}.$$

Mivel $\Lambda$ spektruma $S$-nek, így $\widehat{\mathbb{1}}_S$ eltűnik $(\Lambda - \Lambda) \setminus \{0\}$ halmazon. Olyan $\widehat{T}$ függvényt kell konstruálnunk, mely eltűnik $(\Lambda - \Lambda)^c \setminus \{0\}$ halmazon. Vegyük a $\hat{T} = \frac{|G|}{|\Lambda|^2} \mathbb{1}_\Lambda * \mathbb{1}_{-\Lambda}$. Precízebben

$$\hat{T}(\chi_h) = \frac{|G|}{|\Lambda|^2} m_h, \text{ ahol } m_h \ h \text{ multiplicitása } \Lambda - \Lambda\text{-ban}$$

Vegyük észre, hogy a függvény az $\chi_0$ helyen $\frac{|G|}{|\Lambda|}$ vesz fel. Továbbá mivel $|S| = |\Lambda|$, így $\widehat{\mathbb{1}}_S(\chi_0)\widehat{T}(\chi_0) = |G|$. Most legyen $T = \mathcal{F}^{-1}(\widehat{T})$, aminek tartója $\Lambda - \Lambda$. Az eddigiek alapján 2. tulajdonság teljesül.

A Fourier inverziós formula alapján

$$T = \frac{|G|}{|G||\Lambda|^2} \sum_{\chi_h \in \hat{G}} (\mathbb{1}_\Lambda * \mathbb{1}_{-\Lambda})(\chi_h)\chi_h =$$
$$= \frac{1}{|\Lambda|^2} \sum_{\chi_h \in \hat{G}} m_h \chi_h = \frac{1}{|\Lambda|^2} \sum_{h \in \Lambda - \Lambda} m_h \chi_h$$

Mivel $\chi_h(0) = 1$, így 0-ban a szumma éppen a $\Lambda - \Lambda$ multihalmaz mérete, vagyis $|\Lambda|^2$. Vagyis $T(0) = 1$.

Vegyük észre, hogy $\lambda \in \Lambda - \Lambda$ pontosan akkor, ha $-\lambda \in \Lambda - \Lambda$, és multiplicitásuk megegyezik. Vagyis bármilyen $t$-re a szummában ugyanannyiszor szerepel $\chi_\lambda(t)$ és $\chi_{-\lambda}(t)$, melyek egymás konjugáltjai, így $T(t) \in \mathbb{R}$. $m_0 = |\Lambda|$ és $\chi_0(t) = 1$ minden $t$-re.

$$\sum_{h \in \Lambda - \Lambda} m_h \chi_h(t) = m_0 \chi_0(t) + \sum_{\substack{h \neq 0 \\ h \in \Lambda - \Lambda}} m_h \chi_h(t) =$$
$$= |\Lambda| + \sum_{\substack{h \neq 0 \\ h \in \Lambda - \Lambda}} m_h \operatorname{Re}(\chi_h(t)) \geq |\Lambda| - \sum_{\substack{h \neq 0 \\ h \in \Lambda - \Lambda}} m_h \geq 0$$

Az első egyenlőtlenség abból következik, hogy $\chi_h(t)$ egységgyök, a második pedig abból, hogy $\sum_{h \in \Lambda - \Lambda} m_h = |\Lambda|^2$. Tehát $T \geq 0$.

□

Vegyük észre, hogy $T \leq 1$ és ha $T$ előáll $\mathbb{1}_L$ $L \subseteq G$ alakban, akkor $S$ parkettázás ($L$-el). Tehát ezek a függvények a parkettázások egy bővebb halmazát definiálják.

**3.1.2. Definíció.** Az $S$ halmaz gyengén parkettázza $G$-t $T : G \to \mathbb{R}$ függvénnyel, ha $T$ teljesíti az előző tételben szereplő három feltételt. Ekkor $T$-t gyenge parkettának hívjuk. Jelölése: $S \oplus T = G$ gyengén.

A következőkben azt vizsgáljuk meg, hogy a $\mathbb{1}_S * T = \mathbb{1}_G$ feltételből milyen következtetések vonhatók le. Ehhez bevezetünk egy újabb fogalmat.

**3.1.3. Definíció.** Adott egy $T : G \to \mathbb{R}$ függvény. Ekkor a

$$\widetilde{T}(t) := \frac{1}{\varphi(|G|)} \sum_{\substack{k < |G| \\ (k, |G|) = 1}} T(kt)$$

függvényt, T átlagfüggvényének nevezzük.

**3.1.4. Lemma.** Tegyük fel, hogy $A \oplus T = G$ gyengén. Ekkor $A \oplus \widetilde{T} = G$ gyengén. Továbbá $\widetilde{\mathbb{1}}_A * T = \widetilde{\mathbb{1}}_A * \widetilde{T} = \mathbb{1}_G$.

*Bizonyítás.* Jelölje az $f$ függvény gyökeit $\mathcal{Z}(f)$. Figyeljük meg, hogy $(K, \cdot)$ csoport, $K = \{1 \leq k < |G| \mid (k, |G|) = 1\}$, hat $G$-n és $\hat{G}$-n. A csoporthatások: $x \mapsto kx,\ x \in G$ és $\chi \mapsto \chi^k,\ \chi \in \hat{G}$.

Először belátjuk, hogy $\widetilde{\mathbb{1}}_A * T = \mathbb{1}_G$. $\chi \in \mathcal{Z}(\mathbb{1}_A)$ esetén igaz

$$\widehat{\mathbb{1}}_A(\chi) = \sum_{a \in A} \chi(a) = 0$$

Erre az egyenletre alkalmazva $Gal(\mathbb{Q}(\xi) \mid \mathbb{Q})$ tetszőleges elemét, ahol $\xi$ $|G|$-edik primitív egységgyök, kapjuk, hogy minden $(k, |G|) = 1$-re

$$\sum_{a \in A} \chi^k(a) = 0.$$

Ebből következik, hogy $\mathcal{Z}(\widehat{\mathbb{1}_A}) \subset \mathcal{Z}(\mathcal{F}(\widetilde{\mathbb{1}}_A))$, hiszen, ha $\chi \in \mathcal{Z}(\widehat{\mathbb{1}_A})$

$$\mathcal{F}(\widetilde{\mathbb{1}_A})(\chi) = \frac{1}{\varphi(|G|)} \sum_{g \in G} \overline{\chi(g)} \sum_{k \in K} \mathbb{1}_A(kg) = \frac{1}{\varphi(|G|)} \sum_{k' \in K} \sum_{a \in A} \overline{\chi(k'g)} = 0$$

Továbbá $\mathcal{F}(\widetilde{\mathbb{1}}_A)(\chi_0) = \widehat{\mathbb{1}}_A(\chi_0)$. Vagyis beláttuk, hogy $\widetilde{\mathbb{1}}_A * T = \mathbb{1}_G$.

Figyeljük meg, hogy az előző gondolatmenetből az is kijött, hogy ha $\chi \in \mathcal{Z}(\widehat{\mathbb{1}}_A)$, akkor $\chi^k \in \mathcal{Z}(\widehat{\mathbb{1}}_A), k \in K$, vagyis $\mathcal{Z}(\widehat{\mathbb{1}}_A)$ nem más mint $K$ által meghatározott orbitok uniója. Így $\mathcal{O} = \mathcal{Z}(\widehat{\mathbb{1}}_A)^c \cup \{\chi_0\}$ is orbitok uniója, továbbá $\mathcal{O} \subset \mathcal{Z}(\widehat{T})$ . Vagyis ha $\chi \in \mathcal{O}$, akkor $\chi^k \in \mathcal{O},\ (k, |G|)$ is igaz és itt

$$\widehat{T}(\chi) = \sum_{g \in G} T(g)\overline{\chi(g)} = 0 = \widehat{T}(\chi^k) = \sum_{g \in G} T(g)\overline{\chi^k(g)} = \sum_{g \in G} T(k'g)\overline{\chi(g)}$$

Továbbá ilyen $\chi$-re

$$\mathcal{F}(\widetilde{T})(\chi) = \frac{1}{\varphi(|G|)} \sum_{g\in G} \overline{\chi(g)} \sum_{k\in K} T(kg) = \frac{1}{\varphi(|G|)} \sum_{k'\in K} \sum_{g\in G} T(g)\overline{\chi(k'g)} = 0$$

vagyis $\chi \in \mathcal{Z}(\mathcal{F}(\widetilde{T}))$. Nyilván $\widetilde{T} \geq 0$, és ellenőrizhető, hogy $\widetilde{T}(0) = T(0)$, vagyis $A \oplus T = G$.

$\widetilde{\mathbb{1}}_A * \widetilde{T} = \mathbb{1}_G$ már következik a kettő előzőből.

$\square$

A következőkben kényelmi okokból bevezetjük a

$$B_i = \mathbb{1}_{A_i} = \sum_{a\in A_i} \delta_a$$

Vegyünk egy $x \mapsto kx$, $(|G|, k)$ függvényt és jelölje $A_1 = \{0\}, A_2, \ldots A_n$ a csoport függvény szerinti orbitjait. Ezek egy partícióját adják $G$-nek. Vegyünk egy tetszőleges $T : G \mapsto \mathbb{R}_{0\leq}$ gyenge parkettát.

$$\widetilde{T}(t) = \sum_{(k,|G|)=1} T(kt) = \sum_{i=1}^{n} d_i B_i(t)$$

Itt $d_i$-k 0 és 1 közé eső számok. Az előző lemma alapján $\widetilde{T} * \mathbb{1}_S = \mathbb{1}_G$, ez új jelölésekkel felírva

$$(\widetilde{T} * \mathbb{1}_S)(t) = ((\sum_{i=1}^{n} d_i B_i) * \mathbb{1}_S)(t) = \sum_{g\in G} \sum_{i=1}^{n} d_i B_i(t-g)\mathbb{1}_S(g) =$$

$$\sum_{s\in S} \sum_{i=1}^{n} d_i B_i(t-s) = 1 \tag{3.1}$$

Hasonlóan fel tudjuk írni $\mathbb{1}_S$ átlagolását

$$\widetilde{\mathbb{1}_S}(t) = \sum_{(k,|G|)=1} \mathbb{1}_S(kt) = \sum_{i=1}^{n} c_i B_i(t)$$

Tehát $c_i$ elemek nem mások, mint az $\mathbb{1}_S$ függvény kiátlagolása $A_i$ orbiton, vagyis $\frac{|S\cap A_i|}{|A_i|}$.

**3.1.5. Állítás.** Legyen $T$ gyenge parketta és tegyük fel, hogy $d_i \in \{0, 1\}$ minden $i$-re. Ekkor $T$ parketta.

*Bizonyítás.* $d_i = \frac{\frac{\varphi(|G|)}{|A_i|}}{\varphi(|G|)} \sum_{a\in A_i} T(a) = \frac{1}{|A_i|} \sum_{a\in A_i} T(a)$. Tudjuk, hogy $0 \leq T(a) \leq 1$. Tehát, ha $d_i = 0$, akkor $T(a) = 0$ $\forall a \in A_i$, ha pedig $d_i = 1$, akkor $T(a) = 1$ $\forall a \in A_i$. Ha ez minden $i$-re teljesül, akkor $T$ értékkészlete $\{0, 1\}$. $\square$

**3.1.6. Állítás.** Tegyük fel, hogy $f * h = \mathbb{1}_G$. Ekkor

$$\left(\sum_{g\in G} f(g)\right)\left(\sum_{g\in G} h(g)\right) = |G|$$

Speciálisan, ha $S \oplus T = G$ gyengén, akkor $|S| \left(\sum_{g\in G} T(g)\right) = |G|$.

*Bizonyítás.* Vegyük észre, hogy a függvények felírhatók a következő alakokban:

$$f = \sum_{g\in G} f(g)\delta_g \quad h = \sum_{g\in G} h(g)\delta_g$$

Konvolválva őket kapjuk, hogy

$$\mathbb{1}_G = \sum_{g\in G} \delta_g \left(\sum_{i+j=g} f(i)g(j)\right)$$

Ha most ezt a függvényt szummázzuk minden $g$-re, akkor kapjuk, hogy

$$|G| = \sum_{i,j \in G} f(i)g(j) = \left(\sum_{g \in G} f(g)\right)\left(\sum_{g \in G} h(g)\right)$$

□

**3.1.7. Lemma.** Tegyük fel, hogy $S$ gyengén parkettázza $G$-t $T$-vel. Ekkor $i \neq 1$ és $(S - S) \cap A_i \neq \varnothing$ esetén $d_i = 0$.

*Bizonyítás.* Legyen $\widetilde{T}(t) = \sum_{i=1}^{n} d_i B_i(t)$. 3.1.4 lemma alapján $\widetilde{T} * \mathbb{1}_S = \mathbb{1}_G$, vagyis tetszőleges $t \in G$ esetén

$$\sum_{g \in G} \widetilde{T}(t-g)\mathbb{1}_S = \sum_{s \in S} \widetilde{T}(t-s) = \sum_{s \in S} \sum_{i=0}^{n} d_i B_i(t-s) = 1$$

A feltétel alapján $s_1 - s_2 \in A_i$, tehát $s_1$-t behelyettesítve $1 + d_i \leq 1$, vagyis $d_i = 0$. □

**3.1.8. Következmény.** $c_i d_i = 0 \ \forall i \neq 1$.

*Bizonyítás.* Ha $c_i$ pozitív, akkor $A_i \cap S \neq \varnothing$. Mivel $0 \in S$, így a lemma alapján $d_i = 0$. □

## 3.2. A módszer alkalmazása

Rátérünk a Fuglede sejtés spektrálitásból parkettázás irányának bizonyítására néhány csoport esetén. Ehhez a fő tételünk 3.1.1 tétel lesz. Meg fogjuk mutatni, hogy egy gyenge parketta szükségszerűen egy halmazból jön. 3.1.5 állítás miatt elég azt belátnunk, hogy $d_i$-k csupán 0 vagy 1 értéket vehetnek fel.

Egy technikai lemmára még szükségünk lesz. Emlékezzünk vissza, hogy $(S \implies T)(H)$ azt jelenti, hogy ha $A \subset H$ spektrális, akkor parkettáz.

**3.2.1. Lemma.** Tegyük fel, hogy $S \subset G$ spektrális és $\langle S \rangle \neq G$. Továbbá igaz $(S \implies T)(H)$, ahol $H$ $G$-nek tetszőleges valódi részcsoportja. Ekkor $S$ parkettáz.

*Bizonyítás.* Mivel $S$ pontosan akkor spektrális $G$-ban, ha $\langle S \rangle \subset G$, így létezik $T \subset \langle S \rangle$, melyre $S \oplus T = \langle S \rangle$. Ha $B$ $\langle S \rangle$ mellékosztályainak reprezentánsrendszere, akkor $S \oplus T \oplus B = G$, vagyis $S$ parkettáz. □

Innentől minden rendelkezésünkre áll, hogy belássuk a következő tételt:

**3.2.2. Tétel.** Legyen $G = \mathbb{Z}_{pq}$, és $S \subseteq G$ spektrális. Ekkor S parkettáz.

*Bizonyítás.* Tegyük fel, hogy $0 \in S$. 3.1.1 alapján $S$ gyengén parkettázza $G$-t valamilyen $T$-vel. $g \mapsto kg$, $(k, |G|) = 1$ függvény orbitjait jelölje $A_0 = \{0\}, A_p, A_q, A_{pq}$, az utolsó három sorra a $p, q, pq$ rendű elemeket tartalmazzák. Felhasználva az előző fejezet jelöléseit:

- $B_i = \sum_{g \in A_i} \delta_g$
- $\mathbb{1}_G = B_0 + B_p + B_q + B_{pq}$
- $\widetilde{\mathbb{1}_S} = c_0 B_0 + c_p B_p + c_q B_q + c_{pq} B_{pq}$
- $\widetilde{T} = d_0 B_0 + d_p B_p + d_q B_q + d_{pq} B_{pq}$

3.1.4 lemmából kapjuk, hogy

$$(c_0B_0 + c_pB_p + c_qB_q + c_{pq}B_{pq}) * (d_0B_0 + d_pB_p + d_qB_q + d_{pq}B_{pq}) = \mathbb{1}_G \tag{3.2}$$

1.1.2 állítás miatt tagonként szorozhatunk, vagyis elég kiszámítani $c_iB_i * d_iB_j$ szorzatokat. Vegyük észre, hogy 3.1.8 következmény miatt a $B_i * B_i,\ i \neq 0$ szorzatok együtthatói 0-k.
Most megadjuk $B_pB_{pq}$ szorzatot. Legyen $(a_1, a_2) \in A_{pq}$. Ekkor $(a_1-g, a_2)+(g, 0) = (a_1, a_2),\ (a_1-g, a_2) \in A_{pq},\ (g, 0) \in A_p$ pontosan akkor áll fenn, ha $g \neq 0,\ a_1$, vagyis $g$-t $p-2$ félének választhatjuk meg. Legyen $(0, a_1) \in A_q$. $(g, a_1) + (-g, 0) = (0, a_1),\ (ag, a_1) \in A_{pq},\ (-g, 0) \in A_p$ pontosan akkor áll fenn, ha $g \neq 0$, tehát $g$ $p-1$ féle lehet. Ugyanígy látható, hogy $A_1$ és $A_p$ halmazbeli elem nem rakható ki ezek összegeként. Hasonló gondolatmenettel meg tudjuk, mondani az összes lehetséges szorzatot. Ezek

$$\begin{aligned}
&B_0B_i = B_i \quad B_pB_q = B_{pq}\\
&B_pB_{pq} = (p-1)B_q + (p-2)B_{pq}\\
&B_qB_{pq} = (q-1)B_p + (q-2)B_{pq}
\end{aligned}$$

3.2 szorzatot kibontva az együtthatókra kapjuk, hogy

$$\begin{aligned}
&d_p + c_p + (c_qd_{pq} + d_qc_{pq}(q-1)) = 1\\
&d_q + c_q + (c_pd_{pq} + d_pc_{pq})(p-1) = 1\\
&c_pd_q + c_qd_p + d_{pq} + c_{pq} + (p-2)(c_pd_{pq} + d_pc_{pq}) + (q-2)(c_qd_{pq} + d_qc_{pq}) = 1.
\end{aligned}$$

A 6 darab ismeretlenből 3.1.8 következmény miatt legalább 3 nulla. Most ezeket az eseteket nézzük végig. Mindegyik esetben azt próbáljuk belátni $d_i \in \{0, 1\}$, hiszen 3.1.5 állítás miatt ekkor $T$ parketta.

**1. eset** $c_p = c_q = c_{pq} = 0$. Ez azt jelenti, hogy $S = \{0\}$, ami tényleg parkettáz.

**2. eset** $c_p = c_q = d_{pq} = 0$. Helyettesítsük be ezeket az egyenletekbe.

$$\begin{aligned}
&d_p + d_qc_{pq}(q-1) = 1\\
&d_q + d_pc_{pq}(p-1) = 1\\
&c_{pq} + (p-2)d_pc_{pq} + (q-2)d_qc_{pq} = 1.
\end{aligned}$$

Ekkor $c_{pq} > 0$ a 3. egyenlet miatt. Ha létezik $(s, s_1),\ (s, s_2) \in S,\ s_1 \neq s_2$, akkor 3.1.7 alapján $d_q = 0$, amiből következik, hogy $d_q = 1$, amivel készen vagyunk. Hasonló gondolatmenetet kapunk $d_p$-re. Tehát feltehető, hogy ilyen párok nincsenek. Ha $|S| = 2$, akkor 3.1-be megfelelő elemet helyettesítve kapjuk, hogy $d_p = d_q = 1$. Legyen $|S| \geq 3$. Ha $(s_1, s_2), (s_3, s_4) \in S$, akkor $(s_1, s_4)$-et behelyettesítve 3.1-be azt kapjuk, hogy $d_p + d_q \leq 1$.
Az $S$-beli elemek lehetséges koordinátáinak értékeit megszámolva kapjuk, hogy $|S| \leq \min(p-1, q-1)+1$, így $c_{pq} \leq \frac{\min(p-1,q-1)}{(p-1)(q-1)}$. Legyen $p < q$. Az első egyenletbe a becslést beírva kapjuk, hogy $1 \leq d_p + d_q$. Megkaptuk, hogy $d_p + d_q = 1$. Behelyettesítve az első, majd a második egyenletbe (és felhasználva, hogy $d_p,\ d_q \neq 0$) azt kapjuk, hogy $\frac{1}{p-1} = c_{pq} = \frac{1}{q-1}$, ellentmondás.

**3. eset** $c_p = d_q = c_{pq} = 0$. Ekkor $S$-ben csak a 0 és $p$ rendű elemek vannak, amik nem generálják $G$-t. Továbbá $p$ rendű ciklikus csoportban, ha egy halmaz spektrális akkor parkettáz is, így 3.2.1 lemma miatt készen vagyunk.

**4. eset** $c_p = d_q = d_{pq} = 0$. Legyen $g \in A_p$. 3.1 egyenletből

$$\sum_{s \in S} d_pB_p(g-s) = 1$$

$B_p(g-s)$ csak akkor lesz nem-nulla, ha $s = 0$. Vagyis $d_p = 1$.

**5. eset** $d_p = d_q = c_{pq} = 0$. Tegyük fel, hogy létezik $(a_1, 0) \in A_p \cap S$ és $(0, a_2) \in A_q \cap S$. Ekkor 3.1.7 lemma miatt kapjuk, hogy $d_{pq} = 0$. Ellenkező esetben $c_p = 0$ vagy $c_q = 0$, amivel visszakaptunk egy előző esetet. $\square$

**3.2.3. Tétel.** Legyen $G = \mathbb{Z}_p^2$, és $S \subseteq G$ spektrális. Ekkor $S$ parkettázza $G$-t.

*Bizonyítás.* A bizonyítás hasonló az előzőhöz. Ekkor az orbitok a $A_0 = \{0\}$, illetve a $p+1$ darab valódi részcsoport.

$$B_i B_j = \sum_{k=1}^{p+1} B_k - B_i - B_j \ , \ i \neq j \ i \neq 0 \ j \neq 0$$
$$B_i B_0 = B_i$$
$$B_0 B_0 = B_0$$

A $\sum_{i=0}^{p+1} c_i B_i * \sum_{i=0}^{p+1} d_i B_i$ szorzatot kibontva az együtthatók

$$c_0 d_k + d_0 c_k + \sum_{\substack{i,j \neq 0 \\ i,j \neq k}} c_i d_j = 1$$

Feltehető, hogy $0 \notin S$. Legyen $D = \sum_{i \geq 1} d_i$ és $C = \sum_{i \geq 1} c_i$. A fenti egyenlet a következőképpen írható fel:

$$c_k + (D - d_k)(C - c_k) = 1$$

Ha $d_i = 0$, akkor

$$c_i(1 - D) = 1 - CD \tag{3.3}$$

**1. eset.** $1 - D \neq 0$. Mivel $c_i$ nem függ $i$-től, így $1 - D$-val átosztva azt kapjuk, hogy ha $c_i, c_j > 0$, akkor $c_i = c_j$. Az is feltehető, hogy $c_j$ és $d_j$ közül legalább az egyik pozitív, mert ha lenne ilyen pár, akkor $1 - CD = 0$ lenne, így mindegyik $c_i$ is 0 lenne.

Legyen $c = |\{i : i > 0 \ c_i > 0\}|$ és $d = |\{i : i > 0 \ d_i > 0\}|$. Az előbbiek alapján $c + d = p + 1$. Szummázzuk 3.3 egyenletet minden pozitív $c_i$-re:

$$C = c\frac{1 - CD}{1 - D}$$

$c_i$ definíciója alapján és $0 \notin S$ miatt igaz, hogy $c(p-1)c_i = (p-1)C = |S|$. 3.1.6 állítás alapján $p \mid |S|$. Mivel $(p-1)c_i \leq p - 1$, így $p \mid c$, de $c \leq p + 1$, tehát $c = p$. Így $d = 1$, ami azt jelenti, hogy a gyenge parketta csak egyetlen $A_k$-n nem azonosan 0, és itt nincs eleme $S$-nek.

3.1 egyenlet most a következő alakba írható:

$$\sum_{s \in S} (d_0 B_0(t - s) + d_k B_k(t - s)) = 1 \ \forall t \in G$$

Helyettesítsünk be egy $t \in A_k$ elemet. $t \notin S$, tehát minden $d_0$ együtthatós tag kiesik. Ha lenne $s \in S$, hogy $t - s \in A_k$, akkor $s \in A_k$ is teljesülne, hiszen $A_k \cup \{0\}$ részcsoport. De ez ellentmondás, mert $A_k \cup \{0\}$ nem tartalmaz $S$-beli elemet.

**2. eset** $1 = D$. A feltételből következik, hogy $G \setminus \{0\}$-n összegezve a gyenge parkettát az eredmény $p - 1$, így egész $G$-n pedig $p$. 3.1.6 állítás alapján pedig $|S|p = p^2$, így $|S| = p$. Viszont az is kiolvasható az egyenletekből, hogy ekkor $1 = C$, vagyis $\sum_{i=1}^{p+1} \frac{|S \cap A_i|}{p-1} = 1$. Mivel $0 \notin S$ így azt kaptuk, hogy $|S| = p - 1$, ami ellentmondás. $\square$

**3.2.4. Tétel.** Legyen $G = \mathbb{Z}_{p^2}$, és $S \subseteq G$ spektrális. Ekkor $S$ parkettázza $G$-t.

*Bizonyítás.* A partíció most $A_0 = \{0\}, A_p = \{p \text{ rendű elemek}\}, A_{p^2} = \{p^2 \text{ rendű elemek}\}$. Ha $c_{p^2} = d_p = 0$, akkor 3.2.1 lemma miatt készen vagyunk. Tehát egyetlen nemtriviális eset van $c_p = d_{p^2} = 0$. $|S \cap A_{p^2}| \leq p - 1$, mert ha $k_1 p + l,\ k_2 p + l$ különböző $S$-beli elemek, akkor a különbségük $A_p$-beli, tehát 3.1.7 lemma miatt $d_p = 0$ állna fenn, amivel készen vagyunk. Vagyis ebben az esetben $|S|$ és a spektruma 1 elemű.

Legyen $kp + l \notin S$ és $s \in S$, és teljesüljön rájuk, hogy a különbségük $A_p$-beli. Az előzőek alapján legfeljebb egyetlen ilyen $s$ lehet. Ezek alapján 3.1-be $kp+l$ elemet behelyettesítve kapjuk, hogy $d_p = 1$. □

# 4. fejezet

# Parkettázásból Spektralitás

## 4.1. Rédei tétele

A parkettázás fogalmát értelemszerűen ki lehet terjeszteni több komponensre: $A_1, A_2, \ldots, A_m \subset G$ halmazrendszer parkettázza $G$-t, ha minden $G$-beli elem egyértelműen előáll $a_1 + a_2 + \ldots + a_m, a_i \in A_i$ alakban. Jelölése $A_1 \oplus A_2 \oplus \ldots \oplus A_m = G$. A következő tételt Rédei tételnek szokás hívni, először [19]. Mi csak néhány speciális feltétel mellett fogjuk bebizonyítani a tételt. A $\mathbb{Z}_p^2$ eset bizonyítása [2] cikkbeli.

**4.1.1. Tétel** (Rédei)**.** Tegyük fel, hogy $A_1 \oplus A_2 \oplus \ldots \oplus A_m = G$, továbbá $|A_i|$ prím és $0 \in A_i$ minden $i$-re. Ekkor létezik $j$, melyre $A_j$ részcsoport.

Idézzük fel hogy egy $A(x)$ polinom deriváltját $A'(x)$-el jelöljük.

**4.1.2. Tétel.** Legyen $A \oplus B = \mathbb{Z}_p^2$, továbbá $0 \in A,\ 0 \in B$ és $|A| = |B| = p$. Ekkor $A$ vagy $B$ részcsoport.

*Bizonyítás.* Vegyünk egy nemnulla $a$ elemet $A$-ból. Ha $\langle a \rangle = B$, akkor készen vagyunk, egyébként pedig vegyünk egy $b \notin \langle a \rangle$ $B$-beli elemet. Ekkor $a$ és $b$ vektorok már generálják $\mathbb{Z}_p^2$-et, mint vektorteret. Írjuk fel a két halmazt ezekkel a vektorokkal, ahol $a_i, \alpha_i, b_i, \beta_i \in \mathbb{Z}_p$ minden $i$-re:

$$A = \{a_0 u + \alpha_0 v, a_1 u + \alpha_1 v, \ldots, a_{p-1} u + \alpha_{p-1} v\},$$
$$B = \{b_0 u + \beta_0 v, b_1 u + \beta_1 v, \ldots, b_{p-1} u + \beta_{p-1} v\}.$$

Legyen $\xi = e^{\frac{2\pi i}{p}}$. Az $(y, 1) \in \mathbb{Z}_p^2$ elemhez tartozó karakter $\chi_{(y,1)}(iu + jv) = \xi^{iy+j}$.

Egy $\chi \in \hat{G}$ reprezentációra és $A \subset G$ részhalmazra vezessük be a $\chi(A) := \sum_{a \in A} \chi(a)$ jelölést. Már láttuk, hogy $0 = \chi_{(y,1)}(G)$. Könnyen ellenőrizhető, hogy $\chi_y(A)\chi_y(B) = \chi_y(G)$. Mivel $y$ $p$ különböző értéket vehet fel, így $\chi_{(y,1)}(A)$ vagy $\chi_{(y,1)}(B)$ legalább $\frac{p+1}{2}$ $y$ értékre 0. Tegyük fel, hogy $\chi_y(A)$ rendelkezik ezzel a tulajdonsággal. Ha ez 0-t vesz fel egy $y$-ra az azt jelenti, hogy $a_i y + \alpha_i$ teljes maradékrendszert alkot modulo $p$. Az ilyen $y$-ok halmazát jelöljük $Y$-nal.

Legyen $\alpha'_0, \ldots, \alpha'_m$ azok a különböző értékek, amik előfordulnak $\alpha_0, \ldots \alpha_{p-1}$ között. Definiáljuk a következő polinomokat $\mathbb{Z}_p$ fölött:

$$D(x, y) = \prod_{i=0}^{p-1} (x - a_i y - \alpha_i) \quad E(x) = D(x, 0) \quad F(x) = \prod_{i=0}^{m} (x - \alpha'_i)$$

Rögzített $y$-ra $D(x, y) \in \mathbb{Z}_p[y][x]$ együtthatói legyenek $d_i(y)$-k, $E(x)$ együtthatói pedig $e_i$. Nyilván $d_i(0) = e_i$.

Rögzített $y \in Y$-ra $D(x,y) = x^p - x$, hiszen a kis Fermat tétel miatt $\mathbb{Z}_p$ összes eleme gyöke a $p$ fokú $x^p - x$ polinomnak. Tudjuk, hogy

$$\prod_{i=0}^{p-1}(x-i) = \sum_{i=0}^{p}(-1)^i \sigma_i(x_1, x_2, \ldots, x_{p-1})x^{p-i},$$

ahol $\sigma_i(x_1, x_2, \ldots, x_{p-1})$ az $i$-edik szimmetrikus polinom. Így

$$d_{p-i}(y) = (-1)^i \sigma_i(a_0 y + \alpha_0, \ldots, a_{p-1}y + \alpha_{p-1}) = 0$$

$d_{p-i}(y)$ polinom foka legfeljebb $i$, és legalább $\frac{p+1}{2}$ gyöke van, így $0 \leq i \leq \frac{p-1}{2}$ esetekre 0. Ezért $E(x) = (\sum_{i=2}^{\frac{p-1}{2}} e_i x^i) + x^p$. Először gondoljuk meg, hogy $E(x) \mid F(x)E'(x)$, ahol $E'(x)$ az $E(x)$ polinom deriváltját jelöli. Az nyilvánvaló, hogy $F(x)$ osztja $E(x)$-et. Ha $\alpha'_i$ $k$-szoros gyöke $E(x)$-nek, akkor $F(x)E'(x)$ legalább $k$-szoros gyöke, hiszen $F(x)$-nek egyszeres, $E'(x)$-nek pedig legalább $k-1$-szeres.

Legyen $G(x) = E(x) - (x^p - x)$. Mivel $F(x)$ osztja $(x^p - x)$-et, így $G(x)$-et is. Vegyük észre, hogy $G'(x) = E'(x) + 1$. Vagyis

$$E(x) \mid F(x)E'(x) \mid G(x)(G'(x) - 1)$$

$E(x)$, $G(x)$, és $G'(x) - 1$ fokai sorra $p$, $\frac{p-1}{2}$, és $\frac{p-3}{2}$, vagyis az oszthatóság csak úgy állhat fönn, ha $G(x)(G'(x)-1)$ a nullapolinom. $G(x)$ nem lehet a nullapolinom, mert szerepel benne egy $x$-es tag. Vagyis $1 = G'(x) = E'(x) + 1$, $E'(x) = 0$. Mivel $E'(x) = \sum_{i=2}^{\frac{p-1}{2}} ie_i x^{i-1}$, így $e_i i = 0$ minden $i$-re, ami csak úgy lehet, hogy $e_i = 0$ minden $2 \leq i \leq \frac{p-1}{2}$, vagyis $E(x) = x^p$. Ez pontosan azt jelenti, hogy $\alpha_i = 0$, minden $i$-re.

□

**4.1.3. Állítás.** Tegyük fel, hogy $A \oplus B = \mathbb{Z}_n$. Ekkor a következőkből legalább az egyik igaz:

1. Nincs olyan $A - A$-beli elem, mely relatív prím $|B|$-hez.
2. Nincs olyan $B - B$-beli elem, mely relatív prím $|A|$-hoz.

*Bizonyítás.* Tegyük fel, hogy egyik sem igaz, vagyis létezik $a = a_1 - a_2 \in A - A$ és $b = b_1 - b_2 \in B - B$, hogy $(b, |A|) = 1$ és $(a, |B|) = 1$. A Tijdeman lemma alapján ekkor $bA \oplus aB = \mathbb{Z}_n$. De ekkor $ba_1 + ab_2 = ba_2 + ab_1$, ami nem lehet. □

**4.1.4. Tétel.** Legyen $\mathbb{Z}_{p^2} = A \oplus B$, és $0 \in A, B$. Ekkor $A$ vagy $B$ részcsoport.

*Bizonyítás.* $\Phi_p(x)$ osztja $A(x)$-t vagy $B(x)$-t. Tegyük fel, hogy $A(x)$-et osztja.

$$A(x) \equiv \sum_{i=0}^{d-1} |A_{i \bmod p}| x^i \mod x^p - 1$$

Továbbá a feltétel miatt

$$A(x) \equiv (1 + x + \ldots + x^{p-1})G(x) \equiv (1 + x + \ldots + x^{p-1})G(1) \mod x^p - 1$$

A két egyenletet összevetve kapjuk, hogy $|A_{i \bmod p}|$ konstans, vagyis csak 1 lehet. Ha viszont ez a helyzet, akkor $A - A$-nak van olyan eleme, mely relatív prím $|B|$-hez. Az előző állítás alapján minden $B - B$-beli elem osztható $p$-vel. Mivel feltettük, hogy $0 \in B$ ezért $B$ elemei éppen a $p$ rendű elemek, vagyis $B$ részcsoport. □

## 4.2. Parkettázásból spektralitás

Az ötlet, hogy a Rédei tételt használjuk fel a bizonyítás során [12] cikkbeli.

**4.2.1. Tétel.** Ha $\mathbb{Z}_p^2$ egy részhalmaza parkettáz, akkor spektrális is.

*Bizonyítás.* Legyen $A \oplus B = \mathbb{Z}_p^2$. Feltehető, hogy $0 \in A \cap B$. A Rédei tétel miatt feltehető, hogy $A$ részcsoport. Már láttuk, hogy ekkor $(A, A)$ spektrális pár. $B$ ekkor $A$ mellékosztályainak egy reprezentánsrendszere. Legyen $T$ $A$-nak a merőleges kiegészítő altere. Ekkor

$$\sum_{b \in B} \chi_{t_1 - t_2}(b) = \sum_{b \in B} \chi_t(b) = \sum_{b \in B} e^{\frac{2\pi i \langle t, b \rangle}{p}}$$

$T$ választása miatt $\langle t, b \rangle$ befutja az összes lehetséges értéket, így az összeg 0. $\square$

**4.2.2. Tétel.** Ha a $\mathbb{Z}_N$ négyzetmentes ciklikus csoport egy részhalmaza parkettáz, akkor spektrális is.

*Bizonyítás.* Következik abból, hogy teljesülnek a Coven-Meyerowitz feltételek, amiből pedig következik a spektralitás. $\square$

**4.2.3. Tétel.** Ha $\mathbb{Z}_{p^2}$ egy részhalmaza parkettáz, akkor spektrális.

*Bizonyítás.* Legyen $A \oplus B = \mathbb{Z}_{p^2}$. Feltehető, hogy $0 \in A \cap B$, és a rédei tétel miatt az is, hogy $A$ részcsoport. Ekkor $A$ spektrális, $B$ pedig teljes maradékrendszer $\bmod p$. Azt állítjuk, hogy $B$-nek spektruma lesz $A$. Ugyanis $a_1, a_2 \in A$ különböző elemekre

$$\sum_{b \in B} \chi_{a_1 - a_2}(b) = \sum_{b \in B} \chi_a(b) = \sum_{b \in B} e^{\frac{2\pi i a b}{p^2}}$$

$ab$ nyilván osztható lesz $p$-vel, és $\frac{ab}{p}$ az összes lehetséges értéket befutja $\bmod p$, így a szumma eltűnik. $\square$

# 5. fejezet

# Ellenpéldák

## 5.1. Hadamard Mátrixok

**5.1.1. Definíció.** Egy $\mathbb{A} \in \mathbb{C}^{n\times n}$ mátrixot komplex Hadamard mátrixnak hívunk, ha teljesülnek rá a következő feltételek:

- $|\mathbb{A}_{i,j}| = 1$ minden $1 \leq i, j \leq n$ indexre,
- $\mathbb{A}\mathbb{A}^* = nI$, ahol $\mathbb{A}^*$ az $\mathbb{A}$ mátrix transzponáltjának konjugáltja, vagyis adjungáltja.

Ha $\mathbb{A}_{i,j}$ egy $k$-adik egységgyök, akkor $A$-t $B(n,k)$, vagy Butson típusú Hadamard mátrixnak hívjuk. A $B(n,2)$ típusú mátrixokat valós hadamard mátrixoknak is hívjuk.

**5.1.2. Állítás.** Ha $\mathbb{A} \in \mathbb{C}^{n\times n}$ komplex Hadamard mátrix, akkor sorai (oszlopai) ortogonális bázist alkotnak $\mathbb{C}^n$-ben.

*Bizonyítás.* Ha $v_1$ és $v_2$ két különböző sora $\mathbb{A}$-nak, akkor definíció alapján $v_1\overline{v_2}^T = 0$ □

Megemlítjük a valós Hadamard mátrixok egy fontos tulajdonságát és egy hozzátartozó híres sejtést.

**5.1.3. Állítás.** Legyen $\mathbb{A} \in \mathbb{C}^{n\times n}$ $B(n,2)$ típusú. Ekkor $n \mid 4$, vagy $n = 1, 2$.

*Bizonyítás.* Az nyilvánvaló, hogy $n$ nem lehet páratlan, hiszen két páratlan hosszú $1, -1$ koordinátájú vektor skalárszorzata nem lehet 0.

Legyen $\mathbb{A}$ $B(2(2k+1), 2)$ típusú. Oszlop- és sorcserékkel, illetve oszlopok, sorok $-1$-el való szorzásával elérhető, hogy az első sor minden koordinátája 1 legyen. Ekkor minden további sorban pontosan $2k+1$ darab $-1$-es kell, hogy legyen. Rendezzük a koordinátákat 4 osztályba aszerint, hogy a 2. és 3. sorból milyen típusú koordináták találkoznak. $x, y, z, w$ legyen sorra a pozitív-pozitív, negatív-negatív, pozitív-negatív, negatív-pozitív típusúak elemszáma. Szorozva az 1. és 2. sort, majd a 2. és 3. sort kapjuk, hogy

$$x - y + z - w = 0$$
$$x + y - z - w = 0$$

amiből következik, hogy $x = w$, vagyis $x + w$ páros. De $x + w$ éppen azoknak a koordinátákatnak az elemszáma, amelyek pozitívak a harmadik sorban, ami $2k + 1$, vagyis páratlan.

$n = 2$ esetre példa a

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

mátrix.

Az $n = 1$ esetet az olvasóra bízzuk. □

**5.1.4. Sejtés.** Minden $4n$ alakú számra létezik $B(4n, 2)$ típusú Hadamard mátrix. [18]

**5.1.5. Állítás.** Legyen $\mathbb{A} \in \mathbb{C}^{n\times n}$ a $G$ csoport karaktertáblája. $(T, S)$, $T = \{t_1, t_2, \dots t_k\}$, $S = \{s_1, s_2, \dots s_k\}$ pár akkor és csak akkor spektrális, ha $\mathbb{A}$-nak a $t_1, t_2, \dots t_k$ oszlopok és $s_1, s_2, \dots s_k$ sorok által meghatározott részmátrixa komplex Hadamard.

*Bizonyítás.* A részmátrix pontosan akkor Hadamard, ha tetszőleges $(\chi_{s_1}(t_1), \chi_{s_1}(t_2), \dots \chi_{s_1}(t_k))$ és $(\chi_{s_2}(t_1), \chi_{s_2}(t_2), \dots \chi_{s_2}(t_k))$ különböző sorára, a

$$(\chi_{s_1}(t_1), \chi_{s_1}(t_2), \dots \chi_{s_1}(t_k))(\overline{\chi_{s_2}(t_1)}, \overline{\chi_{s_2}(t_2)}, \dots \overline{\chi_{s_2}(t_k)})^T = \sum_{i=1}^{k} \chi_{s_1 - s_2}(t_i)$$

kifejezés 0. Az egyenlőség jobb oldala pont a spektralitás definíciója. □

**5.1.6. Definíció.** Egy $\{a_{i,j}\}_{i,j=1}^n = \mathbb{A} \in \mathbb{Z}_m^{n\times n}$ mátrixot log-Hadamard mátrixnak nevezünk $\mathbb{Z}_m$ felett, ha $\{e^{\frac{2\pi i a_{i,j}}{m}}\}_{i,j=1}^n = \mathbb{A}'$ mátrix komplex Hadamard.

Emlékezzünk arra, hogy ha $a \in \mathbb{Z}_p^d$, akkor az ehhez tartozó karakter $\chi_a = e^{\frac{2\pi i \langle a, x\rangle}{p}}$.

**5.1.7. Tétel.** Legyen $p$ prím. Ekkor a következő két kijelentés ekvivalens:

1. Létezik $\mathbb{Z}_p^d$-ben $(S, T)$ spektrális pár, melyre $|S| = |T| = m$
2. Létezik egy $m \times m$-es log-Hadamard mátrix $\mathbb{Z}_p$ felett, melynek rangja legfeljebb $d$.

*Bizonyítás.* Legyenek $\mathbb{S}$ és $\mathbb{T}$ $m \times d$ méretű mátrixok, melyeknek sorai $S$-beli, illetve $T$-beli vektorok. Ekkor $\mathbb{S}$ és $\mathbb{T}$ rangja legfeljebb $d$ lehet. Az $\mathbb{L} = \mathbb{S}\mathbb{T}^T$ $m \times m$-es mátrix. $\mathbb{L}$ rangja legfeljebb a minimuma $\mathbb{S}$ és $\mathbb{T}$ rangjának, vagyis legfeljebb $d$. $\mathbb{L}$ $i$-edik sorának $j$-edik eleméhez tartozó eleme $\langle s, t\rangle$ alakú valamilyen $s, t$ $\mathbb{S}$-beli, illetve $\mathbb{T}$-beli sorokra. Viszont ez éppen $s$ értéke a $t$-hez tartozó karakternél, vagyis $\mathbb{L}$ részmátrixa $\mathbb{Z}_p^d$ karaktertáblájának.

Most legyen adva egy $m \times m$-es $\mathbb{L}$ log-Hadamard mátrix $\mathbb{Z}_p$ felett, melynek rangja legfeljebb $d$. Ekkor $\mathbb{L}$ egy $\mathbb{Z}_p^m \mapsto \mathbb{Z}_p^m$ lineáris leképezést. Továbbá a rangra tett feltétel miatt $\mathbb{L}$ képe legfeljebb $d$ dimenziós altér. Ez a lineáris leképezés kifejezhető, $\mathbb{A} : \mathbb{Z}_p^m \mapsto \mathbb{Z}_p^k$ és $\mathbb{B} : \mathbb{Z}_p^k \mapsto \mathbb{Z}_p^m$ lineáris leképezések kompozíciója, ahol $B$ a természetes beágyazás és $k \leq d$. Bázist választva $\mathbb{A}$-t és $\mathbb{B}$-t reprezentálhatjuk $k \times m$-es és $m \times k$ mátrix alakban. Tehát $\mathbb{L} = \mathbb{B}\mathbb{A}$.

$\mathbb{B}$ sorai különbözőek. Ellenkező esetben $\mathbb{L}$-nek is van két ugyanolyan sora, de ekkor nem lehet $\mathbb{L}$ log-Hadamard mátrix, hiszen a hozzárendelt Hadamard mátrixnak ez a két sora nem lenne merőleges. Ugyanez elmondható $\mathbb{A}$ mátrix oszlopaira. Legyen $S, T \subset \mathbb{Z}_p^k$ $\mathbb{A}$ sorai, illetve $\mathbb{B}$ sorai. Ekkor $|S| = |T| = m$. Vagyis $S$ és $T$ által meghatározott részmátrixa a karaktertáblának log-Hadamard, így az előző állítás miatt ez spektrális pár $\mathbb{Z}_p^k \subset \mathbb{Z}_p^d$-ben, amivel készen vagyunk. □

## 5.2. Ellenpéldák

Konstruálni fogunk a Fuglede sejtésre ellenpéldákat $\mathbb{Z}_p^d$, ahol $p$ prím. $p = 12$ esetén $d = 12$, $p$ páratlan prím esetén $d = 5$, alkalmas feltételeket szabva $p$-re pedig tovább fogjuk csökkenteni $d$-t 4-re. Azonban megmutatható, hogy minden páratlan prímre jó választás a $d = 4$, lásd [5]. A szekció [1] alapján lett feldolgozva.

A következő tételben szereplő mátrixot [23]-ban használták ellenpélda gyártásra.

**5.2.1. Tétel.** Létezik olyan $S \in \mathbb{Z}_2^{12}$ halmaz, ami spektrális, de nem parkettáz.

*Bizonyítás.* Nézzük a következő mátrixot:

$$
\begin{pmatrix}
+1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1\\
+1 & +1 & -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & -1 & +1\\
+1 & +1 & +1 & -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & -1\\
+1 & -1 & +1 & +1 & -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1\\
+1 & +1 & -1 & +1 & +1 & -1 & +1 & -1 & -1 & -1 & +1 & +1\\
+1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 & -1 & -1 & -1 & +1\\
+1 & +1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 & -1 & -1 & -1\\
+1 & -1 & +1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 & -1 & -1\\
+1 & -1 & -1 & +1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 & -1\\
+1 & -1 & -1 & -1 & +1 & +1 & +1 & -1 & +1 & +1 & -1 & +1\\
+1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & -1 & +1 & +1 & -1\\
+1 & -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & -1 & +1 & +1
\end{pmatrix}
$$

Kiszámolható, hogy ez egy Hadamard mátrix. Az ebből képzett log-Hadamard mátrix rangja legfeljebb 12, így létezik $(S, T)$ spektrális pár, melyre $|S| = |T| = 12$. Viszont a 12 nem osztja $2^{12}$, így nem parkettázhat. $\square$

**5.2.2. Megjegyzés.** Ha nem lenne a fenti mátrix a kezünkbe adva, hanem csak az lenne a feladatunk, hogy keressünk egy spektrális nem parkettázó halmazt és írjuk fel spektrumával mátrix alakban, 5.1.3 állítás alapján egy $12 \times 12$ méretű mátrix keresése lenne a legtermészetesebb, ugyanis 12 a legkissebb nem 2 hatvány, melyre létezhet $B(12, 2)$ típusú mátrix.

Amíg mást nem mondunk legyen $p$ páratlan prím. Most definiálni fogunk egy $2p \times 2p$-es $\mathbb{L}$ mátrixot $\mathbb{Z}_p$ felett. A célunk az lesz, hogy belássuk, hogy ez log-Hadamard.

Definiáljuk az

$$\mathbb{L} = \begin{pmatrix} \mathbb{A} & n\mathbb{A} \\ \mathbb{B} & \mathbb{C} \end{pmatrix}$$

ahol $\mathbb{A}$, $\mathbb{B}$, $\mathbb{C}$ mind $p \times p$ méretű mátrixok $\mathbb{A}_{i,j} = 2ij - i^2$, $\mathbb{B}_{i,j} = (j - ni)^2$, $\mathbb{C}_{i,j} = n(i - j)^2$, ahol $0 \leq i, j \leq p - 1$ és $n$ kvadratikus nemmaradék $\mod p$.

**5.2.3. Definíció.** Azt mondjuk, hogy a $v \in \mathbb{Z}_p^d$ vektor kiegyensúlyozott, ha $v$ koordinátái között minden $\mathbb{Z}_p$-beli elem ugynannyiszor szerepel.

Alkalmazni fogjuk a következő jelöléseket. Ha $f : \{0, 1, \dots, p-1\} \mapsto \mathbb{Z}_p$ és $g : \{0, 1, \dots, p-1\} \mapsto \mathbb{Z}_p$ függvények, akkor az $(f(0), f(1), \dots, f(p-1))$ vektorra az $[f(k)]$ jelölést alkalmazzuk és az $(f(0), f(1), \dots, f(p-1), g(0), g(1), \dots g(p-1))$ $2p$ hosszú vektorra az $[f(k) \mid g(k)]$. Az indexeket $k$-val fogjuk jelölni.

**5.2.4. Lemma.** Az $\mathbb{A}$ négyzetes mátrix pontosan akkor log-Hadamard, ha bármely két sorának (oszlopának) különbsége kiegyensúlyozott.

*Bizonyítás.* Legyen $\mathbb{A}$ log-Hadamard, és $\mathbb{A}' = \{e^{\frac{2\pi i a_{i,j}}{p}}\}_{i,j=1}^{p}$ a hozzátartozó Hadamard mátrix. Mivel $\mathbb{A}'$ Hadamard, így tetszőleges $i \neq j$-re

$$\sum_{k=1}^{p} e^{\frac{2\pi i (a_{i,k} - a_{j,k})}{p}} = 0$$

$p$-edik egységgyökök összege, akkor és csak akkor lehet 0, ha az összegben mindegyik egységgyök ugyanannyiszor szerepel. Vagyis az $a_{i,k} - a_{j,k},\ k = 1, 2, 3 \dots p$ különbségek között, minden $\mathbb{Z}_p$-beli elem ugyanannyiszor szerepel. $\square$

**5.2.5. Állítás.** Az $\begin{pmatrix}\mathbb{A} & n\mathbb{A}\end{pmatrix}$ mátrix bármely két sorának különbsége kiegyensúlyozott. Továbbá a sorait kifeszítik az $[k|kn]$ és $[1|n]$ vektorok.

*Bizonyítás.* $v_i,\ v_j$ különböző sorokra

$$\begin{aligned} v_i - v_j &= [2ik - i^2 - (2jk - j^2) \mid 2nik - ni^2 - (2njk - nj^2)] = \\ &= [k(2i - 2j) - i^2 + j^2) \mid nk(2i - 2j) - n(i^2 - j^2))] = \\ &= (2i - 2j)[k \mid nk] - (i^2 - j^2)[1 \mid n] \end{aligned}$$

Továbbá vegyük észre, hogy $v_0 = [2ik - i^2 \mid 2nik - ni^2] = 2i[k \mid nk] - i^2[1 \mid n]$. Ebből következik, hogy $[k \mid nk]$ és $[1 \mid n]$ generálják a mátrix sorait. Továbbá $[k \mid nk]$ kiegyensúlyozott és egy nemnulla konstanssal való szorzás csupán permutálja a baloldali, illetve a jobboldali koordinátákat. Hozzáadva egy vektort, amely konstans a bal- és jobboldali koordinátáiban nem változtat a kiegyensúlyozottságon. □

**5.2.6. Állítás.** A $\begin{pmatrix}\mathbb{B} & \mathbb{C}\end{pmatrix}$ mátrix bármely két sorának különbsége kiegyensúlyozott. Továbbá sorterét kifeszítik a $[k \mid k], [1 \mid n]$ és $[k^2 \mid nk^2]$ vektorok.

*Bizonyítás.* $v_i,\ v_j$ különböző sorokra

$$\begin{aligned} v_i - v_j &= [(k - ni)^2 - (k - nj)^2 \mid n(i - k)^2 - n(j - k)^2] = \\ &= [k(2nj - 2ni) + n(ni^2 - nj^2) \mid ni^2 - nj^2 - k(2in - 2jn)] = \\ &= (2nj - 2ni)[k \mid k] + (ni^2 - nj^2)[n \mid 1] \end{aligned}$$

Vegyük észre, hogy a nulladik sor a $[k^2 \mid nk^2]$ vektor. Ezért minden sor előáll, mint

$$v_i = v_i - v_0 + v_0 = -2ni[k \mid k] + ni^2[n \mid 1] + [k^2 \mid nk^2]$$

Tehát a 3 vektor generálja a sorteret. □

**5.2.7. Állítás.** $4 \leq r(\mathbb{L}) \leq 5$, ahol $r(\mathbb{L})$ a mátrix rangját jelöli. Továbbá, ha $p \equiv 3 \mod 4$, akkor $n = -1$ kvadratikus nemmaradék választással $r(\mathbb{L}) = 4$.

*Bizonyítás.* Az előzőek alapján $[k \mid kn]$, $[1 \mid n]$, $[k \mid k]$, $[n \mid 1]$ és $[k^2 \mid nk^2]$ vektorok generálják $\mathbb{L}$ sorait. Tehát $r(\mathbb{L}) \leq 5$.

Az könnyen látható, hogy $[k \mid k]$ és $[k \mid kn]$ lineárisan független, hiszen $n \neq 1$. $[1 \mid n]$ lineárisan független a két vektortól, mert az $\alpha[k \mid k] + \beta[k \mid kn]$ összegben a legelső baloldali koordináta mindig 0.

Végül $\alpha[k \mid k] + \beta[k \mid kn] + \gamma[1 \mid n] = [(\alpha + \beta)k + \gamma \mid (\alpha + n\beta)k + \gamma n] = [k^2 \mid nk^2]$. A $k \mapsto (\alpha + n\beta)k$ függvény képterének mérete $p$ vagy 1, hiszen $k$-ban lineáris. A $k \mapsto k^2$ kvadratikus függvény képterének mérete viszont $\frac{p+1}{2}$. Tehát $r(\mathbb{L}) \geq 4$.

Az Euler kritérium alapján $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$, ahol a baloldali kifejezés a Legendre szimbólum. Más szavakkal a $-1$ pontosan akkor kvadratikus nemmaradék, ha $p \equiv 3 \pmod 4$. Ekkor ennek választva $n$-et $[1 \mid n]$ és $[n \mid 1]$ egymás skalárszorosai, így $r(\mathbb{L}) = 4$. □

**5.2.8. Állítás.** Az $\mathbb{L}$ mátrix log-Hadamard.

*Bizonyítás.* Ahhoz, hogy megmutassuk, hogy $\mathbb{L}$ log-Hadamard már csak annyira van szükségünk, hogy bármely "felső" és bármely "alsó" sor különbsége kiegyensúlyozott.

$$\begin{aligned} v_i - v_j &= [2ik - i^2 - (k - nj)^2 \mid n(2ik - i^2) - n(j - k)^2] = \\ &= [k(2i + 2nj) - k^2 - i^2 - n^2j^2 \mid k(2in + 2nj) - nk^2 - ni^2 - nj^2] \end{aligned}$$

Tehát a koordinátákat 2 darab másodfokú polinom írja le. Jelölje az első polinomfüggvényt $f$, a másodikat $g$. Arra van tehát szükségünk, hogy minden $m \in \mathbb{Z}_p$ súlya az $\operatorname{Im} f \bigcup \operatorname{Im} g$ multihalmazban 2 legyen.

A $\mathbb{Z}_p$ test felett a másodfokú egyenlet megoldóképlete ugyanúgy vezethető le, mint a valós számtest felett, így a megoldások elemszáma a diszkriminánson múlik. Vagyis, ha $\mathcal{M}$ jelöli az

$$ax^2 + bx + c = 0$$

egyenlet megoldásait, akkor

$$\begin{aligned} \mathcal{M} = 0 &\iff b^2 - 4ac \text{ kvadratikus nemmaradék} \\ \mathcal{M} = 1 &\iff b^2 - 4ac = 0 \\ \mathcal{M} = 2 &\iff b^2 - 4ac \text{ kvadratikus maradék} \end{aligned}$$

$f$ és $g$ diszkriminánsai a következők:

$$\begin{aligned} 4(i + nj)^2 - 4(i^2 + n^2 j^2) &= 8ijn \\ n^2(2i + j)^2 - 4n^2(i^2 + j^2) &= 8ijn^2 \end{aligned}$$

Végezetül, ha $n$ kvadratikus nemmaradék, akkor az $n$-el való szorzás bijekció $\mathbb{Z}_p$ kvadratikus maradékai és nemmaradékai között (illetve a 0-t 0-ba viszi). Mivel $g$ diszkriminánsa $f$-nek az $n$-szerese, így készen vagyunk.

$\square$

**5.2.9. Tétel.** Minden $p$ páratlan prímre $\mathbb{Z}_p^5$-ben létezik $2p$ elemű, $S$ spektrális halmaz. Ha $p \equiv 3 \mod 4$, már $\mathbb{Z}_p^4$-ben is létezik ilyen halmaz. Továbbá az $S$ halmaz nem parkettázza a csoportot.

*Bizonyítás.* Az eddigi állítások alapján, és 5.1.7 tétel alapján az első rész könnyen következik. Továbbá $2p$ nem osztja $p^d$, $d = 4, 5$ számot. $\square$

**5.2.10. Példa.** Legyen $p = 3$, $n = 2$ kvadratikus nemmaradék. Ekkor $\mathbb{L}$ a következő:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 2 & 0 \\ 2 & 0 & 1 & 1 & 0 & 2 \\ 0 & 1 & 1 & 0 & 2 & 2 \\ 1 & 1 & 0 & 2 & 0 & 2 \\ 1 & 0 & 1 & 2 & 2 & 0 \end{pmatrix}$$

A hozzárendelt Hadamard mátrix pedig

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \omega^2 & \omega & 1 & \omega & \omega^2 & 1 \\ \omega^2 & 1 & \omega & \omega & 1 & \omega^2 \\ 1 & \omega & \omega & 1 & \omega^2 & \omega^2 \\ \omega & \omega & 1 & \omega^2 & 1 & \omega^2 \\ \omega & 1 & \omega & \omega^2 & \omega^2 & 1 \end{pmatrix}$$

ahol $\omega = e^{\frac{2\pi i}{p}}$.

A fejezet utolsó tételében egy ismert konstrukciót mutatunk be. Ezt általában Hadamard mátrixokkal csinálják, és ekkor két mátrixnak az úgynevezett tenzorszorzatát szokták használni. Mi is ezt fogjuk csinálni átfogalmazva a műveletet a log-Hadamard mátrixok nyelvére.

**5.2.11. Tétel.** Bármely $p$ prímre konstruálható $2^m p^k$ nagyságú, $\mathbb{Z}_p$ feletti log-Hadamard mátrix, ahol $m \leq k$ nemnegatív egészek.

*Bizonyítás.* $\mathbb{A}$ és $\mathbb{B}$ $n \times n$ és $k \times k$ méretű négyzetes mátrixokra a $\mathbb{A} \boxplus \mathbb{B}$ mátrixot a következőképpen definiáljuk: $\mathbb{A}$ $i$-edik sorának $j$-edik oszlopába beírjuk az $\mathbb{B}'$ mátrixot, amit úgy kapunk, hogy $\mathbb{B}$ mátrix minden egyes eleméhez hozzáadjuk $\mathbb{A}_{i,j}$-t. Így kapunk egy $nk \times nk$ méretű mátrixot. Belátjuk, hogy ha $\mathbb{A}$ és $\mathbb{B}$ mátrixok log-Hadamardok voltal, akkor a $\mathbb{A} \boxplus \mathbb{B}$ is az.

Vegyünk két sort, vegyük a különbségüket és nézzük az első $k$ ($\mathbb{B}$ rendje) darab koordinátáját. Ez a "részvektor" a következő alakú:

$$(\mathbb{A}_{i,1} - \mathbb{A}_{j,1} + \mathbb{B}_{i',1} - \mathbb{B}_{j',1},\ \mathbb{A}_{i,1} - \mathbb{A}_{j,1} + \mathbb{B}_{i',2} - \mathbb{B}_{j',2}, \dots \mathbb{A}_{i,1} - \mathbb{A}_{j,1} + \mathbb{B}_{i',k} - \mathbb{B}_{j',k})$$

Ha $i' \neq j'$, akkor mivel $B$ log-Hadamard, így ez a részvektor kiegyensúlyozott. Az összes többi részvektorra is megnézve kapjuk, hogy kiegyensúlyozott.

Ha $i' = j'$, akkor ez a részvektor konstans lesz. De ekkor megnézve az összes többi részvektorra, azt látjuk, hogy csak $\mathbb{A}$ elemei vannak benne. Felhasználva, hogy $\mathbb{A}$ log-Hadamard, készen vagyunk.

Legyen $\mathbb{K}$ $\mathbb{Z}_p$ karaktertáblájából képzett log-Hadamard mátrix, $\mathbb{L}$ pedig az előzőleg generált mátrix. $\mathbb{L}$ mérete $2p \times 2p$, $\mathbb{K}$ mérete $p \times p$. Ebből tudunk tetszőleges $2^n p^k \times 2^n p^k$ $(n \leq k)$ méretű mátrixot generálni.

Ha $p = 2$, akkor a feladat az, hogy $2^m$ méretű mátrixot generáljunk. A

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

log-Hadamard mátrixot $m$-szer önmagával $\boxplus$-összeadva megkapjuk a kívánt előállítást. $\square$

# Függelék

## Parkettázás az egész számokon

Ahogy azt már említettük $\mathbb{Z}$ véges parkettázásai visszavezethetők a véges ciklikus csoportok parkettázásaira. A szekció [6] alapján lett feldolgozva.

**Definíció.** Legyen $A \subset \mathbb{Z}$. Azt mondjuk, hogy $A$ periodikus, ha $a + A = A$ valamilyen $a$ nemnulla számmal.

Nyilvánvaló a definícióból, hogy $A$ mindkét irányban végtelen. Azt hogy egy halmaz parkettázza $\mathbb{Z}$-t pont ugyanúgy definiáljuk, mint $\mathbb{Z}_n$-en. A véges esethez hasonlóan belátható, hogy ha a $A \oplus B = \mathbb{Z}$, akkor $(A + \{a\}) \oplus (B + \{b\})$ tetszőleges $a, b \in \mathbb{Z}$ számokra. Ezek alapján mindig feltehető, hogy $A$ csak nemnegatív számokat tartalmaz és a legkisebb eleme a 0.

**Tétel.** Tegyük fel, hogy $A \oplus B = \mathbb{Z}$ és $A$ véges. Ekkor $B$ periodikus.

*Bizonyítás.* Tegyük fel, hogy $A$ csak nemnegatív számokból áll, legkissebb eleme a 0, legnagyobb eleme $n$. Rögzített $k$-ra legyen $B(k) = \{b \in B : b < k\}$. Az $A + B(k)$ halmaz tartalmazza az összes elemet, ami $k$-nál szigorúan kissebb, de $n + k$-nál nagyobb számok közül egyet se tartalmaz.

Legyen $k + l$ az a legkisebb szám, ami nincs benne $A + B(k)$-ban. Ekkor $l \leq n$. A $k + l', 0 \leq l' < l$ számok mind előállnak $a' + b'$ alakban. Ha valamilyik ilyen számra $a' + b' \in B$, akkor szükségszerűen $a' = 0$ és $b' \in B(k)$, ami nem lehet hiszen $b' > k$. Ha $k + l = a + b \notin B$, akkor $b \geq k$ és $a > 0$, vagyis $k + l$. De ekkor a $0 + b$ szám se eleme $A + B(k)$, ami kisebb mint $a + b$. Vagyis $k + l'$, $0 \leq l' < l$ alakú számok nem $B$-beliek, de $k + l$ már az.

Megismételve a gondolatmenetet $B(x), k + 1 \leq x \leq k + l$ halmazokra mindegyiknél ugyanaz a $k + l$ lesz a legkisebb elem, ami nem eleme $A + B(x)$-nek. Csupán $B(k + l + 1)$-re fogunk új elemet kapni, mondjuk $k + l + 1 + d$-t, és ekkor a $k + l + 1, k + l + 2, \ldots k + l + d$ számok egyike se $B$-beli. Vagyis az $A + B(k)$ halmazok egyértelműen meghatározzák $B$-t.

Van-e olyan $k$ és $l$, melyre létezik $m > 0$, hogy $m + A + B(k) = A + B(l)$? Ilyen pontosan, akkor van, ha az $(A+B(k)) \cap \{k, k+1, \ldots, k+n-1\}$ pozitív eltoltjával a $(A+B(l)) \cap \{l, l+1, \ldots, l+n-1\}$ halmazt kapjuk. Mivel csak véges sokféleképpen helyezkedhetnek el a kiválasztott számok $k$ és $k+n-1$ között, így biztosan létezik ilyen $(k, l)$ számpáros. Könnyen látható, hogy ugyanez az $m$ jó lesz $(k + 1, l + 1), (k + 2, l + 2) \ldots$ párosokra is. Ebből és az előző megállapításból pedig már következik, hogy $m + B = B$. $\square$

**Következmény.** Legyen $A \subset \mathbb{Z}$ véges halmaz. A következő 3 kijelentés ekvivalens:

1. Létezik $B \subset \mathbb{Z}$, hogy $A \oplus B = \mathbb{Z}$.
2. Létezik $C \in \mathbb{Z}$ véges halmaz és $m$ pozitív egész szám, hogy $A \oplus (C \oplus \mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}$.
3. Létezik $C \in \mathbb{Z}$ véges halmaz és $m$ pozitív egész szám, hogy $A + C$ teljes maradékosztály modulo $m$.

Speciálisan, $A$ véges halmaz pontosan akkor parkettázza $\mathbb{Z}$-t, ha parkettázza $\mathbb{Z}_m$-et, valamilyen $m$ pozitív egészre.

**Megjegyzés.** Az hogy egy véges ciklikus csoportban egy részhalmaz periodikus-e, pontosan ugyanúgy lehet értelmezni, mint $\mathbb{Z}$-n. Tehát fel lehet tenni kérdést: milyen $\mathbb{Z}_n$ csoportokban igaz az, hogy ha $A \oplus B = \mathbb{Z}_n$, akkor $A$ vagy $B$ szükségszerűen periodikus. [6] összefoglalója alapján pontosan akkor igaz a tulajdonság, ha $n$ felírható a következő alakban: $p^N q$, $p^2q^2$, $p^2qr$, $pqrs$ vagy ilyen alakú számoknak az osztói, ahol $p, q, r, s$ különböző prímek és $N$ pozitív egész.

## Ellenpélda folytonos Fuglede sejtésre

A következőkben vázlatosan ismertetjük az ellenpélda konstrukciót a folytonos Fuglede sejtés spektrális parkettázó irányára. A szekció [17] alapján lett feldolgozva. Követve a forrás terminológiáját néhány definíciót módosítunk az eddigiekhez képest. A komplex Hadamard mátrix definíciója nem változik.

**Definíció.** Az $\mathbb{A} = \{a_{i,j}\}_{i,j=1}^d \in \mathbb{Z}^{d\times d}$ mátrixra azt mondjuk, hogy log-Hadamard mátrix, ha az $\{e^{2\pi i a_{i,j}}\}_{i,j=1}^d$ mátrix komplex Hadamard.

**Definíció.** Legyen $T = \{t_1, t_2, \dots t_k\} \subset \mathbb{Z}^d$ véges halmaz és jelölje $\mathbb{T}$ azt a $k \times d$ méretű mátrixot, melynek $j$-edik oszlopa $t_j$. Azt mondjuk, hogy $T$ spektrális, ha létezik $\mathbb{L} \in \mathbb{R}^{k\times d}$, melyre $\mathbb{L}\mathbb{T}$ log-Hadamard.

Bebizonyítható, hogy ez a definíció egyenértékű az általános spektralitás fogalmával. A következőkben $[0,n)^d_{\mathbb{Z}}$-vel fogjuk jelölni a $[0,n)^d \cap \mathbb{Z}^d$ halmazt.

**Definíció.** Azt mondjuk, hogy a $T \subset \mathbb{Z}^d$ halmaz $m-$parkettáz, ha létezik $S \subset \mathbb{Z}^d$ halmaz, hogy $T \oplus S = [0,m)^d_{\mathbb{Z}}$ oly módon, hogy két tag összeadása után a koordinátákat redukáljuk modulo $m$. Azt mondjuk, hogy a $T \subset \mathbb{Z}^d$ halmaz $m-$spektrális, ha létezik spektruma ($\mathbb{Z}^d$-ben), melynek minden eleme $\frac{1}{m}\mathbb{Z}^d$-beli.

**Állítás** ([17])**.** Ha $T \subset \mathbb{Z}^d$ spektrális ($\mathbb{Z}^d$-ben), akkor $T + [0,1)^d$ spektrális $\mathbb{R}^d$-ben.

**Állítás** ([17] proposition 2.1)**.** Tegyük fel, hogy $T \subset \mathbb{Z}^d$ egy $m-$parketta ($m-$spektrális) és $S \subset \mathbb{Z}^d$ pedig $n-$parketta ($n-$spektrális). Ekkor $T + mS$ halmaz $mn-$parketta ($mn-$spektrális).

**Állítás** ([17] proposition 2.5)**.** Tegyük fel, hogy a $T \subset \mathbb{Z}^d$ nem $m-$parketta. Ekkor létezik nagy $n$ szám, melyre $T + m[0,n)^d_{\mathbb{Z}}$ nem parkettázza $\mathbb{Z}^d$-t.

**Tétel.** Ha $d = 4$, akkor létezik $S = \{s_1, s_2, \dots, s_t\}$ halmaz, hogy a $\Omega = \cup_{i=1}^t (s_i + [0,1)^d)$ halmaz spektrális, de nem parkettáz.

*Bizonyítás vázlat.* 5.2.9 tétel alapján tudunk generálni, olyan $\mathbb{K}$ mátrixot $\mathbb{Z}_3$ felett, melynek rangja 4 és $\frac{1}{3}\mathbb{K}$ log-Hadamard. Így léteznek szintén $\mathbb{Z}_p$ felett $\mathbb{L}$ $6 \times 4$-es és $\mathbb{T}$ $4 \times 6$-os mátrixok, melyek szorzata $\mathbb{K}$. Ha most $\mathbb{L}$-re és $\mathbb{T}$-re úgy tekintünk, mint $\mathbb{Z}$ feletti mátrixok, akkor $\frac{1}{3}\mathbb{L}\mathbb{T}$ mátrix log-Hadamard. $T \subset \mathbb{Z}^4$ halmaznak választva $\mathbb{T}$ sorait azt kapjuk, hogy $T$ 3-spektrális. Mivel 6 nem osztja $3^4$-t, így $T$ nem 3-parketta.

Az előző állítások miatt nagy $n$-re $S = T + 3[0,n)^4$ $3n$-spektrális, de nem $3n$-parketta.

Szintén előző állítás miatt ekkor $\cup_{s\in S}\{s + [0,1)^4\}$ halmaz spektrális $\mathbb{R}^4$-ben. Meggondolható, hogy ekkor mivel $S$ nem parkettáz $\mathbb{Z}^4$-ben, így $\cup_{s\in S}\{s + [0,1)^4\}$ nem parkettázza $\mathbb{R}^4$. □

A bizonyítás hasonlóan megy $d \geq 5$ esetre.

# Irodalomjegyzék


[1] C. Aten, B. Ayachi, E. Bau, D. FitzPatrick, A. Iosevich, H. Liu, A. Lott, I. MacKinnon, S. Maimon, S. Nan, J. Pakianathan, G. Petridis, C. Rojas Mena, A. Sheikh, T. Tribone, J. Weill, and C. Yu. Tiling sets and spectral sets over finite fields. *Journal of Functional Analysis*, 273(8):2547–2577, 2017.

[2] K. Corrádi and S. Szabó. A new proof of rédei's theorem. *Pacific Journal of Mathematics*, 140(1):53–61, 1989.

[3] E. Coven and A. Meyerowitz. Tiling the integers with translates of one finite set. *Journal of Algebra*, 212(1):161–174, 1999.

[4] D. E. Dutkay and C. Lai. Some reductions of the spectral set conjecture to integers. *Mathematical Proceedings of the Cambridge Philosophical Society*, 156(1):123–135, 2013.

[5] S. J. Ferguson and N. Sothanaphan. Fuglede's conjecture fails in 4 dimensions over odd prime fields. *Discrete Mathematics*, 343(1):111507, 2020.

[6] L. Fuchs. *Abelian Groups*. Akadémiai Kiadó, 1966.

[7] B. Fuglede. Commuting self-adjoint partial differential operators and a group theoretic problem. *Journal of functional analysis*, 16(1):101–121, 1974.

[8] G. Hajós. Sur le problème de factorisation des groupes cycliques. *Acta Mathematica Academiae Scientiarum Hungarica*, 1(2-4):189–195, 1950.

[9] A. Iosevich, N. H. Katz, and T. Tao. Convex bodies with a point of curvature do not have fourier bases. *American Journal of Mathematics*, 123(1):115–120, 2001.

[10] A. Iosevich, N. H. Katz, and T. Tao. The fuglede spectral conjecture holds for convex planar domains. *Mathematical Research Letters*, 10(5):559–569, 2003.

[11] G. Kiss, R. D. Malikiosis, G. Somlai, and M. Vizer. Fuglede's conjecture holds for cyclic groups of order $pqrs$. *arXiv preprint arXiv:2011.09578*, 2020.

[12] G. Kiss, R. D. Malikiosis, G. Somlai, and M. Vizer. On the discrete fuglede and pompeiu problems. *Analysis and Partial Differential Equations*, 13(3):765–788, 2020.

[13] M. Kolountzakis. Lattice tilings by cubes: whole, notched, extended. *The electronic journal of combinatorics*, 5, 1998.

[14] M. Kolountzakis. Non-symmetric convex domains have no basis of exponentials. *Illinois Journal of Mathematics*, 44(3):542–550, 1999.

[15] M. Kolountzakis and M. Matolcsi. Tilings by translation. *arXiv preprint arXiv:1009.3799*, 2010.

[16] N. Lev and M. Matolcsi. The fuglede conjecture for convex domains is true in all dimensions. *arXiv preprint arXiv:1904.12262*, 2019.

[17] M. Matolcsi. Fuglede's conjecture fails in dimension 4. *Proceedings of the American Mathematical Society*, 133(10):3021–3026, 2005.

[18] R. Mohan. On hadamard conjecture. *arXiv preprint cs/0604050*, 2006.

[19] L. Rédei. Die neue theorie der endlichen abelschen gruppen und verallgemeinerung des hauptsatzes von hajós. *Acta Mathematica Academiae Scientiarum Hungarica*, 16(3):329–373, 1965.

[20] R. Shi. Fuglede's conjecture holds on cyclic groups $\mathbb{Z}_{pqr}$. *Discrete Analysis*, 14(14):12–13, 2019.

[21] B. Steinberg. *Representation theory of finite groups.* Springer, 2012.

[22] T. Tao. Some notes on the coven-meyerowitz conjecture. `https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/`.

[23] T. Tao. Fuglede's conjecture is false on 5 or higher dimensions. *Mathematical Research Letters*, 11(2):251–258, 2004.

[24] I. Łaba. Fuglede's conjecture for a union of two intervals. *Proceedings of the American Mathematical Society*, 129(10):2965–2972, 01 2001.

[25] I. Łaba. The spectral set conjecture and multiplicative properties of roots of polynomials. *Journal of the London Mathematical Society*, 65(3):661–671, 2002.